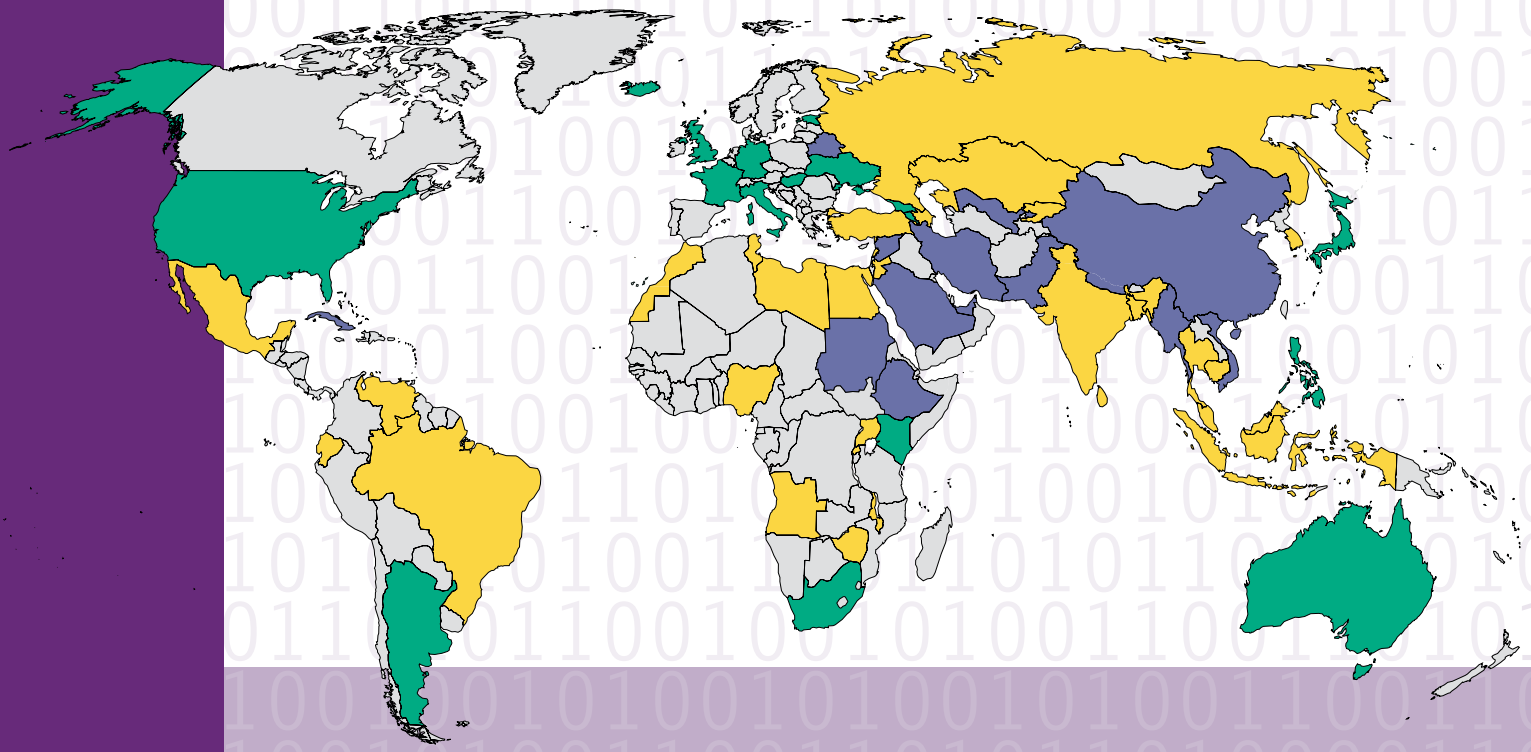
FREEDOM ON THE NET 2013

A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA



SUMMARY OF FINDINGS
AND COUNTRY REPORTS

www.freedomhouse.org

FREEDOM ON THE NET 2013

A Global Assessment of Internet and Digital Media

Sanja Kelly
Mai Truong
Madeline Earp
Laura Reed
Adrian Shahbaz
Ashley Greco-Stoner

EDITORS

October 3, 2013

This report was made possible by the generous support of the Dutch Ministry of Foreign Affairs, the U.S. State Department's Bureau of Democracy, Human Rights and Labor (DRL), and Google. The content of this publication is the sole responsibility of Freedom House and does not necessarily represent the views of the Dutch Foreign Ministry, DRL, or Google.

TABLE OF CONTENTS

COUNTRY REPORTS

COUNTRY REPORTS

ACKNOWLEDGMENTS

Completion of the *Freedom on the Net* publication would not have been possible without the tireless efforts of the following individuals.

As project director, Sanja Kelly oversaw the research, editorial, and administrative operations, supported by research analysts Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz, and senior research assistant Ashley Greco-Stoner. Together, they provided essential research and analysis, edited the country reports, conducted field visits in Uganda, Indonesia, Mexico, Jordan, and Hungary, and led capacity building workshops abroad. Over 70 external consultants served as report authors and advisors, and made an outstanding contribution by producing informed analyses of a highly diverse group of countries and complex set of issues.

Helpful contributions and insights were also made by Daniel Calingaert, executive vice president; Arch Puddington, vice president for research; as well as other Freedom House staff in the United States and abroad. Freedom House is also grateful to Cristiana Gonzalez and Eleonora Rabinovich for their contributions during the Latin America ratings review meeting.

This publication was made possible by the generous support of the Dutch Ministry of Foreign Affairs, U.S. State Department's Bureau of Democracy, Human Rights, and Labor (DRL), and Google. The content of the publication is the sole responsibility of Freedom House and does not necessarily reflect the views of the Dutch Foreign Ministry, DRL, Google, or any other funder.

DESPITE PUSHBACK, INTERNET FREEDOM DETERIORATES

By Sanja Kelly

In June 2013, revelations made by former contractor Edward Snowden about the U.S. government's secret surveillance activities took center stage in the American and international media. As part of its antiterrorism effort, the U.S. National Security Agency (NSA) has been collecting communications data on Americans and foreigners on a much greater scale than previously thought. However, while the world's attention is focused on Snowden and U.S. surveillance—prompting important discussions about the legitimacy and legality of such measures—disconcerting efforts to both monitor and censor internet activity have been taking place in other parts of the world with increased frequency and sophistication. In fact, global internet freedom has been in decline for the three consecutive years tracked by this project, and the threats are becoming more widespread.

Global internet freedom has been in decline for the three consecutive years tracked by this project.

Of particular concern are the proliferation of laws, regulations, and directives to restrict online speech; a dramatic increase in arrests of individuals for something they posted online; legal cases and intimidation against social-media users; and a rise in surveillance. In authoritarian states, these tools are often used to censor and punish users who engage in online speech that is deemed critical of the government, royalty, or the dominant religion. In some countries, even blogging about environmental pollution, posting a video of a cynical rap song, or tweeting about the town mayor's poor parking could draw the police to a user's door. Although democratic states generally do not target political speech, several have sought to implement disproportionate restrictions on content they perceive as harmful or illegal, such as pornography, hate speech, and pirated media.

In some countries, even posting a video of a cynical rap song could draw the police to a user's door.

Nonetheless, in a number of places around the world, growing efforts by civic activists, technology companies, and everyday internet users have been able to stall, at least in part, newly proposed restrictions, forcing governments to either shelve their plans or modify some of the more problematic aspects of draft legislation. In a handful of countries, governments have been increasingly open to engagement with civil society, resulting in the passage of laws perceived to protect internet freedom. While such

Sanja Kelly directs the *Freedom on the Net* project at Freedom House.

positive initiatives are significantly less common than government attempts to control the online sphere, the expansion of this movement to protect internet freedom is one of the most important developments of the past year.

To illuminate the nature of evolving threats in the rapidly changing global environment, and to identify areas of opportunity for positive change, Freedom House has conducted a comprehensive study of internet freedom in 60 countries around the world. This report is the fourth in its series and focuses on developments that occurred between May 2012 and April 2013. The previous edition, covering 47 countries, was published in September 2012. *Freedom on the Net 2013* assesses a greater variety of political systems than its predecessors, while tracing improvements and declines in the countries examined in the previous editions. Over 70 researchers, nearly all based in the countries they analyzed, contributed to the project by examining laws and practices relevant to the internet, testing the accessibility of select websites, and interviewing a wide range of sources.

Of the 60 countries assessed, 34 have experienced a negative trajectory since May 2012.

Of the 60 countries assessed, 34 have experienced a negative trajectory since May 2012. Further policy deterioration was seen in authoritarian states such as Vietnam and Ethiopia, where the downgrades reflected new government measures to restrict free speech, new arrests, and harsh prison sentences imposed on bloggers for posting articles that were critical of the authorities. Pakistan's downgrade reflected the blocking of thousands of websites and pronounced violence against users of information and communication technologies (ICTs). In Venezuela, the decline was caused by a substantial increase in censorship surrounding politically sensitive events: the death of President Hugo Chávez and the presidential elections that preceded and followed it.

Deterioration was also observed in a number of democracies, often as a result of struggles to balance freedom of expression with security. The most significant year-on-year decline was seen in India, which suffered from deliberate interruptions of mobile and internet service to limit unrest, excessive blocks on content during rioting in northeastern states, and an uptick in the filing of criminal charges against ordinary users for posts on social-media sites. The United States experienced a significant decline as well, in large part due to reports of extensive surveillance tied to intelligence gathering and counterterrorism. And in Brazil, declines resulted from increasing limitations on online content, particularly in the context of the country's stringent electoral laws; cases of intermediary liability; and increasing violence against online journalists.

Deterioration was also observed in a number of democracies, often as a result of struggles to balance freedom of expression with security.

At the same time, 16 countries registered a positive trajectory over the past year. In Morocco, which was analyzed for the first time in this edition of the report, the government has unblocked previously censored websites as part of its post–Arab Spring reform effort, although it still frequently punishes those who post controversial information. Burma's continued improvement included significant steps toward the lifting of internet censorship, which may allow the country to

shed its history of repression and underdevelopment and create a more progressive media environment. Tunisia's gains are the result of the government's sustained efforts to open up the online sphere following years of repression under former president Zine el-Abidine Ben Ali, and institute protections for journalists and bloggers, although there is still much to be done. And in several countries like Georgia and Rwanda, improvements stemmed from a decline in the number of negative incidents from the previous coverage period.

Despite the noted improvements, restrictions on internet freedom continue to expand across a wide range of countries. Over the past year, the global number of censored websites has increased, while internet users in various countries have been arrested, tortured, and killed over the information they posted online. Iran, Cuba, and China remain among the most restrictive countries in the world when it comes to internet freedom. In Iran, the government utilized more advanced methods for blocking text messages, filtering content, and preventing the use of circumvention tools in advance of the June 2013 election, while one blogger was found dead in police custody after being arrested for criticizing the government online. In Cuba, the authorities continued to require a special permit for anyone wishing to access the global internet; the permits are generally granted to trusted party officials and those working in specific professions. And as in previous years, China led the way in expanding and adapting an elaborate technological apparatus for systemic internet censorship, while further increasing offline coercion and arrests to deter free expression online.

Over the past year, the global number of censored websites has increased, while internet users in various countries have been arrested, tortured, and killed over the information they posted online.

Based on a close evaluation of each country, this study identifies the 10 most commonly used types of internet control, most of which appear to have become more widespread over the past year:

Blocking and filtering:

Governments around the world are increasingly establishing mechanisms to block what they deem to be undesirable information. In many cases, the censorship targets content involving child pornography, illegal gambling, copyright infringement, or the incitement of violence. However, a growing number of governments are also engaging in deliberate efforts to block access to information related to politics, social issues, and human rights. Of the 60 countries evaluated this year, 29 have used blocking to suppress certain types of political and social content. China, Iran, and Saudi Arabia possess some of the most comprehensive blocking and filtering capabilities, effectively disabling access to thousands of websites, but even some democratic countries like South Korea and India have at times blocked websites of a political nature. Jordan and Russia, which previously blocked websites only sporadically, are among the countries that have intensified their efforts over the past year.

Cyberattacks against regime critics:

Some governments and their sympathizers are increasingly using technical attacks to disrupt activists' online networks, eavesdrop on their communications, and cripple their websites. Over the past year, such attacks were reported in at least 31 of the countries covered in this study. In Venezuela, for example, during the 2012 and 2013 presidential campaigns, the websites of popular independent media—Noticiero Digital, Globovisión, and La Patilla—were repeatedly subject to distributed denial-of-service (DDoS) attacks, which increased on election days and during the vote count. In countries ranging from Belarus to Vietnam to Bahrain, opposition figures and activists are routinely targeted with malicious software that is masked as important information about political developments or planned protests. When downloaded, the malware can enable attackers to monitor the victims' keystrokes and eavesdrop on their personal communications. Although activists are increasingly aware of this practice and have been taking steps to protect themselves, the attacks are becoming more sophisticated and harder to detect.

New laws and arrests for political, religious, or social speech online:

Instead of merely blocking and filtering information that is deemed undesirable, an increasing number of countries are passing new laws that criminalize certain types of political, religious, or social speech, either explicitly or through vague wording that can be interpreted in such a way. Consequently, more users are being arrested, tried, or imprisoned for their posts on social networks, blogs, and websites. In fact, some governments may prefer to institute strict punishments for people who post offending content rather than actually blocking it, as this allows officials to maintain the appearance of a free and open internet while imposing a strong incentive for users to practice self-censorship. Even countries willing to invest in systematic filtering often find that criminal penalties remain an important deterrent. Turkey, Bangladesh, and Azerbaijan are among the countries that have, over the past year, significantly stepped up arrests of users for their online activism and posts.

More users are being arrested, prosecuted, or imprisoned for their posts on social networks, blogs, and websites.

Paid progovernment commentators manipulate online discussions:

Already evident in a number of countries assessed in the previous edition of *Freedom of the Net*, the phenomenon of paid progovernment commentators has spread in the past two years, appearing in 22 of the 60 countries examined in this study. The purpose of these commentators—covertly hired by government officials, often by using public funds—is to manipulate online discussions by trying to smear the reputation of government opponents, spread propaganda, and defend government policies when the discourse becomes critical. China, Bahrain, and Russia have been at the forefront of this practice for several years, but countries like Malaysia, Belarus, and Ecuador are increasingly using the same tactics, particularly surrounding politically sensitive events such as elections or major street protests.

Physical attacks and murder:

Governments and powerful nonstate actors are increasingly resorting to physical violence to punish those who disseminate critical content, with sometimes fatal consequences. In 26 of the 60 countries assessed, at least one blogger or internet user was attacked, beaten, or tortured for something posted online. In 5 of those countries, at least one activist or citizen journalist was killed in retribution for information posted online, in most cases information that exposed human rights abuses. Syria was the most dangerous place for online reporters, with approximately 20 killed over the past year. In Mexico, several online journalists were murdered after refusing to stop writing exposés about drug trafficking and organized crime. In Egypt, several Facebook group administrators were abducted and beaten, while citizen journalists were allegedly targeted by the security forces during protests.

In 5 countries, at least one activist or citizen journalist was killed in retribution for information posted online.

Surveillance:

Many governments are seeking less visible means to infringe on internet freedom, often by increasing their technical capacity or administrative authority to monitor individuals' online behavior or communications. Governments across the spectrum of democratic performance have enhanced their surveillance capabilities in recent years or have announced their intention to do so. Although some interception of communications may be necessary for fighting crime or preventing terrorist attacks, surveillance powers are increasingly abused for political ends. Governments in nearly two-thirds of the countries examined upgraded their technical or legal surveillance powers over the past year (see surveillance section in "Major Trends" below). It is important to note that increased surveillance, particularly in authoritarian countries where the rule of law is weak, often leads to increased self-censorship, as users become hesitant to risk repercussions by criticizing the authorities online.

Governments across the spectrum of democratic performance have enhanced their surveillance capabilities in recent years.

Takedown requests and forced deletion of content:

Instead of blocking objectionable websites, many governments opt to contact the content hosts or social-media sites and request that the content be "taken down." While takedown notices can be a legitimate means of dealing with illegal content when the right safeguards are in place, many governments and private actors are abusing the practice by threatening legal action and forcing the removal of material without a proper court order. A more nefarious activity, which is particularly common in authoritarian countries, involves government officials informally contacting a content producer or host and requesting that particular information be deleted. In some cases, individual bloggers or webmasters are threatened with various reprisals should they refuse. In Russia and Azerbaijan, for example, bloggers have reported deleting comments from their websites after being told that they would be fired from their jobs, barred from universities, or detained if they did not comply.

Blanket blocking of social media and other ICT platforms:

Given the increasing role that social media have played in political and social activism, particularly after the events of the Arab Spring, some governments have been specifically targeting sites like YouTube, Twitter, and Facebook in their censorship campaigns. In 19 of the 60 countries examined, the authorities instituted a blanket ban on at least one blogging, microblogging, video-sharing, social-networking, or live-streaming platform. However, as their knowledge and sophistication grows, some governments are beginning to move toward blocking access to individual pages or profiles on such services or requesting from the companies to disable access to the offending content. These dynamics were particularly evident surrounding protests that erupted after the anti-Islam video *Innocence of Muslims* appeared on YouTube. Voice over Internet Protocol (VoIP) and free messaging services such as Skype, Viber, and WhatsApp are also frequently targeted—in some countries due to difficulties the authorities face in intercepting such communication tools, and in others because the telecommunications industry perceives them as a threat to their own revenue. Lebanon, Ethiopia, and Burma are among several countries where the use of VoIP services remained prohibited as of May 2013.

Holding intermediaries liable:

An increasing number of countries are introducing directives, passing laws, or interpreting current legislation so as to make internet intermediaries—whether internet service providers (ISPs), site hosting services, webmasters, or forum moderators—legally liable for the content posted by others through their services and websites. As a consequence, intermediaries in some countries are voluntarily taking down or deleting potentially objectionable websites or comments to avoid legal liability. In the most extreme example, intermediary liability in China has resulted in private companies maintaining whole divisions responsible for monitoring the content of social-media sites, search engines, and online forums, deleting tens of millions of messages a year based on administrators' interpretation of both long-standing taboos and daily directives from the ruling Communist Party. In 22 of the 60 countries examined, intermediaries were held to a disproportionate level of liability, either by laws that clearly stipulate such rules or by court decisions with similar effects. In one recent example, Brazilian authorities issued arrest warrants for two senior Google Brazil executives on the grounds that the company failed to remove content that was prohibited under strict laws governing electoral campaigns.

Intermediaries in some countries are voluntarily taking down or deleting potentially objectionable websites or comments to avoid legal liability.

Throttling or shutting down internet and mobile service:

During particularly contentious events, a few governments have used their control over the telecommunications infrastructure to cut off access to the internet or mobile phone service in a town, a region, or the entire country. Egypt became the best-known case study in

January 2011, when the authorities shut off the internet for five days as protesters pushed for the ouster of longtime president Hosni Mubarak. However, a number of other countries have also cut off access to the internet or mobile phone networks. In Syria, several such shutdowns occurred over the past year. In Venezuela, the dominant ISP temporarily shut off access during the presidential election in 2012, allegedly due to cyberattacks. India and China disabled text messaging on mobile phones in particular regions during protests and rioting. In addition to outright shutdowns, some countries have used throttling, the deliberate slowing of connection speeds, to prevent users from uploading videos or viewing particular websites without difficulty. Over the past year, however, there were fewer instances of internet shutdowns and throttling than in the previous year, most likely because countries affected by the Arab Spring in 2011 had moved past the point where such tactics would be useful to the authorities.

MAJOR TRENDS

Although many different types of internet control have been institutionalized in recent years, three particular trends have been at the forefront of increased censorship efforts: increased surveillance, new laws that restrict online speech, and arrests of users. Despite these threats, civic activism has also been on the rise, providing grounds for hope that the future may bring more positive developments.

Surveillance grows considerably as countries upgrade their monitoring technologies

Starting in June 2013, a series of leaks by former U.S. contractor Edward Snowden revealed that the NSA was storing the personal communications metadata of Americans—such as the e-mail addresses or phone numbers on each end, and the date and time of the communication—and mining them for leads in antiterrorism investigations. Also exposed were details of the PRISM program, through which, among other things, the NSA monitored communications of non-Americans via products and services offered by U.S. technology companies. It then came to light that several other democratic governments had their own surveillance programs aimed at tracking national security threats and cooperating with the NSA. While there is no evidence that the NSA surveillance programs were abused to suppress political speech, they have drawn strong condemnations at home and abroad for their wide-reaching infringements on privacy. Since many large technology companies—with millions of users around the world—are based in the United States, the NSA was able to collect information on foreigners without having to go through the legal channels of the countries in which the targeted users were located.

Although the U.S. surveillance activities have taken the spotlight in recent months, this study reveals that most countries around the world have enhanced their surveillance powers over the past year. In 35 of the 60 countries examined in *Freedom on the Net 2013*, the government has either obtained more sophisticated technology to conduct surveillance, increased the scope and number of people monitored, or passed a new law giving it greater monitoring authority. There is a strong suspicion that many of the remaining 25 countries' governments have also stepped up their surveillance activities, though some may be better than others at covering their tracks.

In 35 of the 60 countries examined, the government has obtained more sophisticated surveillance technology, increased the scope of people monitored, or passed a new law giving it greater monitoring authority. Growing surveillance is also suspected in many of the remaining 25 countries, but they may be better at covering their tracks.

While democratic countries have often engaged in legally dubious surveillance methods to combat and uncover terrorism threats, officials in many authoritarian countries also monitor the personal communications of their citizens for political reasons, with the goal of identifying and suppressing government critics and human rights activists. Such monitoring can have dire repercussions for the targeted individuals, including imprisonment, torture, and even death. In Bahrain, Ethiopia, Azerbaijan, and elsewhere, activists reported that their e-mail, text messages, or other communications were presented to them during interrogations or used as evidence in politicized trials. In many of these countries, the state owns the main telecommunications firms and ISPs, and it does not have to produce a warrant from an impartial court to initiate surveillance against dissidents.

Russia has emerged as an important incubator of surveillance technologies and legal practices that are emulated by other former Soviet republics. Russia itself has dramatically expanded its surveillance apparatus in recent years, particularly following the events of the Arab Spring. Moreover, in December 2012, the Russian Supreme Court upheld the legality of the government's hacking into the phone of an opposition activist. The court grounded its decision on the fact that the activist had participated in antigovernment rallies, prompting fears that the case would be used as a legal basis for even more extensive surveillance against opposition figures in the future. Belarus, Uzbekistan, Kyrgyzstan, Kazakhstan, and Ukraine are among the countries that have implemented the ICT monitoring system used by the Russians authorities (known by the acronym SORM) and have either passed or considered legislation that would further expand their surveillance powers, in some cases mimicking the current legislation in Russia.

All 10 of the African countries examined in this report have stepped up their online monitoring efforts in the past year.

Until recently, only a handful of African countries had the means to conduct widespread surveillance. However, this seems to be changing rapidly as internet penetration increases and surveillance technologies become more readily available. All 10 of the African countries examined in this report have stepped up their online monitoring efforts in the past year, either by obtaining new technical capabilities or by expanding the government's legal authority. In Sudan, the government's ICT surveillance was particularly pronounced in 2012

during a series of street protests, and it became dangerous for activists to use their mobile phones. One activist switched off his phone for a few days to avoid arrest while hiding from the authorities. When he turned it back on to call his family, officials quickly determined his location and arrested him the same day.

In the Middle East and North Africa, where extralegal surveillance has long been rampant, the authorities continue to use ICT monitoring against regime opponents. In Saudi Arabia, the government has been proactively recruiting experts to work on intercepting encrypted data from mobile applications such as Twitter, Viber, Vine, and WhatsApp. In Egypt, President Mohamed Morsi's advisers reportedly met with the Iranian spy chief in December 2012 to seek assistance in building a surveillance apparatus that would be controlled by the office of the president and operated outside of traditional security structures. Even in postrevolutionary Libya, reports surfaced in mid-2012 that surveillance tools left over from the Qadhafi era had been restored, apparently for use against suspected loyalists of the old regime.

Perhaps most worrisome is the fact that an increasing number of countries are using malware to conduct surveillance when traditional methods are less effective. Opposition activists in the United Arab Emirates, Bahrain, Malaysia, and more than a dozen other countries were targeted with malware attacks over the past year, giving the attackers remote access to victims' e-mail, keystrokes, and voice communications. While it is difficult to know with a high degree of certainty, there are strong suspicions that these activists' respective governments were behind the attacks. Some democratic governments—including in the United States and Germany—have used malware to conduct surveillance in criminal investigations, but any such use typically must be approved by a court order and narrowly confined to the scope of the investigation.

Censorship intensifies as countries pass new laws and directives to restrict online speech

Until several years ago, very few countries had laws that specifically dealt with ICTs. As more people started to communicate online—particularly via social media, which allow ordinary users to share information on a large scale—an increasing number of governments have introduced new laws or amended existing statutes to regulate speech and behavior in cyberspace. Since launching *Freedom on the Net* in 2009, Freedom House has observed a proliferation of such legislative activity. This trend accelerated over the past year, and since May 2012 alone, 24 countries have passed new laws or implemented new regulations that could restrict free speech online, violate users' privacy, or punish individuals who post certain types of content.

24 countries have passed new laws or implemented new regulations that could restrict free speech online, violate users' privacy, or punish individuals who post certain types of content.

Many authoritarian countries have used legitimate concerns about cybercrime and online identity theft to introduce new legal measures that criminalize critical political speech. In November 2012, the government of the United Arab Emirates issued a new cybercrime law that provides a sounder legal basis for combatting

online fraud, money laundering, hacking, and other serious abuses. However, the law also contains punishments for offending the state, its rulers, and its symbols, and for insulting Islam and other religions. Those found guilty of calling for a change to the ruling system can face a sentence of life in prison. In September 2012, Ethiopia's government passed the Telecom Fraud Offenses law, which is supposed to combat cybercrime but also includes provisions that toughen the ban on VoIP, require users to register all ICT equipment (including smartphones) and carry registration permits with them, and apply penalties under an antiterrorism law to certain types of electronic communications. Considering that free speech activists have already been tried under the antiterrorism laws for criticism of the regime, the new legislation was met with significant concern.

Several countries have also passed new laws intended to block information that is perceived as "extremist" or harmful to children. While such concerns have led to legitimate policy discussions in a wide range of countries, some of the recent legislation is so broadly worded that it can easily be misused or turned on political dissidents. For example, the Russian parliament in July 2012 passed what is commonly known as the "internet blacklist law," which allows blocking of any website with content that is considered harmful to minors, such as child pornography and information related to suicide techniques and illegal drug use. However, the law has also been used occasionally to block other websites, such as a blog by an opposition figure (no official reason for blocking was provided) or another blog that featured a photo-report on the self-immolation of a Tibetan independence activist protesting the visit of the Chinese president (the official reason for blocking was that the post promoted suicide). In Kyrgyzstan, a new law allows the government to order web hosting services to shut down websites hosted in Kyrgyzstan, or the blocking of any sites hosted outside the country, if officials recognize the content as "extremist," which is very broadly defined.

In some countries, the authorities have decided to institute stricter regulations specifically aimed at online news media. The traditional media in authoritarian states are typically controlled by the government, and users often turn to online news outlets for independent information. The tighter controls are designed to help rein in this alternative news source. A new law in Jordan requires any electronic outlet that publishes domestic or international news, press releases, or comments to register with the government; it places conditions on who can be the editor in chief of such outlets; and it prohibits foreign investment in news media. The penalties for violations include fines and blocking, and in May 2013 the government proceeded to block over 200 websites that failed to comply with the new rules. Similarly, in Sri Lanka, online news outlets are now required to obtain a license, which can be denied or withdrawn at any time.

More users are arrested, and face harsher penalties, for posts on social media

Laws that restrict free speech are increasingly forcing internet users into courts or behind bars. Over the past year alone, in 28 of the 60 countries examined, at least one user was arrested or imprisoned for posting certain types of political, social, or religious content online. In fact, a growing number of governments seem to exert control over the internet not through blocking and filtering, but by arresting people after the posts are published online. In addition, courts in some

In 28 of the 60 countries examined, at least one user was arrested or imprisoned for posting political, social, or religious content online.

countries have allowed higher penalties for online speech than for equivalent speech offline, arguably because of the internet's wider reach.

As more people around the world utilize social media to express their opinions and communicate with others, there has been a dramatic increase in arrests for posts on sites such as Twitter, Facebook, and YouTube. In at least 26 of the examined countries, users were arrested for politically or socially relevant statements on social-media sites. Although political activists are targeted most frequently, more and more ordinary, apolitical users have found themselves in legal trouble after casually posting their opinions and jokes. Unlike large media companies and professional journalists with an understanding of the legal environment, many users of this kind may be unaware that their writings could land them in jail.

Last year in India, for example, at least eleven users were charged under the so-called IT Act for posting or "liking" posts on Facebook. In one of the best-known cases, police arrested a woman for complaining on Facebook about widespread traffic and service disruptions in her town to mark the death of the leader of a right-wing Hindu nationalist party. The woman's friend, who "liked" the comment, was also arrested. The detentions were widely criticized, both on social media and by public figures, and the charges were later dropped. In Ethiopia, a student was arrested and charged with criminal defamation after he posted a comment on his Facebook page that criticized the "rampant corruption" at another local university.

A woman in India was arrested for "liking" a friend's status on Facebook.

Users are most often detained and tried for simply criticizing or mocking the authorities. At least 10 users were arrested in Bahrain over the past year and charged with "insulting the king on Twitter," and several ultimately received prison sentences ranging from one to four months. In Morocco, an 18-year-old student was sentenced to 18 months in prison for "attacking the nation's sacred values" after he allegedly ridiculed the king in a Facebook post, and a 25-year-old activist received an even harsher sentence for criticizing the king in a YouTube video. In Vietnam, several bloggers were sentenced to between 8 and 13 years in prison on charges that included "defaming state institutions" and "misuse of democratic freedoms to attack state interests."

In addition to criticism of political leaders, speech that might offend religious sensitivities is landing a growing number of users in jail. This is most prevalent in the Middle East, but it has occurred elsewhere in the world. In Saudi Arabia, any discussion that questions the official interpretation of Islam commonly leads to arrest. Prominent writer Turki al-Hamad was arrested in December 2012 after tweeting that "we need someone to rectify the doctrine of [the prophet] Muhammad;" he was held in detention for five months. In April 2013, a Tunisian court upheld a prison sentence of seven and a half years for a man who published cartoons depicting the prophet Muhammad on his Facebook page. And earlier this year in Bangladesh, several bloggers were charged with "harming religious sentiments" under the country's ICT Act for openly atheist posts that criticized Islam. The

charges carried a prison sentence of up to 10 years, though in August 2013 the law was amended to increase the maximum penalty to 14 years.

Some regimes have also shown very little tolerance for humor that may cast them or the country's religious authorities in a negative light, leading to more arrests and prosecutions. For instance, in June 2012, a popular Turkish composer and pianist was charged with offending Muslims with his posts on Twitter, including one in which he joked about a call to prayer that lasted only 22 seconds, suggesting that the religious authorities had been in a hurry to get back to their drinking and mistresses. He was charged with inciting hatred and insulting "religious values," and received a suspended sentence of 10 months in prison. In another example, in India, a 25-year-old cartoonist was arrested on a charge of sedition—which carries a life sentence—and for violating laws against insulting national honor through his online anticorruption cartoons, one of which depicted the national parliament as a toilet. He was released on bail after the sedition charge was dropped.

Growing activism stalls negative proposals and promotes positive change

Although threats to internet freedom have continued to grow, the study's findings also reveal a significant uptick in citizen activism online. While it has not always produced legislative changes—in fact, negative developments in the past year vastly outnumber positive developments—there is a rising public consciousness about internet freedom and freedom of expression issues. Citizens' groups are able to more rapidly disseminate information about negative proposals and put pressure on the authorities. In addition, ICTs have started to play an important role in advocacy for positive change on other policy topics, from corruption to women's rights, enabling activists and citizens to more effectively organize, lobby, and hold their governments accountable.

This emergent online activism has taken several forms. In 11 countries, negative laws were deterred as a result of civic mobilization and pressure by activists, lawyers, the business sector, reform-minded politicians, and the international community. In the Philippines, after the passage of the restrictive Cybercrime Prevention Act, online protests and campaigns ran for several months. Individuals blacked out their profile pictures on social networks, and 15 petitions were filed with the Supreme Court, which eventually put a restraining order on the law, deeming it inapplicable in practice. In Kyrgyzstan, the government proposed a law on protection of children—modeled on the similar law in Russia—that activists feared would be used as a tool for internet censorship, as it allowed the government to close sites without a court decision. The proposal sparked public outrage, spurring local advocacy efforts that eventually compelled parliament to postpone the bill until it could be amended.

In 11 countries, negative laws were deterred as a result of civic mobilization and pressure by activists, lawyers, the business sector, reform-minded politicians, and the international community.

In a select few countries, civic activists were able to form coalitions and proactively lobby governments to pass laws that protect internet freedom or amend previously restrictive legislation.

In Mexico, for example, following a public campaign by 17 civil society organizations that joined forces in early 2013, freedom of access to the internet in now guaranteed in Article 6 of the constitution. Although the Mexican government has not introduced any secondary legislation that would specify how the new right will be protected in practice, the constitutional amendment is seen as a significant victory. In the United Kingdom, the government passed a law to revise the Defamation Act, discouraging the practice of "libel tourism" and limiting intermediary liability for user-generated content of defamatory nature. Civil society has also been increasingly active on the global stage, lobbying for greater transparency and inclusion in advance of the World Conference on International Telecommunications (WCIT-12) in Dubai, and in some instances placing pressure on their national delegations.

ICTs have also been an important tool for mobilization on issues other than internet freedom, leading to important changes. In Morocco, online activism contributed to a national debate on Article 475 of the penal code, which allows rapists to avoid prosecution if they agree to marry their victims. Although women's rights advocates have been lobbying for years to alter this law, the necessary momentum was created only after a 16-year-old girl committed suicide, having been forced to wed her alleged rapist. Women's rights activists successfully used social media and online news platforms to counter arguments made by state-controlled radio and television outlets, rallying popular support for reforms. In January 2013, the government announced plans to revise the article in question. In other countries—including many authoritarian states like China, Saudi Arabia, and Bahrain—citizen journalists' exposés of corruption, police abuse, pollution, and land grabs forced the authorities to at least acknowledge the problem and in some cases punish the perpetrators.

In addition to activism by groups, citizens, and other stakeholders, the judiciary has played an important role as protector of internet freedom, particularly in more democratic countries where the courts operate with a greater degree of independence. Since May 2012, the courts in at least 9 countries have issued decisions that may have a positive impact on internet freedom. In South Korea, the Constitutional Court overturned a notorious law that required all users to register with their real names when commenting on large websites. In Italy, a court issued a ruling to clarify that blogs cannot be considered illegal "clandestine press" under an outdated law stipulating that anyone providing a news service must be a "chartered" journalist. In practice this rule had led some bloggers and internet users to collaborate with registered journalists when publishing online in order to protect themselves from legal action.

KEY INTERNET CONTROLS BY COUNTRY

Country (By FOTN 2013 ranking)	FOTN 2013 Status (F=Free, PF=Partly Free, NF=Not Free)	Social media and/or communication apps blocked	Political, social, and/or religious content blocked	Localized or nationwide ICT shutdown	Progovernment commentators manipulate online discussions	New law /directive increasing censorship or punishment passed	New law /directive incr. surveillance or restricting anonymity passed	Blogger/ICT user arrested for political or social writings	Blogger/ICT user physically attacked or killed (incl. in custody)	Technical attacks against government critics and human rights orgs
Iceland	F									
Estonia	F									
Germany	F						X			
USA	F									
Australia	F						X			
France	F									
Japan	F					X				
Hungary	F					X			X	
Italy	F									
UK	F									
Philippines	F					X	X			
Georgia	F									
South Africa	F						X			
Argentina	F								X	X
Kenya	F									
Ukraine	F							X	X	X
Armenia	F									X
Nigeria	PF									
Brazil	PF							X	X	
South Korea	PF		X		X					
Angola	PF								X	X
Uganda	PF									X
Kyrgyzstan	PF		X		X				X	
Ecuador	PF				X	X	X		X	X
Mexico	PF				X			X	X	X
Indonesia	PF		X							
Tunisia	PF							X		X
Malawi	PF				X			X		
Morocco	PF				X			X	X	X
Malaysia	PF		X		X			X		X

Country (By FOTN 2013 ranking)	FOTN 2013 Status (F=Free, PF=Partly Free, NF=Not Free)	Social media and/or communication apps blocked	Political, social, and/or religious content blocked	Localized or nationwide ICT shutdown	Progovernment commentators manipulate online discussions	New law /directive increasing censorship or punishment passed	New law /directive incr. surveillance or restricting anonymity passed	Blogger/ICT user arrested for political or social writings	Blogger/ICT user physically attacked or killed (incl. in custody)	Technical attacks against government critics and human rights orgs
Lebanon	PF	X						X	X	X
Libya	PF		X						X	
Jordan	PF					X				X
Cambodia	PF		X							
India	PF	X	X	X	X			X		
Rwanda	PF		X			X				
Bangladesh	PF	X	X			X		X	X	X
Turkey	PF	X	X					X		
Azerbaijan	PF	X	X				X	X		
Venezuela	PF		X	X	X			X	X	X
Russia	PF		X		X	X		X	X	X
Zimbabwe	PF							X		X
Sri Lanka	PF		X			X		X	X	X
Kazakhstan	PF	X	X		X					X
Egypt	PF				X			X	X	X
Thailand	PF		X		X		X			
Burma	NF	X								X
Sudan	NF	X	X		X			X	X	X
UAE	NF	X	X			X		X	X	X
Belarus	NF	X	X		X			X	X	X
Pakistan	NF	X	X	X			X		X	
Saudi Arabia	NF	X	X		X		X	X		X
Bahrain	NF	X	X		X			X	X	X
Vietnam	NF		X		X	X	X	X	X	X
Uzbekistan	NF	X	X		X	X				X
Ethiopia	NF	X	X		X	X		X		X
Syria	NF	X	X	X				X	X	X
China (PRC)	NF	X	X	X	X		X	X	X	X
Cuba	NF	X	X		X	X		X	X	
Iran	NF	X	X					X	X	X
TOTAL		19	29	5	22	14	11	28	26	31

X = Internet control observed during the May 2012 – April 2013 coverage period;
X = Internet control observed after May 1, 2013

KEY INTERNET CONTROLS BY COUNTRY

CHARTS AND GRAPHS OF KEY FINDINGS

Freedom on the Net measures the level of internet and digital media freedom in 60 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of **FREE (0-30 points)**, **PARTLY FREE (31-60 points)**, or **NOT FREE (61-100 points)**.

Ratings are determined through an examination of three broad categories:

A. **OBSTACLES TO ACCESS:** assesses infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; and legal, regulatory, and ownership control over internet and mobile phone access providers.
B. **LIMITS ON CONTENT:** examines filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.
C. **VIOLATIONS OF USER RIGHTS:** measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

FREEDOM ON THE NET 2013: GLOBAL SCORES

COUNTRY	FREEDOM ON THE NET 2013 STATUS	FREEDOM ON THE NET 2013 TOTAL *0-100 Points*	A. SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B. SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C. SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
ICELAND	Free	6	1	1	4
ESTONIA	Free	9	1	3	5
GERMANY	Free	17	4	4	9
UNITED STATES	Free	17	4	1	12
AUSTRALIA	Free	18	2	5	11
FRANCE	Free	20	4	4	12
JAPAN	Free	22	4	7	11
HUNGARY	Free	23	5	8	10
ITALY	Free	23	5	6	12
UNITED KINGDOM	Free	24	2	6	16

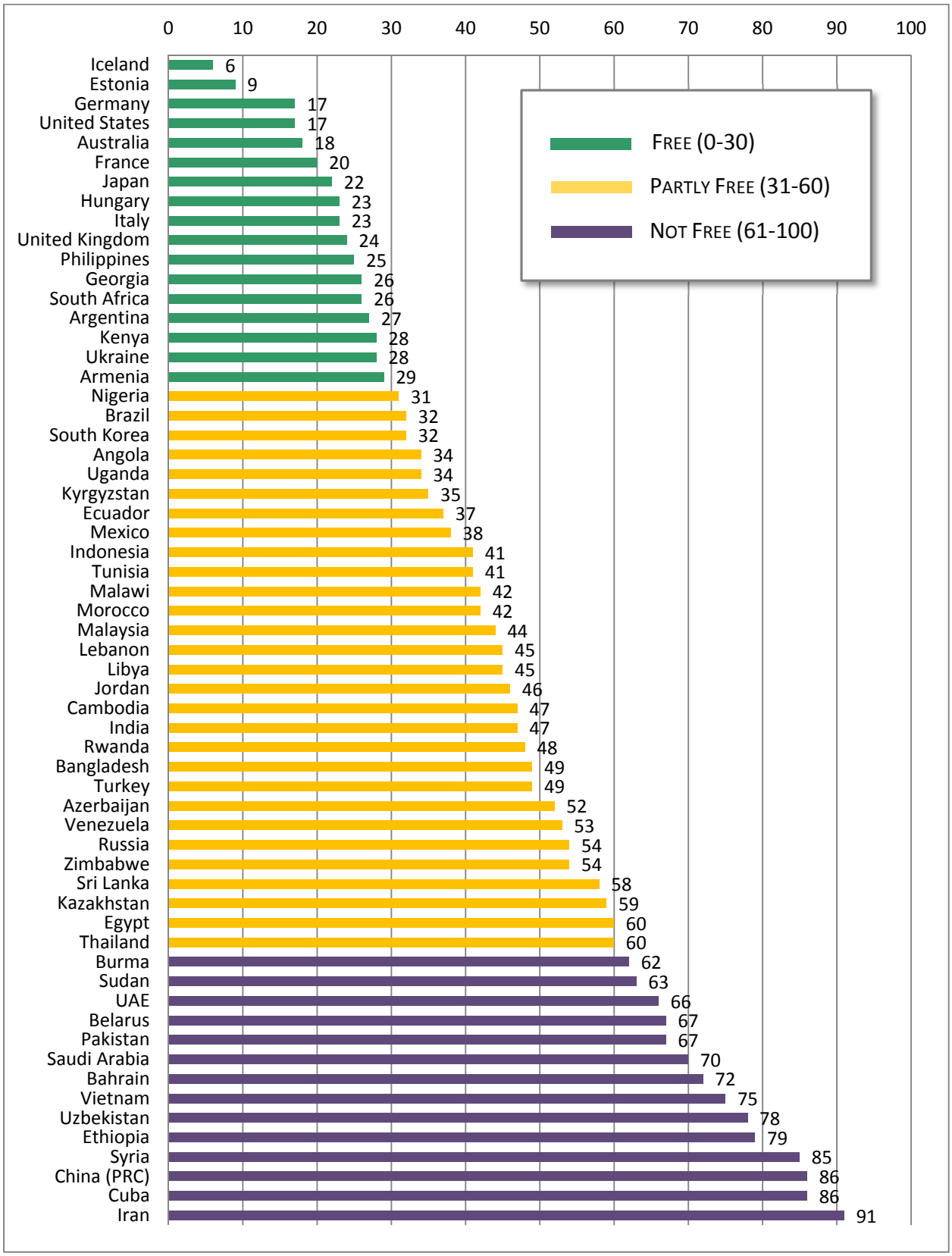
COUNTRY	FREEDOM ON THE NET 2013 STATUS	FREEDOM ON THE NET 2013 TOTAL *0-100 Points*	A. SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B. SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C. SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
PHILIPPINES	Free	25	10	5	10
GEORGIA	Free	26	8	7	11
SOUTH AFRICA	Free	26	7	8	11
ARGENTINA	Free	27	8	10	9
KENYA	Free	28	9	7	12
UKRAINE	Free	28	7	7	14
ARMENIA	Free	29	8	9	12
NIGERIA	Partly Free	31	10	8	13
BRAZIL	Partly Free	32	7	8	17
SOUTH KOREA	Partly Free	32	3	13	16
ANGOLA	Partly Free	34	15	6	13
UGANDA	Partly Free	34	11	8	15
KYRGYZSTAN	Partly Free	35	12	10	13
ECUADOR	Partly Free	37	10	11	16
MEXICO	Partly Free	38	11	10	17
INDONESIA	Partly Free	41	11	11	19
TUNISIA	Partly Free	41	12	8	21
MALAWI	Partly Free	42	16	11	15
MOROCCO	Partly Free	42	11	7	24
MALAYSIA	Partly Free	44	9	15	20
LEBANON	Partly Free	45	14	10	21
LIBYA	Partly Free	45	17	9	19
JORDAN	Partly Free	46	13	13	20
CAMBODIA	Partly Free	47	14	15	18
INDIA	Partly Free	47	15	12	20

CHARTS AND GRAPHS OF KEY FINDINGS

COUNTRY	FREEDOM ON THE NET 2013 STATUS	FREEDOM ON THE NET 2013 TOTAL *0-100 Points*	A. SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B. SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C. SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
RWANDA	Partly Free	48	12	18	18
BANGLADESH	Partly Free	49	13	12	24
TURKEY	Partly Free	49	12	18	19
AZERBAIJAN	Partly Free	52	13	17	22
VENEZUELA	Partly Free	53	16	16	21
RUSSIA	Partly Free	54	10	19	25
ZIMBABWE	Partly Free	54	16	14	24
SRI LANKA	Partly Free	58	15	20	23
KAZAKHSTAN	Partly Free	59	15	23	21
EGYPT	Partly Free	60	15	12	33
THAILAND	Partly Free	60	10	21	29
BURMA	Not Free	62	20	16	26
SUDAN	Not Free	63	17	19	27
UNITED ARAB EMIRATES	Not Free	66	13	22	31
BELARUS	Not Free	67	16	22	29
PAKISTAN	Not Free	67	20	20	27
SAUDI ARABIA	Not Free	70	14	24	32
BAHRAIN	Not Free	72	11	26	35
VIETNAM	Not Free	75	14	28	33
UZBEKISTAN	Not Free	78	20	28	30
ETHIOPIA	Not Free	79	22	28	29
SYRIA	Not Free	85	24	25	36
CHINA (PRC)	Not Free	86	19	29	38
CUBA	Not Free	86	24	29	33
IRAN	Not Free	91	22	32	37

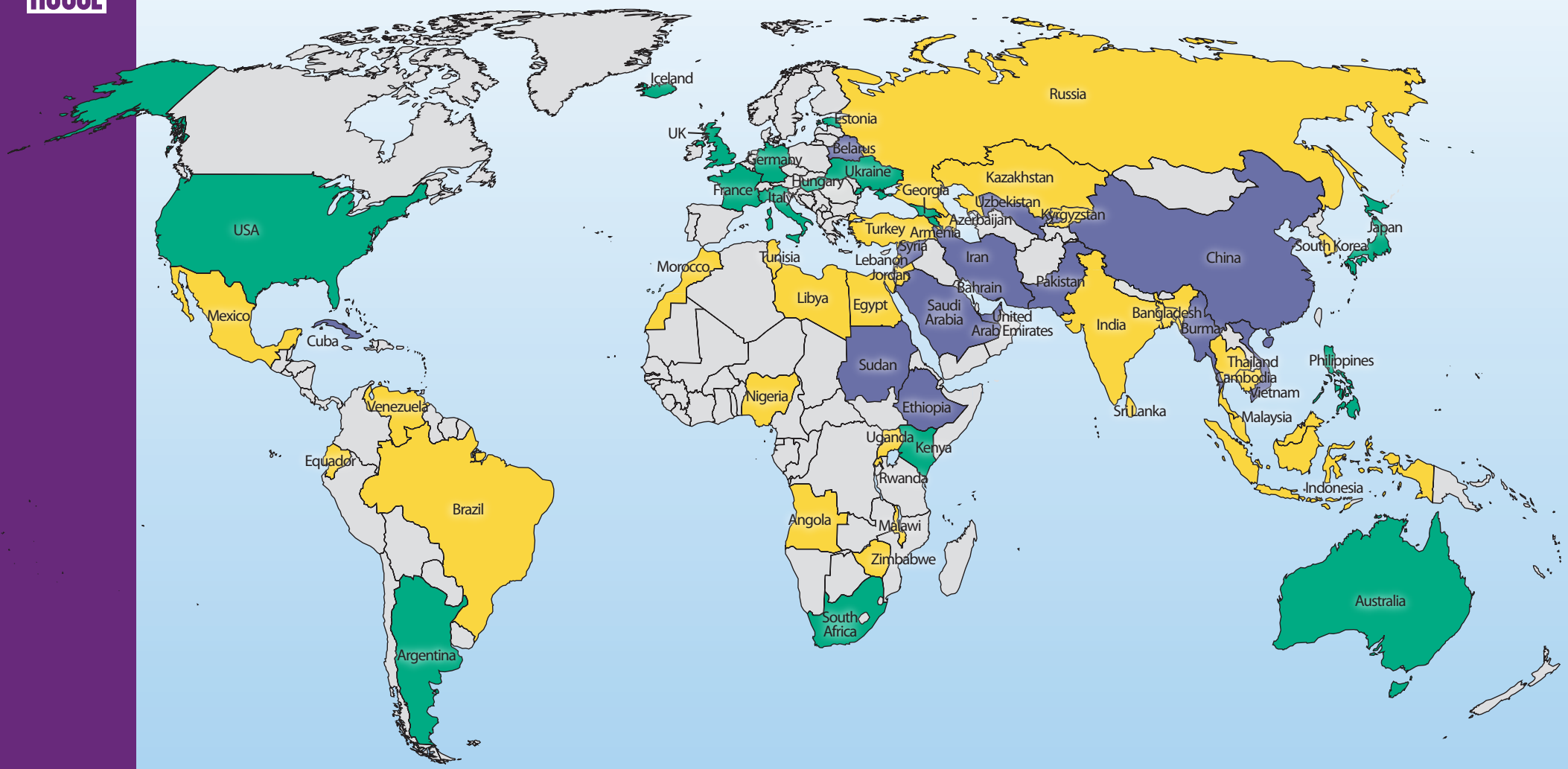
CHARTS AND GRAPHS OF KEY FINDINGS

60 COUNTRY SCORE COMPARISON (0 = Most Free, 100 = Least Free)



Freedom on the Net 2013

A Global Assessment of Internet and Digital Media



FREE

PARTLY FREE

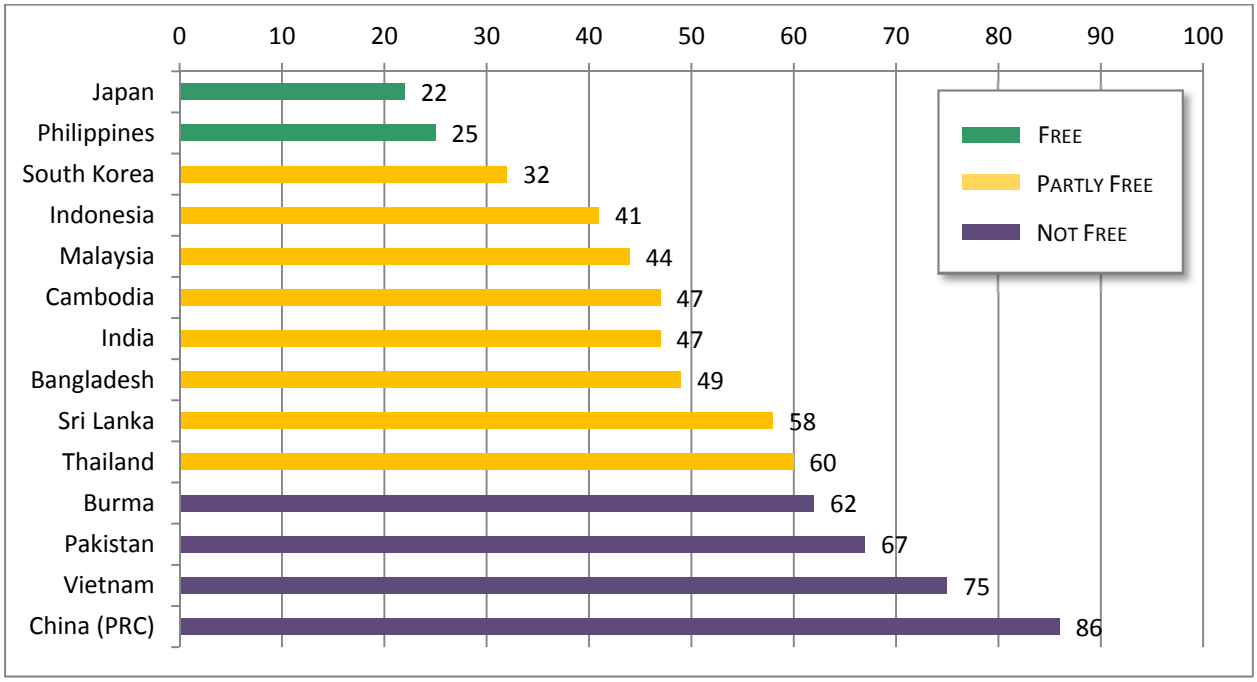
NOT FREE

COUNTRY NOT ASSESSED IN 2013

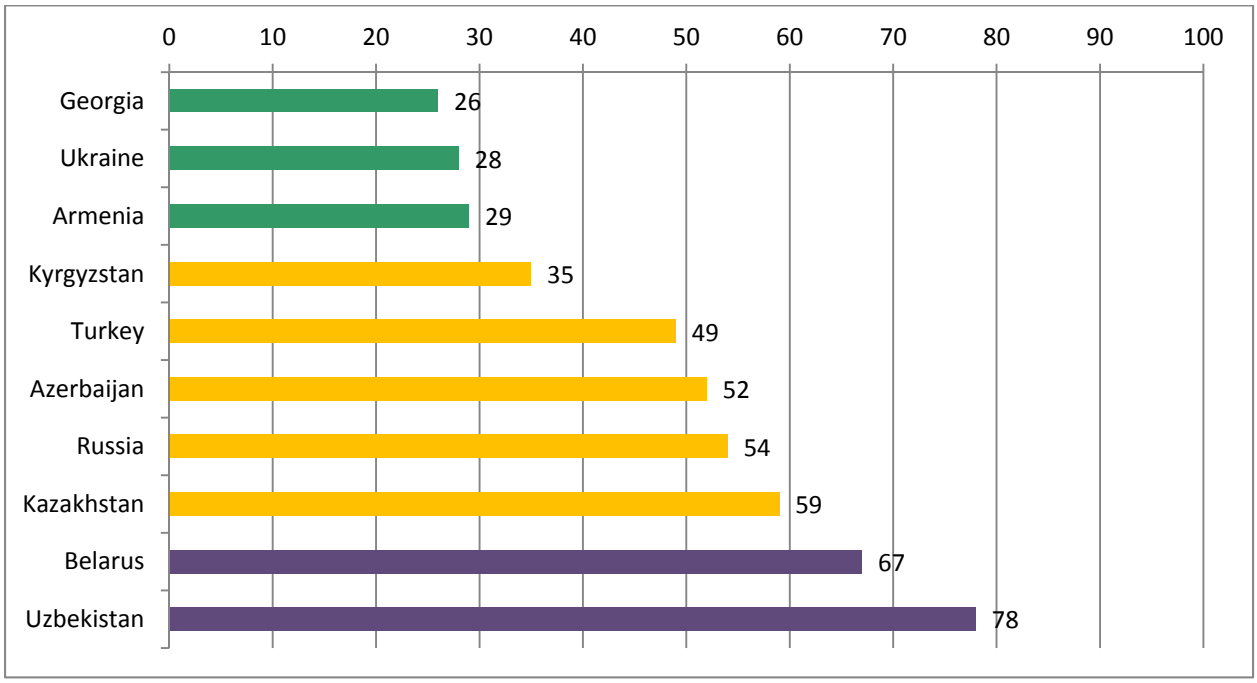
Freedom on the Net 2013 assessed 60 countries around the globe. The project is expected to expand to more countries in the future.

REGIONAL GRAPHS

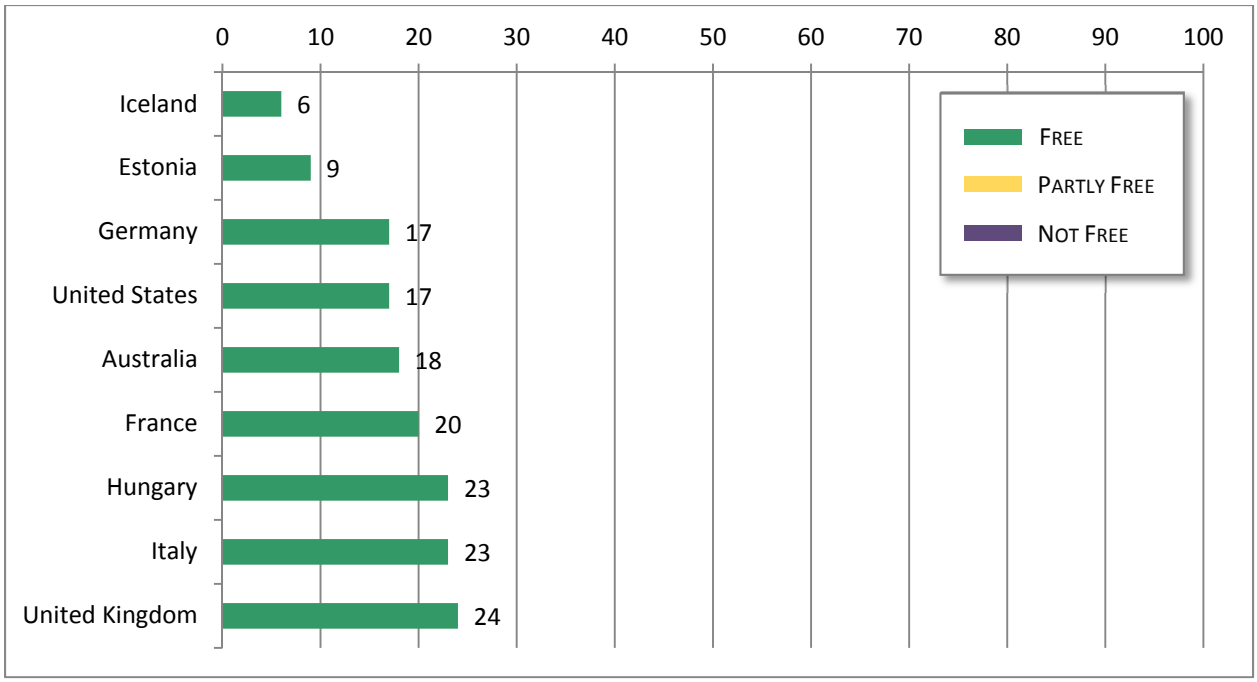
ASIA (0 = Most Free, 100 = Least Free)



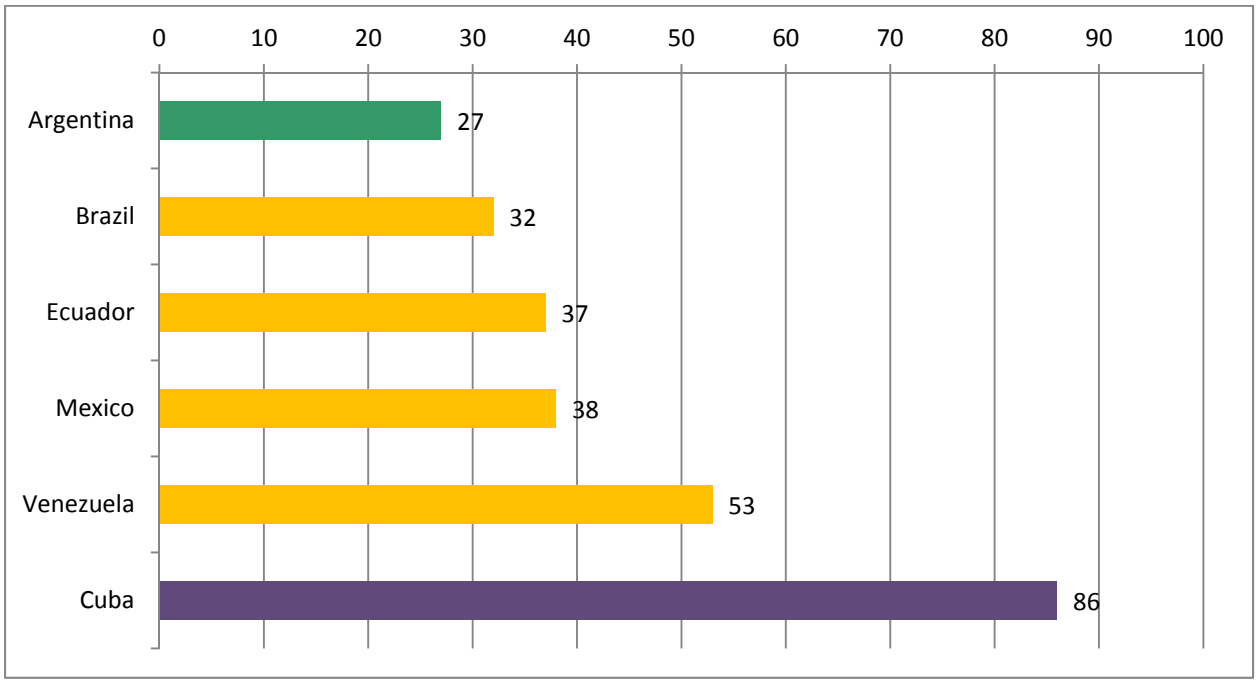
EURASIA (0 = Most Free, 100 = Least Free)



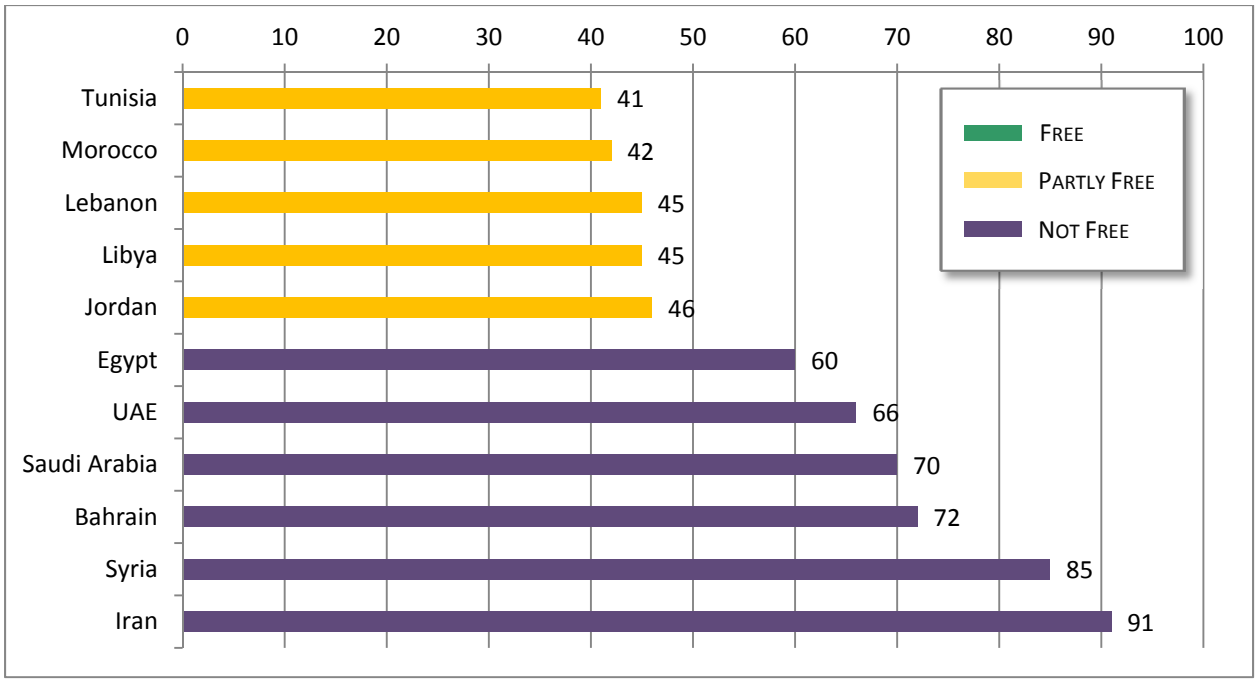
AUSTRALIA , EU, ICELAND & UNITED STATES (0 = Most Free, 100 = Least Free)



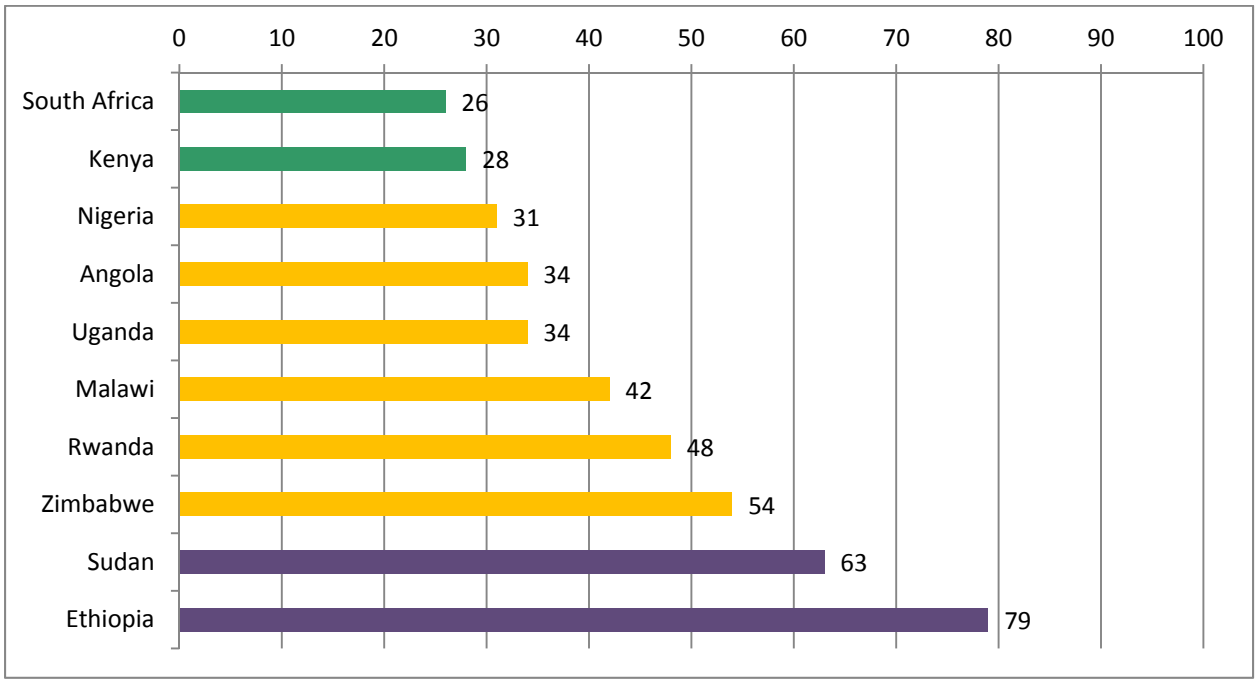
LATIN AMERICA (0 = Most Free, 100 = Least Free)



MIDDLE EAST & NORTH AFRICA (0 = Most Free, 100 = Least Free)

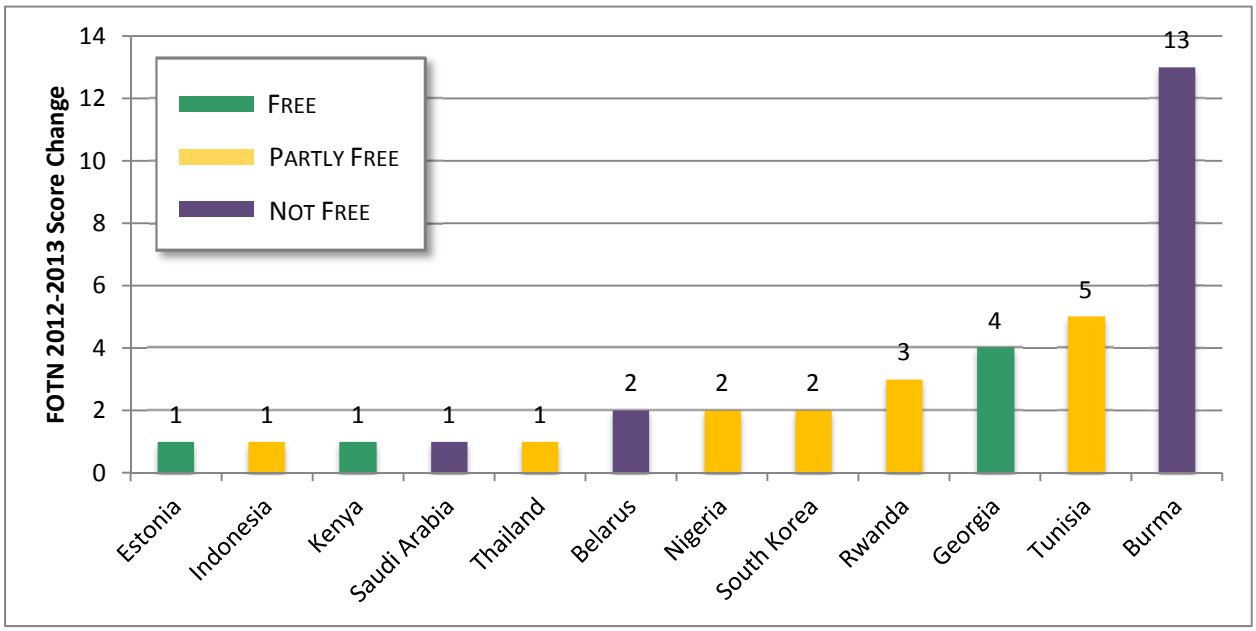


SUB-SAHARAN AFRICA (0 = Most Free, 100 = Least Free)



SCORE CHANGES: FREEDOM ON THE NET 2012 VS. 2013

SCORE IMPROVEMENTS

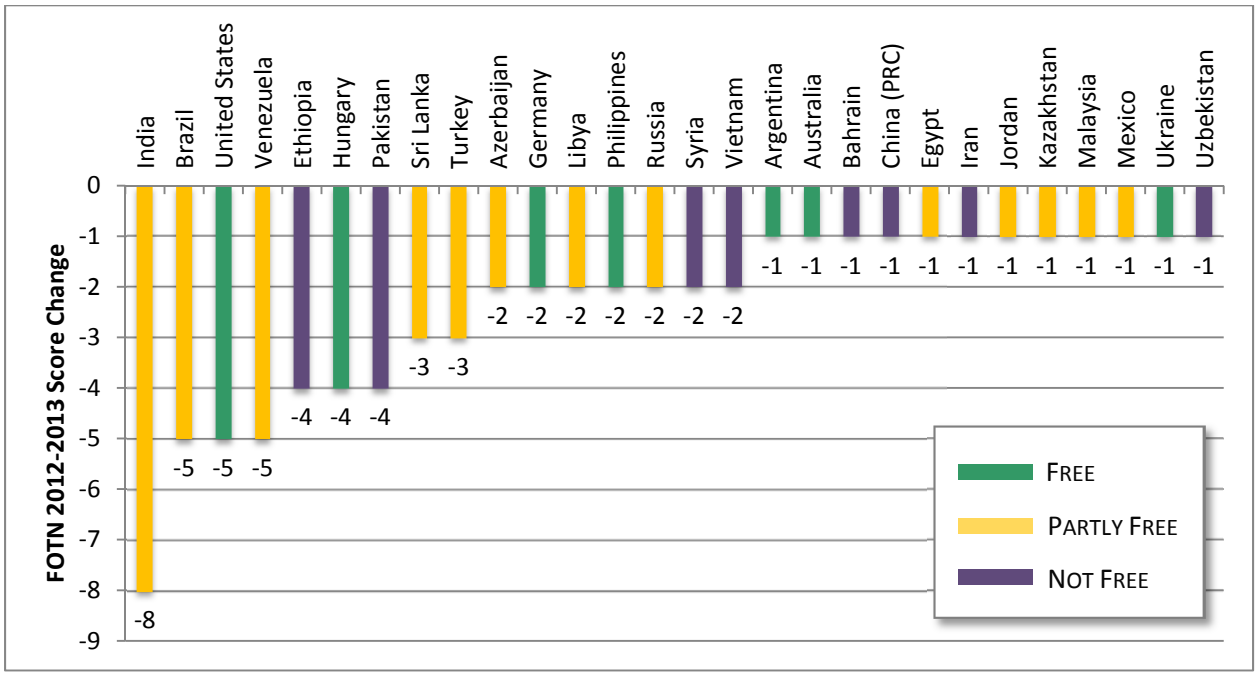


Twelve countries registered positive score changes between the 2012 and 2013 editions of *Freedom on the Net*. In some countries—such as Tunisia and Burma—the improvements reflect government efforts to open up the online sphere. In several countries, however, the improvements registered mainly because of a decrease in the number of negative incidents from the previous coverage period, at times because the authorities had less need to utilize certain types of internet control.

COUNTRY	FOTN 2012	FOTN 2013	TRAJECTORY*	COUNTRY	FOTN 2012	FOTN 2013	TRAJECTORY*
Estonia	10	9	Slight ↑	**Nigeria**	33	31	Slight ↑
Indonesia	42	41	Slight ↑	**South Korea**	34	32	Slight ↑
Kenya	29	28	Slight ↑	**Rwanda**	51	48	Notable ↑
Saudi Arabia	71	70	Slight ↑	**Georgia**	30	26	Notable ↑
Thailand	61	60	Slight ↑	**Tunisia**	46	41	Significant ↑
Belarus	69	67	Slight ↑	**Burma**	75	62	Significant ↑

*A *Freedom on the Net* score decrease represents a positive trajectory (↑) for internet freedom.

Score Declines



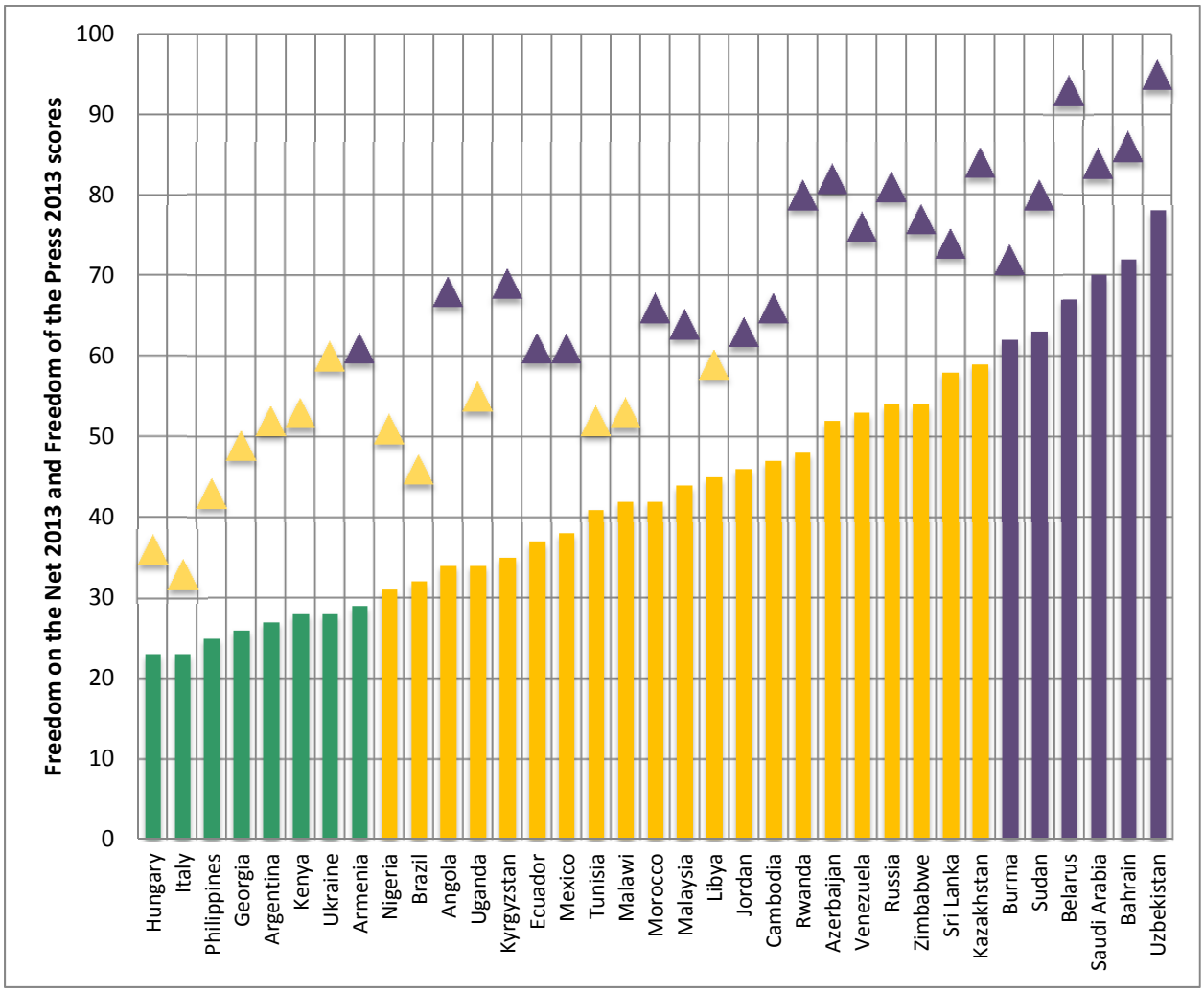
Country	FOTN 2012	FOTN 2013	Trajectory*	Country	FOTN 2012	FOTN 2013	Trajectory*
India	39	47	Significant ↓	Syria	83	85	Slight ↓
Brazil	27	32	Significant ↓	Vietnam	73	75	Slight ↓
United States	12	17	Significant ↓	Argentina	26	27	Slight ↓
Venezuela	48	53	Significant ↓	Australia	17	18	Slight ↓
Ethiopia	75	79	Notable ↓	Bahrain	71	72	Slight ↓
Hungary	19	23	Notable ↓	China (PRC)	85	86	Slight ↓
Pakistan	63	67	Notable ↓	Egypt	59	60	Slight ↓
Sri Lanka	55	58	Notable ↓	Iran	90	91	Slight ↓
Turkey	46	49	Notable ↓	Jordan	45	46	Slight ↓
Azerbaijan	50	52	Slight ↓	Kazakhstan	58	59	Slight ↓
Germany	15	17	Slight ↓	Malaysia	43	44	Slight ↓
Libya	43	45	Slight ↓	Mexico	37	38	Slight ↓
Philippines	23	25	Slight ↓	Ukraine	27	28	Slight ↓
Russia	52	54	Slight ↓	Uzbekistan	77	78	Slight ↓

*A *Freedom on the Net* score increase represents a negative trajectory (↓) for internet freedom.

INTERNET FREEDOM VS. PRESS FREEDOM

Digital media in several of the 60 countries covered was relatively unobstructed when compared to the more repressive or dangerous environment for traditional media. This difference is evident from the comparison between a country's score on Freedom House's *Freedom on the Net 2013* and *Freedom of the Press 2013* assessments.

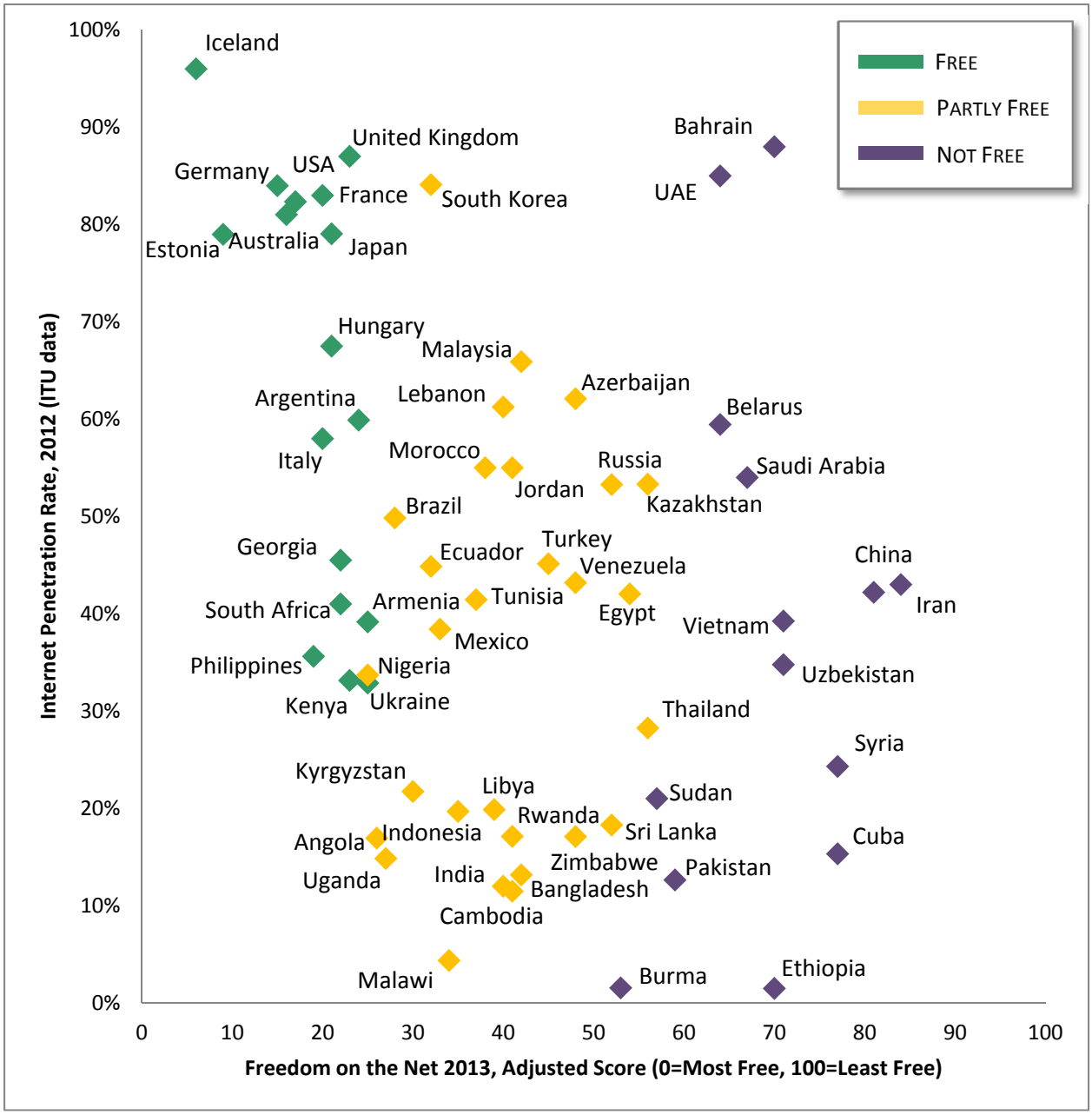
The figure below shows the 35 countries in this edition with a score difference of 10 points or greater. The bar graph characterizes a country's *Freedom on the Net 2013* score, while the scatterplot (▲) represents the country's score in *Freedom of the Press 2013*, which measures media freedom in the broadcast, radio, and print domains. This difference is cause for concern. Pressures that constrain expression in print or broadcast formats have the potential to exert a negative impact, in the short or long term, on the space for online expression.



INTERNET FREEDOM VS. INTERNET PENETRATION

The figure below depicts the relationship between internet penetration rates and the level of digital media freedom in *Freedom on the Net 2013*. Each point reflects a country's internet penetration rate, as well as its overall performance in the rest of the survey.

The PARTLY FREE countries in the middle are particularly noteworthy. As digital access increases, they have a choice—to move right, and join the countries that are high-tech but NOT FREE; or left, with the FREE countries that better protect expression.



FREEDOM ON THE NET 2013: COUNTRY REPORTS

ANGOLA

	2012	2013
INTERNET FREEDOM STATUS	N/A	PARTLY FREE
Obstacles to Access (0-25)	n/a	15
Limits on Content (0-35)	n/a	6
Violations of User Rights (0-40)	n/a	13
Total (0-100)	n/a	34

* 0=most free, 100=least free

POPULATION: 21 million
INTERNET PENETRATION 2012: 17 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Parliamentary elections held in August 2012 saw the innovative and widespread use of digital media tools that aimed to advance electoral transparency (see **LIMITS ON CONTENT**).
- An investigative report conducted by an exile news outlet revealed in April 2013 that the Angolan state security services may be planning to implement an electronic monitoring system that could track e-mail and other digital communications, with assistance from Germany (see **VIOLATIONS OF USER RIGHTS**).
- A journalist for the online radio news outlet, Voice of America, was assaulted in December 2012 for his reporting on human rights issues, political violence, and corruption in Angola. The journalist's e-mail was also hacked (see **VIOLATIONS OF USER RIGHTS**).
- A targeted malware attack was launched against a prominent Angolan writer and blogger in early 2013, purportedly to compromise his communications during an ongoing defamation lawsuit lodged against him (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Since the end of the Angolan Civil War in 2002 that ravaged the country from its start in 1975, access to information and communication technologies (ICTs) has improved dramatically. Throughout the war, the country's telecommunications were run primarily by the state under the ruling People's Movement for the Liberation of Angola–Labour Party (MPLA), with the party's Angola Telecom holding a monopoly of the sector. Toward the end of hostilities in 2001, the government began adopting regulations to liberalize the telecom industry, which enabled private investments to revitalize the country's ICT infrastructure that had been severely damaged by the decades-long conflict. Today, Angola has one of the largest mobile telecom markets in sub-Saharan Africa and internet access is growing steadily.

Despite such improvements that have occurred in tandem with Angola's phenomenal economic growth since 2002,[1] political rights and civil liberties remain tightly controlled and restricted by the MPLA under President Jose Eduardo dos Santos, who has been in power for over 34 years. Recent parliamentary elections in August 2012 led to a highly flawed vote that kept dos Santos in power,[2] in spite of the unprecedented flurry of social media activity and use of innovative digital media tools that endeavored to combat electoral fraud. Nevertheless, such use of ICTs illustrated the empowering ability of the internet and social media for journalists, activists, and opposition parties who are increasingly turning to digital platforms as a means to sidestep the country's longstanding restrictions on traditional media.

While there are no administrative or systematic restrictions on ICT content in Angola, the government has indicated its intent to limit internet freedom through legal measures, such as the alarming draft "Law to Combat Crime in the Area of Information Technologies and Communication" introduced by the National Assembly in March 2011. Often referred to as the cybercrime bill, the draft law was ultimately withdrawn in May 2011 as a result of international pressure and vocal objections from civil society. If enacted, however, the new law would have legally empowered the authorities with the ability intercept information from private devices without a warrant and imposed harsh penalties for objectionable speech expressed via ICTs and on social media platforms, among other restrictions.

In 2012 and early 2013, internet freedom in Angola was limited primarily by increasing violations of user rights. For example, in April 2013, a news report revealed that the Angolan intelligence services may be planning to implement an electronic monitoring system that could track e-mail and other digital communications. Violence against journalists typically experienced within the traditional media sphere seeped into the online sphere in December 2012 when a journalist for the online radio news outlet, Voice of America, was assaulted for his reporting on human rights issues, political violence, and corruption in Angola. Meanwhile, technical attacks against independent and critical news websites, blogs, and opposition voices are common.

[1] Characterized by an average annual GDP growth rate of nearly 12 percent. See, Estefania Jover et al., "Angola, Private Sector Country Profile," African Development Bank, September 2012, http://bit.ly/14Y27HZ.
[2] Freedom House, "Angola," *Freedom in the World 2013*, http://www.freedomhouse.org/report/freedom-world/2013/angola.

OBSTACLES TO ACCESS

Access to ICTs in Angola has improved markedly with increasing investments in the telecommunications sector since the end of the country's civil war in 2002. First introduced in 1996,[3] the internet in Angola reached a penetration rate of 17 percent in 2012, up from just over 3 percent in 2007, according to the International Telecommunications Union (ITU).[4] Fixed-line broadband subscriptions, however, remain low with a penetration rate of only 0.16 percent in 2012,[5] and are largely concentrated in the capital city, Luanda, due to the country's high poverty rate and poor infrastructure in rural areas. By contrast, access to mobile phones is much higher with a penetration rate of 49 percent in 2012.[6]

In addition to infrastructural limitations and widespread poverty characterized by more than 36 percent of Angolans living on less than $2 a day,[7] access to ICTs is further hindered by the country's fractured electricity system that serves only 30 percent of the population. In rural areas, where more than 58 percent of the poor population lives,[8] less than 10 percent have regular access to electricity.[9] Consequently, radio, television, and print outlets—which are subject to high levels of government interference—remain the primary sources of information for the majority of Angolans.

Luanda is reputed to be the second most expensive city in the world,[10] and for those able to access the internet in urban areas, internet subscriptions start at $50 per month but can cost as high as $100 per month for connections via satellite or WiMax. Unlimited internet subscriptions cost an average of $140, while USB dongle devices that provide wireless access cost between $50 and $60. Mobile internet packages come at a monthly cost of about $45.[11] Already expensive for the vast majority of Angolans, voice and data services in rural areas can be twice as expensive and of much poorer quality, subject to frequent cuts and extremely slow connection speeds. According to the ITU, Angola's mobile-cellular sub-basket of prices at purchasing power parity (PPP)—which "expresses the price of goods in terms of buying power and adjusts exchange rates to facilitate

[3] Silvio Cabral Almada and Haymee Perez Cogle, "Internet Development in Angola, Our contribution," Network Startup Resource Center, http://nsrc.org/AFRICA/AO/20060300-Internet-Development-in-Angola.pdf.
[4] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[5] International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2012."
[6] International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2012."
[7] "Angola," African Economic Outlook, 2013, http://www.africaneconomicoutlook.org/fileadmin/uploads/aeo/2013/PDF/Angola%20-%20African%20Economic%20Outlook.pdf.
[8] "Angola," African Economic Outlook, 2013.
[9] "Angola," U.S. Energy Information Administration, last revised January 8, 2013, http://www.eia.gov/countries/analysisbriefs/Angola/angola.pdf.
[10] Ami Sedghi, "Which is the World's Most Expensive City? Cost of living survey 2012," *Guardian,* June 12, 2012, http://www.theguardian.com/news/datablog/2012/jun/12/city-cost-of-living-2012-tokyo.
[11] Interview with a source based in Angola.

international comparisons"—was $28 in 2011, while the fixed-broadband sub-basket at PPP was $74.[12] Due to these high prices, most internet users log online at their workplaces.

Angola's domestic backbone is currently comprised of microwave, VSAT, and fiber-optic cables, while the government's Master Plan for ICT development envisions connecting the country's 18 provinces through a national fiber optic-backbone. Connection to the international internet goes through the South Atlantic 3 (SAT-3) cable, over which the state-owned Angola Telecom has a monopoly. Angola is also looking to connect to the Africa Coast to Europe (ACE) cable and the West Africa Cable System (WACS) in the future, in addition to establishing a submarine cable between Northeastern Brazil and Luanda to reduce the bandwidth costs associated with the distance that internet traffic currently has to travel from Europe and the United States.[13]

According to the telecoms regulator, the Angolan National Institute of Telecommunication (INACOM), there are currently five fixed-line operators in Angola—the state-owned Angola Telecom, Mercury (owned by the state-owned petroleum company, Sonangol), Nexus, Mundo Startel, and Wezacom—while Angola Telecom's Multitel and a number of smaller private ISPs provide internet services.

Mobile services are provided by two private operators—Movicel and Unitel.[14] Portugal Telecom and state-owned Sonangol each have a 25 percent stake in Unitel. Investigative reports have revealed that the president's daughter, Isabel Dos Santos, also holds a 25 percent stake in Unitel, in addition to sitting on the telecom provider's board.[15] Meanwhile, as of 2009, 80 percent of Movicel is split between four private Angolan companies—Portmill Investimentos e Telecomunicações (with 40 percent), Modus Comunicare (19 percent), Ipang–Indústria de Papel e Derivados (10 percent), Lambda (6 percent), and Novatel (5 percent)—while the remainder of Movicel's capital is held by two state enterprises, Angola Telecom and Empresa Nacional de Correios e Telégrafos de Angola, with 18 percent and 2 percent, respectively.[16]

An ITU profile of the Angolan ICT sector characterizes competition in the international gateway, wireless local loop, and fixed-wired broadband markets as monopolistic; by contrast, it describes the markets for mobile, internet, and DSL services as competitive.[17] Based on research conducted by an independent analyst, however, no real competition exists in the provision of mobile and internet services as most of the companies have shares belonging to senior government officials.[18]

---

[12] International Telecommunication Union, "Measuring the Information Society," 2012, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf.
[13] Estefania Jover et al., "Angola, Private Sector Country Profile."
[14] Intituto Angolano das Comunicacoes "Sector Telecom," accessed August 30, 2013, http://www.inacom.og.ao/Inacom_home_page.htm.
[15] Kerry A. Dolan, "Isabel Dos Santos, Daughter Of Angola's President, Is Africa's First Woman Billionaire," *Forbes*, January 23, 2013, http://www.forbes.com/sites/kerryadolan/2013/01/23/isabel-dos-santos-daughter-of-angolas-president-is-africas-first-woman-billionaire/.
[16] Rafael Marques de Morais, "The Angolan Presidency: The Epicentre of Corruption," *Maka Angola* (blog), accessed August 30, 2013, https://wikileaks.org/gifiles/attach/169/169476_Ao100805.pdf.
[17] International Telecommunication Union, "Angola Profile (Latest data available: 2012)," ICT Eye, accessed August 30, 2013, http://www.itu.int/net4/itu-d/icteye/CountryProfile.aspx.
[18] Rafael Marques de Morais, "The Angolan Presidency: The Epicentre of Corruption."

Similar to other countries in sub-Saharan Africa, China has emerged as a key investor and contractor in Angola's telecommunications sector. In 2008, the Angolan government contracted the Chinese telecom ZTE to head the operations of the previously state-owned Movicel,[19] which makes the country's second largest mobile network highly vulnerable to government interception and interference without oversight, particularly given China's own reputation for such ICT abuses.[20] Other research accounts report that ZTE has been involved with assisting with the Angolan military's telecommunication,[21] though in what capacity is unknown. More recently in March 2012, ZTE and Huawei, another major Chinese telecom, were both contracted to develop 4G and LTE networks for Movicel.[22]

Meanwhile in June 2012, the country's other private mobile operator, Unitel, launched a project in partnership with the education ministry and Huawei to provide free access to the internet for secondary school students in both public and private schools across the country's 18 provinces. Known as "E-Net," the project aims to benefit over 18,000 students with computers supplied by Huawei and internet access provided by Unitel.[23]

The Ministry of Post and Telecommunications (MCT) is responsible for oversight of the ICT sector, while the Angolan Institute for Communications (INACOM), established in 1999, serves as the sector's regulatory body. Reporting to the MCT, INACOM determines the sector's regulations and policies, sets prices for telecommunications services, and issues licenses. The regulatory body was set up as an independent public institution with both financial and administrative autonomy from the ministry,[24] though in practice, it has a limited measure of autonomy. According to reports by the ITU and the World Bank, INACOM is not autonomous in its decision making process,[25] in part due to the ministerial appointment of the director general who can be dismissed for any reason. In addition, the MCT has been known to influence staff appointments, while other ministries are often involved in sector policy, leading to politically influenced regulatory decisions.[26]

---

[19] "Angola: China's ZTE Takes on Operational Management of Movicel," *Macauhub*, October 30, 2008, http://www.macauhub.com.mo/en/2008/10/30/5992/.
[20] John Reed, "Africa's Big Brother lives in Beijing," *Foreign Policy*, July 30, 2013, http://www.foreignpolicy.com/articles/2013/07/30/africas_big_brother_lives_in_beijing_huawei_china_surveillance.
[21] Roselyn Hseuh and Michael Byron Nelson, "Who Wins? China Wires Africa: The Cases of Angola and Nigeria," paper prepared for presentation at NYU/Giessen Development Finance Conference, NYU School of Law, April 9, 2013, http://iilj.org/newsandevents/documents/hsueh.pdf.
[22] Michael Malakata, "Angola's Movicel launches LTE," *Computer World Zambia*, April 23, 2012, http://www.pcadvisor.co.uk/news/network-wifi/3353225/angolas-movicel-launches-lte/; Egon Cossou, "High-speed Internet: Angola's big 4G leap," *Africa Review*, May 1, 2012, http://www.africareview.com/Business+++Finance/Angolas+big+4G+leap/-/979184/1397314/-/bnmay/-/index.html.
[23] "MED, Unitel Design Internet Access Project," ANGOP, June 7, 2012, http://bit.ly/17juscJ.
[24] Russell Southwood, "The Case for 'Open Access' Communications Infrastructure in Africa: The SAT-3/WASC cable – Angola case study," Association for Progressive Communications, accessed August 30, 2013, http://www.apc.org/en/system/files/APC_SAT3Angola_20080523.pdf: 5.
[25] International Telecommunication Union, "Angola Profile."
[26] "Private Solutions for Infrastructure in Angola: A Country Framework Report," Public-Private Infrastructure Advisory Facility and the World Bank Group, 2005, http://www.ppiaf.org/sites/ppiaf.org/files/publication/Angola-CFR.pdf: 92.

LIMITS ON CONTENT

To date, there have been no known incidents of the government blocking or filtering ICT content in Angola, and there are no restrictions on the type of information that can be exchanged through digital media technologies, aside from child pornography and copyrighted material.[27] Social media and communications apps such as YouTube, Facebook, Twitter and international blog-hosting services are freely available. In addition, there have been no reported issues of intermediary liability for service or content providers, nor have there been known instances of take-down notices issued for the removal of online content. Nevertheless, according to an independent analyst, the government has been known to deliberately take down its own content when the authorities have wanted to prevent the public from accessing certain government information, such as specific laws.[28]

While there has been no evidence of government efforts to interfere with or manipulate online content, censorship of news and information in the traditional media sphere is common, leading to worries that similar efforts to control the information landscape will eventually affect the internet. The president and members of the ruling MPLA party own and tightly control the most of the country's media outlets, including those that are the most widely disseminated and accessed. Of the dozen or so privately owned newspapers, most are held by individuals connected to the government.

Self-censorship is commonly practiced by journalists in both state-run and private print outlets. As a result of the limited space for Angola's independent voices in the traditional media, many writers and readers are increasingly distributing and reading news online.[29] In addition, journalists, bloggers, and internet users have been generally less fearful expressing themselves and discussing controversial topics online than they might be offline. There is more open criticism of the president and ruling party circulating on blogs and social media platforms,[30] though taboo topics related to land grabs, police brutality, and demolitions are often avoided.

Due to the concentration of internet access and use in urban areas and the limited space for critical voices in Angola's general media sphere, the online information landscape is still lacking in diversity and unable to represent a variety of groups and viewpoints throughout the country. Independent news outlets critical of the government do exist, with *Folha8* and *Agora* being the most prominent, though their audiences are reached primarily through their print publications. Moreover, the economic viability of independent outlets, both online and print, is constrained by the lack of

[27] "Angola, Country Profile," Global Resource & Information Directory, last updated July 16, 2012, http://www.fosigrid.org/africa/angola.
[28] Interview with a Freedom House consultant.
[29] Danny O'Brien, "Using Internet 'Crime' Laws, Authorities Ensnare Journalists," *Attacks on the Press in 2011*, (New York: Committee to Project Journalists, February 2012), http://cpj.org/2012/02/attacks-on-the-press-in-2011-regulating-the-intern.php.
[30] Louise Redvers, "Angola Victory for Cyber Activists?" BBC News, May 27, 2011, http://www.bbc.co.uk/news/world-africa-13569129.

advertising revenue from both state and private sources, since it is often denied to news outlets that publish critical stories.[31]

In recent years, citizens have increasingly taken to the internet as a platform for political debate, to express discontent with the country's current state of affairs, and to launch digital activism initiatives. Similar to many other African countries, the Angolan youth have embraced social media tools and used them to fuel protest movements across the country.[32] The positive impact of digital media tools in Angola was particularly pronounced during the August 2012 parliamentary elections when ICTs were used in innovative ways to advance electoral transparency. For example, citizens were able to report electoral irregularities in real time on the monitoring website Eleições Angola 2012,[33] while the National Electoral Commission used the internet and iPads to scan voter registration cards.[34] A Gallup poll cited by the African Media Initiative found that the internet and smartphones had eroded the government's control over news and information, with only 16 percent of polled Angolans giving the president a thumbs-up rating.[35] Nevertheless, the president's ruling MPLA party still swept the elections with over 70 percent of votes.[36]

VIOLATIONS OF USER RIGHTS

In the past year, concerns over state surveillance of ICTs increased when an investigative news report published in April 2013 said that the Angolan intelligence services were planning to implement an electronic monitoring system that could track e-mail and other digital communications, with equipment and expertize from Germany. One case of violence against a journalist for the online news radio site, Voice of America, was assaulted for his critical reporting, while the prominent writer and blogger Rafael Marques de Morais had his personal computer attacked with malware in a purported attempt to compromise his communications during an ongoing defamation lawsuit lodged against him in early 2013.

The Angolan constitution provides for freedom of expression and the press, and in 2006, Angola became one of the first African countries to enact a freedom of information law. In practice, however, accessing government information remains extremely difficult. The judiciary is subject to considerable political influence, with Supreme Court justices appointed to life terms by the president and without legislative oversight; nevertheless, the courts have been known to rule against the government on occasion, including most recently in May 2012 when the court rejected

[31] Freedom House, "Angola," *Freedom of the Press 2013*, http://www.freedomhouse.org/report/freedom-press/2013/angola.
[32] Sara Moreira, "Year of Change in Angola, But Everything Stays the Same," *Global Voices*, December 29, 2012, http://globalvoicesonline.org/2012/12/29/angola-2012-year-of-change-everything-stays-the-same/.
[33] Eleições Angola 2012: http://eleicoesangola2012.com/
[34] "Angolans Vote in Booths Armed with iPads," *news24*, August 31, 2012, http://www.news24.com/Africa/News/Angolans-vote-in-booths-armed-with-iPads-20120831.
[35] African Media Ini., Twitter post, August 31, 2012, 7:21am, https://twitter.com/African_Media/status/241480901308063744.
[36] "Angola's Ruling Party Declared Election Winner," CNN, September 3, 2012, http://www.cnn.com/2012/09/02/world/africa/angola-elections.

the appointment of the MPLA-favored candidate to head the National Electoral Commission in advance of the August parliamentary elections.[37]

Meanwhile, stringent laws regarding state security and insult run counter to constitutional guarantees and hamper media freedom, such as the Article 26 state security law passed in 2010 known as that allows for the detention of individuals who insult the country or president in "public meetings or by disseminating words, images, writings, or sound."[38] Politicians, on the other hand, are immune. Defamation and libel are crimes punishable by imprisonment. In recent years, a number of journalists in the traditional media sphere have been prosecuted for criminal defamation in lawsuits initiated by government officials,[39] though such actions have not been taken against online journalists or internet users as of yet.

In August 2011, a new Law on Electronic Communications and Services of the Information Society was enacted, which delineated citizens' rights to privacy and security online, among other provisions related to regulating the telecommunications sector.[40] Despite these acknowledgments, the Angolan government has become increasingly keen on limiting internet freedom through legal measures, as indicated by the alarming Law to Combat Crime in the Area of Information Technologies and Communication introduced by the National Assembly in March 2011. Often referred to as the cybercrime bill, the law was ultimately withdrawn in May 2011 as a result of international pressure and vocal objections from civil society. The new law aimed to limit freedom of expression more harshly online than offline by increasing penalties prescribed for offenses laid out under Angola's criminal code committed through electronic media. For example, Article 16 of the cybercrime bill increased the penalty for defamation, libel, and slander conducted online over the penalty defined in the criminal code by a third.[41]

If passed, the law also would have empowered the authorities with the ability to intercept information from private devices without a warrant[42] and prosecute individuals for objectionable speech expressed using electronic media tools and on social media platforms. Sending an electronic message interpreted as an effort to "endanger the integrity of national independence or to destroy or influence the functionality of state institutions" would have yielded a penalty of two to eight years in prisons, in addition to fines. The law would have further criminalized the dissemination of any "recordings, pictures and video" of an individual without the subject's consent,[43] even if produced lawfully, which could have impeded journalists' ability to report on public protests or

[37] "Angola Court Removes 'MPLA' Election Head Susana Ingles," BBC News, May 18, 2012, http://www.bbc.co.uk/news/world-africa-18117413.
[38] "Angola: Revise New Security Law, Free Prisoners in Cabinda," Human Rights Watch, December 9, 2010, http://www.hrw.org/news/2010/12/08/angola-revise-new-security-law-free-prisoners-cabinda.
[39] "Angola: Defamation Laws Silence Journalists," Human Rights Watch, August 12, 2013, http://www.hrw.org/news/2013/08/12/angola-defamation-laws-silence-journalists.
[40] AVM Advogados, "News from Angola," newsletter, August 2011, http://www.avm-advogados.com/newsletter/2011.08/2011-08_avm-newsletter_eng.html#NFA-01.
[41] "Angola: Withdraw Cybercrime Bill," Human Rights Watch, May 13, 2011, http://www.hrw.org/news/2011/05/13/angola-withdraw-cybercrime-bill.
[42] "Angola Clamps Down on Internet, Social Media," *Journalism*, April 15, 2011, http://www.journalism.co.za/index.php/news-and-insight/news130/165-media-freedom1/4034-angola-clamps-down-on-internet-social-media.html.
[43] Committee to Protect Journalists, "Angola," *Attacks on the Press in 2011*, February 2012, http://cpj.org/2012/02/attacks-on-the-press-in-2011-angola.php.

instances of police brutality using digital tools. The bill additionally prescribed penalties between 8 and 12 years in prison for espionage and whistle blowing activities, which would have included the act of seeking access to classified information on an electronic system "in order to reveal such information or to help others to do so." The same penalty was provided for accessing unclassified information that could be deemed as endangering state security.[44]

In an unexpected move, the Angolan government in May 2011 decided to remove the proposed cybercrime legislation from parliament moments before it was due to be voted into law, in large part as a result of widespread opposition and pressure from civil society.[45] However, a government minister publicly stated the same year that special clauses regarding cybercrimes would instead be incorporated into an ongoing revision of the penal code, leaving open the possibility of internet-specific restrictions coming into force in future.

There are no restrictions on anonymous communication such as website or SIM card registration requirements, and to date, there is little evidence that the state illegally monitors and intercepts the electronic communications of its citizens. Nevertheless, an investigative report conducted by the exile news and information outlet *Club-K* revealed in April 2013 that intelligence and state security services were planning to implement an electronic monitoring system that could track e-mail and other digital communications. According to *Club-K*, the sophisticated monitoring equipment was imported from Germany and included German technicians who assisted in the system's installation on a military base in Cape Ledo.[46] The details of *Club-K's* findings could not be corroborated as of August 2013.

Meanwhile, there is no concrete evidence of whether or to what extent ICT service providers are required to assist the government in monitoring the communications of their users, though the strong presence of the state in the ownership structure of Angola's telecoms, particularly of mobile phone operators, suggests that the authorities are likely able to wield their influence over service providers if desired. Cybercafes, however, are not known to be subject to such requirements.

Attacks and extralegal violence against journalists in the traditional media sphere are unfortunately common in Angola,[47] and these actions may become more common against online journalists and social media users as the internet increasingly becomes an empowering tool for citizens to vocalize discontent and mobilize against the government. One case of violence against Antonio Capalandanda, a journalist for the online news and radio site Voice of America, was reported in May 2012, when the journalist was approached by an individual who identified himself as a state security agent and threatened to harm Capalandanda if he continued to report on topics the

[44] "Angola: Withdraw Cybercrime Bill," Human Rights Watch.
[45] Louise Redvers, "Angola Victory for Cyber Activists?"
[46] "Alemães montam sistema de escuta em Angola" [Germans assemble listening system in Angola], *Club-K*, April 23, 2012, http://www.club-k.net/index.php?option=com_content&view=article&id=14932:alemaes-montam-sistema-de-escuta-em-angola&catid=11:foco-do-dia&Itemid=130.
[47] According to the Committee to Protect Journalists, at least 10 journalists have been killed in Angola since 1992. See, "10 Journalists Killed in Angola since 1992/Motive Confirmed", Committee to Protect Journalists, accessed August 2013, http://www.cpj.org/killed/africa/angola/. ; "Angola: Stop Stifling Free Speech," Human Rights Watch, August 1, 2012, http://www.hrw.org/news/2012/08/01/angola-stop-stifling-free-speech.

government deemed objectionable. Known for his reporting on human rights issues, political violence, and corruption in Angola, Capalandanda was later assaulted in December 2012 by two unidentified assailants who also stole his camera, voice recorder, and notepads. In January 2013, Capalandanda's e-mail account was hacked by an unknown entity.[48]

Independent and exile news websites have also been subject to technical violence such as hacking and denial-of-service (DDoS) attacks, particularly during periods of political contestation. For example, at the height of anti-government protests in February 2011, the website of the independent outlet *Club-K* was met with frequent interruptions to the point of temporary disablement. The popular blog *Maka Angola*, produced by the renowned critical writer Rafael Marques de Morais, was also subject to a number of targeted DDoS attacks in 2011.[49] More recently in early 2013, Morais's personal computer was attacked with customized malware, purportedly to compromise his communications during an ongoing defamation lawsuit lodged against him for his 2011 book, *Blood Diamonds: Corruption and Torture in Angola*.[50]

[48] "Angola: Continued Threats, Acts of Intimidation and Surveillance of Journalist Mr Antonio Capalandanda," Frontline Defenders, January 8, 2013, http://www.frontlinedefenders.org/node/21235.
[49] Candido Teixeira, "So This is Democracy, 2011 – National Overview Angola 2011," Media Institute of Southern Africa, 2011, http://www.misa.org/downloads/2011/Angola_STID2011.pdf.
[50] "Angola: Defamation Laws Silence Journalists," Human Rights Watch.

ARGENTINA

	2012	2013
INTERNET FREEDOM STATUS	**FREE**	**FREE**
Obstacles to Access (0-25)	9	8
Limits on Content (0-35)	9	10
Violations of User Rights (0-40)	8	9
Total (0-100)	**26**	**27**

* 0=most free, 100=least free

POPULATION: 40.8 million
INTERNET PENETRATION 2012: 60 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Cases of intermediary liability were on the rise in 2012 and early 2013, with companies such as Google and Yahoo facing take down requests and facing fines should they choose not to comply with court orders (see **LIMITS ON CONTENT**).
- Argentines utilized social media to mobilize thousands of people for 8N, the largest an antigovernment protest movement in Argentina in over a decade, which took issue with corruption, violent crime, and inflation (see **LIMITS ON CONTENT**).
- In November 2012, a pilot cybercrimes unit was created to combat rising incidents of hacking in Argentina (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Although it has been the focus of academic study since the 1980s, the internet was first used for commercial purposes in Argentina in 1991.[1] Internet penetration has steadily increased since, and Argentina is now home to one of the largest contingents of internet users in South America. In 2009, access began accelerating, due in part to government policies aimed at improving services and expanding broadband connections throughout the country.

Argentina has an active legal environment, especially regarding free speech and the internet. The country's legal framework has generally protected online freedom of expression and Argentines have free access to a wide array of online information. During 2012, multiple legal initiatives were presented in Congress regarding matters of intermediary liability, internet neutrality, and network surveillance.

Several court judgments between 2010 and 2013 restricted access to websites on claims of defamation or intellectual property rights violations, with one ruling leading to the accidental blocking of an entire blog-hosting platform. A series of injunctions against search engines in 2012 also imposed intermediary liability and forced companies to delete links from results presented to users. Although some of these rulings threaten internet freedom, due process was generally followed in each case and parties were given the chance to appear before the court to dispute the charges filed against them.

The majority of injunctions filed in 2012 were brought by celebrities regarding content they deemed damaging to their reputations. Although some intermediaries were subsequently ordered to remove links and those individuals who posted the questionable material were ordered to provide plaintiffs with monetary compensation, the Court of Appeals overturned some of these rulings after receiving criticism from freedom of expression advocates as well as international technology companies.[2] In 2012, Argentina also witnessed several instances of retaliation against online journalists, including violence, breaches of privacy, and the exposure of bloggers' personal information.

During the December 2012 World Conference on International Communications,[3] Argentina signed the International Telecommunications Regulations a "binding global treaty designed to facilitate international interconnection and interoperability of information and communication

[1] Jorge Amodio, "*Historia y Evolución de Internet en Argentina*" [History and Evolution of the Internet in Argentina], *Internet Argentina* (blog), May 16, 2010, http://blog.internet-argentina.net/p/indice.html.

[2] The BLUVOL case is particularly relevant. Following a decision regarding defamatory content posted as a comment in a blog hosted on blogspot, a Buenos Aires Court of Appeal ordered Google to pay 10,000 Argentine pesos (US$ 2,300) plus court costs for damages suffered by the claimant. For case details, see: http://www.diariojudicial.com.ar/documentos/2013-Marzo/Bluvol_c_Googlex_daxos_por_blog.doc

[3] The landmark WCIT conference was convened by ITU in Dubai in December 2012. See: ITU, World Conference on International Telecommunications (WCIT-12): http://www.itu.int/en/wcit-12/Pages/default.aspx.

services."[4] Despite its status as a signatory, Argentina maintained reservations about being bound by the regulations, wanting to safeguard the ability to take any measures necessary to protect its national interests.[5] Civil society organizations in Argentina remained heavily involved in the meeting and expressed continued interest in its outcome.[6]

OBSTACLES TO ACCESS

Internet penetration in Argentina has improved consistently over the past decade, reaching 55.8 percent as of 2012.[7] Mobile web connectivity has also increased in recent years, as cellular phones have continued to grow in popularity.[8] The expansion of Argentina's information and communications technology (ICT) sector has been facilitated by increased government investment in telecommunications infrastructure and equipment over the past three years. According to government figures, by September 2012, the number of internet subscriptions in Argentina had reached 12.2 million, with 10.3 million residential connections and 1.9 million commercial connections. As compared to data from 2011, these figures depict an increase of approximately 38 percent in the residential sector and 100 percent in the commercial sector.[9] Broadband connections, offering an average speed of 3 Mbps, have proliferated in recent years, accounting for more than 99 percent of the internet market by late 2012.[10]

Although access is growing across the country, the national Statistics institute,*Instituto Nacional de Estadísticas y Censos*, reports a stark gap between large urban areas (such as the capital Buenos Aires, Cordoba, and Santa Fe) and rural provinces; the former account for over 60 percent of home internet connections in the country.[11] In addition to socioeconomic disparities and price

[4] Anahí Aradas, "*Los Lationamericanos y el Control de Internet*" [Latin Americans and Control over the Internet], *BBC Mundo Tecnología* online, December 14, 2012, http://www.bbc.co.uk/mundo/noticias/2012/12/121214_tecnologia_gobernanza_internet_dubai_aa.shtml.

[5] "*La Argentina Firmó con Reservas la Propuesta para una Nueva Regulación de Internet*" [Argentina Signed the Proposal for New Internet Regulation with Reservations], *Infotechnology*, December 14, 2012, http://www.infotechnology.com/internet/La-Argentina-firmo-con-reservas-la-propuesta-para-una-nueva-regulacion-de-Internet-20121214-0001.html.

[6] Hisham Almiraat, "What Happened at the WCIT-12: Interview with Beatriz Busaniche," *Global Voices Advocacy*, December 15, 2012, http://advocacy.globalvoicesonline.org/2012/12/15/what-happened-at-the-wcit-12-interview-with-beatriz-busaniche; Enrique A. Chaparro, "*Después de la WCIT, y Más Allá*" [After the WCIT, and Beyond], *Fundación Vía Libre*, December 19, 2012, http://www.vialibre.org.ar/2012/12/19/despues-de-la-wcit-y-mas-alla/.

[7] International Telecommunication Union, "Percentage of Individuals Using the Internet, Fixed (Wired) Internet Subscriptions, Fixed (Wired)-broadband Aubscriptions," 2006 & 2011, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#; International Telecommunication Union, "Statistics: Percentage of Individuals Using the Internet, 2000-2012," June 17, 2013, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls.

[8] El Tribuno, "*El Tribuno, con el Presidente de Google en Argentina*" [The Tribune with the President of Google Argentina], *El Tribuno* online, November 22, 2012, http://bit.ly/1dSs6Db.

[9] National Institute of Statistics and Censuses, "Accesos a Internet" [Press Reports on Access to Internet, Third Quarter of 2012], Ministry of Economics and Public Finances, Institute of Statistics and Censuses, accessed March 18, 2013, http://www.indec.gov.ar/nuevaweb/cuadros/14/internet_12_12.pdf.

[10] Yahoo, "*La Argentina está Fuera del Podio de Velocidad de Internet en América Latina*" [Argentina is Outside the Podium of Internet Speed in Latin America], Yahoo News, May 30, 2012, http://ar.noticias.yahoo.com/argentina-podio-velocidad-internet-am%C3%A9rica-latina-181000405.html.

[11] National Institute of Statistics and Censuses, "*Accesos a Internet*" [Press Reports on Access to Internet, Third Quarter of 2012], Ministry of Economics and Public Finances, Institute of Statistics and Censuses, accessed March 18, 2013, http://www.indec.gov.ar/nuevaweb/cuadros/14/internet_12_12.pdf.

differences, National access points in geographically remote areas such as Patagonia and the Northwest contribute to this urban-rural divide.[12] The average broadband plan costs 115 pesos (US$23) per month for the first twelve months, compared to a minimum monthly wage of 2,875 pesos (US$560). While some studies indicate that the average cost of a broadband plan could be almost twice the aforementioned figure, such cost disparity is likely the result of differing scopes of analysis—if only the initial price of service is analyzed, a lower cost estimate results; if cost is based on average prices for the first two years of service, a higher cost estimate is seen.[13]

In recent years, the Argentine government has accelerated its efforts to promote internet access via a number of progressive policies. These include: the Digital Agenda of 2009, which established a national plan for ICTs to connect citizens with government institutions in order to create a "knowledge society;" the Argentina Connected Plan of 2010, a five-year initiative to expand infrastructure and telecommunications services to the entire country; and the Equal Connection Plan of 2010, which led to the provision of internet connections at all public secondary schools and laptop computers for students throughout the country. Although universal service obligations have been in place since 2001, the Universal Service Trust Fund, a government initiative predicated on the enforcement of access commitments, was not enacted until November 2010.[14]

As of 2013, these policies have resulted in increasing internet access in rural areas, schools, parks, and public spaces.[15] Some provinces have also made arrangements with the national government to build a wider fiber-optic network. In certain areas, rural cooperatives are responsible for the installation of the network, resulting in significant growth in local penetration rates, and allowing provincial governments to plan for future triple play service.[16] Considering the national government's share of the mobile spectrum, discussions have arisen regarding the availability of tetra play service (a bundled service package of broadband internet, television and telephone along with wireless service provisions) in the near future. Should the federal government decide to move

[12] Interview with employee of the Library of the National Communications Commission,, February 18, 2012.
[13] Hernán Galperín, "Prices and Quality of Broadband in Latin America: Benchmarking and Trends," Center for Technology and Society, University of San Andrés, August 2012, http://www.udesa.edu.ar/files/AdmTecySociedad/12_ENG.pdf.
[14] The Universal Serice Trust Fund reinvests one percent of profits from ICT telecommunications companies' profits to narrow the gap in access to broadband services across provinces.
[15] "*Inclusion Digital fue Eje de las Politicas Llevadas Adelante*," [Digital Inclusion was the Center of the Policies], *Terra Noticias*, December 19, 2012, http://noticias.terra.com.ar/inclusion-digital-fue-eje-de-las-politicas-llevadas-adelante,474e7ceb0e2bb310VgnCLD2000000ec6eb0aRCRD.html; "," [The Equal Connection Plan Continues its Success in 2013], *AE Tecno,*, December 24, 2012, http://tecno.americaeconomia.com/noticias/programa-argentino-conectar-igualdad-continua-con-exito-hacia-el-2013; "Rural Schools and Islands Will Connect to Internet Through Satellite Antennas," *Diario Victoria*, August 3, 2012, http://www.diariovictoria.com.ar/2012/08/escuelas-rurales-y-de-islas-contaran-con-conexion-a-internet-a-traves-de-antenas-satelitales/; *"Escuelas Rirales y de Islas Contarán con Conexión a Internet a Través de Antenas Satelitales*" [Island and Rural Schools will have Internet Connection via Satellite Dishes], July 30, 2012, http://www.argentinaconectada.gob.ar/notas/3266-avanza-la-instalacin-internet-satelital-escuelas-rurales-y-frontera; Angeles Castro, "*Ochenta Plazas Tendrán Acceso a Internet*" [Eighty Parks will have Internet Access], *La Nacion*, July 2, 2012, http://www.lanacion.com.ar/1486839-ochenta-plazas-tendran-acceso-a-internet.
[16] "*El 91% de los Neuquinos Tiene Acceso a Banda Ancha en su Casa*" [91% of Neuquen People Have Broadband Access at Home] *La Mañana Neuquen*, January 21, 2013, http://www.lmneuquen.com.ar/noticias/2013/1/21/el-91-de-los-neuquinos-tiene-acceso-a-banda-ancha-en-su-casa_175489; "*Cooperativas Instalaron Fibra Optica en el Sur Cordobes*" [Cooperatives Installed Fiber Optics in the South of Cordoba], *El Comercial*, December 27, 2012, http://bit.ly/GzrS8W; "Provinces Will Offer their Version of Triple Play Hand in Hand with the Equal Connection Plan", *iProfesional*, February 2, 2013, http://bit.ly/13Ijpo3; "Implementation of the Network that will Bring Internet to the Whole Province Goes Forward", *El Esquiú,* January 28, 2013, http://www.elesquiu.com/notas/2013/1/28/sociedad-269839.asp.

forward with such offerings, partnerships may be formed with local governments allowing for federal assistance in the form of necessary infrastructure. It is in this context that the government has deemed the Federal Wireless Network an issue of public interest, a classification which will prioritize the expansion of national internet access.[17] In keeping with its expanding ICT investment, the Argentine government is now building the first three communications satellites in the country's history.[18]

The aforementioned government initiatives have resulted in a surge of data traffic over the national network.[19] Although this is a boon to projects dedicated to increasing internet access, in some cases, such occurrences have been detrimental to quality of service.[20] Despite new installations of network access points designed to improve the user experience, the regional landscape has resulted in small businesses being provided with lower quality than residential users.[21] The government has spent substantial time and money improving the national network, however connection gaps remain in some provinces, where penetration rates remain as low as 25 percent.[22]

When the telecommunications industry was privatized in the 1980s, the former state-owned operator was split into two companies: Telecom Argentina, which covers the Northern region of the country, and Telefonica de Argentina, which covers the South. Some 300 other companies have since been granted licenses to operate as internet service providers (ISPs).[23] Many of these enterprises are regional providers and serve as provincial subsidiaries of the aforementioned umbrella companies or other large firms such as Fibertel (of Grupo Clarín), which also controls a notable share of the broadband market.[24]

To date, the State has not interfered with international internet connectivity. However, as part of the Argentina Connected Plan, the government has begun work on an internal state-sponsored fiber-optic cable backbone, to be managed by a government-owned firm upon its completion, which is

[17] "*Declaran de interés público la Red Federal Inalámbrica*" [Federal Wireless Network Declared A Public Interest], *Ambito*, December 17, 2012, http://ambito.com/noticia.asp?id=667793.
[18] "*Por Primera Vez Argentina Construirá Tres Satélites de Comunicaciones*" [For the First Time Argentina Will Build Three Communications Satellites], *Ambito*, September 10, 2012, http://www.ambito.com/noticia.asp?id=653735.
[19] Canal AR, "*En un Año Se Cuadruplicó el Tráfico de Datos en la Red Nacional de NAP*" [In One Year the Data Traffic of the NAP National Network Quadrupled], Canal AR, September 13, 2012, http://www.canal-ar.com.ar/nota.asp?Id=17758.
[20], "*Argentina Ocupa el 38 Lugar en la Calidad del Acceso a Internet*" [Argentina Ranks 38th on Internet Quality], *El Esquiú*, September 7, 2012, http://www.elesquiu.com/notas/2012/9/7/tecnologia-253616.asp.
[21] "Center in La Plata will Improve Internet Connection", Bureau de Presna, June 7, 2012, http://www.bureaudeprensa.com/comunicados/view.php?bn=bureaudeprensa_inte&key=1339083712; "*Brasil y Argentina Lideran el Ranking de Centros de Interconexión a Internet*" [Brazil and Argentina Lead the Ranking of Internet Interconnection Centers", CABASE, December 18, 2012, http://www.cabase.org.ar/wordpress/brasil-y-argentina-lideran-el-ranking-de-centros-de-interconexion-a-internet/; Jorge Gustavo, "*Las Pymes Reciben Peor Servicio de Banda Ancha que el Segmento Residencial*" [Small Businesses Have Worst Internet Quality than ResidentialSegment], *Cronista*, January 28, 2013, http://bit.ly/123ngzN.
[22] "*ArSat Invest 830 Million Dollars on Telecommunications*," *Prensario Internacional*, July 17, 2012; "*Conectar "Desigualdad": Más del 75% de los Hogares de Jujuy No Poseen Acceso a Internet*" ['Unequal´Connection:75% of the Homes in Jujuy Lack Internet Access," *Jujuy al Día*, January 9, 2013, http://www.jujuyaldia.com.ar/2013/01/09/conectar-desigualdad-mas-del-75-de-los-hogares-de-jujuy-no-poseen-acceso-a-internet/; National Institute of Statistics and Censuses, "*Encuesta Nacional sobre Acceso y Uso de Tecnologías de laInformación y la Comunicación (ENTIC)*" [National Inquiry on Access and Use of TICs], December 11, 2012, http://www.indec.gob.ar/nuevaweb/cuadros/novedades/entic_11_12_12.pdf.
[23] "*Informacion de las Empresas*" [Business Information], National Communications Commission, accessed March 20, 2012, http://www.cnc.gob.ar/ciudadanos/internet/empresas.asp?offset=0.
[24] "Argentina Broadband Overview," Point-Topic.

currently scheduled for 2015.[25] It remains to be seen whether or not this project will result in greater centralization – and greater government control – of the backbone.

Mobile phone penetration in Argentina is significantly higher than internet usage, with 59 million lines active as of late 2012,[26] or 143 cellular telephone subscriptions per 100 inhabitants.[27] The mobile phone market in Argentina is dominated by three providers: Telefonica's Movistar, Telecom´s Personal, and Claro, owned by Mexican billionaire and world's richest man Carlos Slim Helu.[28] Each provider covers approximately one third of the market; all offer 3G services.

Following a 2004 agreement that permitted Telefónica to buy Movicom, a cell phone company that was utilizing 850MHz and 1900 MHz cellular frequencies, the government has restricted the use of those specific bands.[29] In accordance with the purchase agreement for Movicom, Telefónica was required to relinquish the frequencies to the state free of charge in order to avoid concentration of the radio-electric spectrum in the hands of a few. After repeated postponement of auctions for the frequency bands in 2012, the situation was finally resolved by the federal government. President Fernandez de Kirchner announced that Libre.ar, a branch of government-owned corporation ArSat, would administer the frequencies, offering cellular phone services through small businesses and telephone cooperatives.[30] This decision, implemented via Resolution 71/2012 of the Communication Secretariat,[31] (and justified with the rationale that only one of the companies bidding for the bands met necessary requirements related to future investment and development[32]) allows the government to regain control over the mobile sector.[33] To date, such control has not extended to the government overtaking ICTs.

The Argentine government planned to launch its proprietary mobile service in March 2013, through an arrangement with Movistar, Personal, and Claro that allows the three providers to use state-owned frequencies. As of publication, however, the government's mobile service had not yet been launched. When implemented, the agreement will allow some telephone cooperatives and small

[25] Government-owned corporation AR-SAT would manage the network. AR-SAT began operating in July 2006. Its stated purpose is to promote the Argentine space industry and increase satellite services to different parts of the country. AR-SAT Company website: http://www.arsat.com.ar.

[26] National Institute of Statistics and Censuses, "Historic Series of Communications: Active Cellphones," National Communications Commission, accessed June 5, 2012, http://www.indec.gob.ar/nuevaweb/cuadros/14/sh_comunicac2.xls

[27] International Telecommunication Union, "Statistics: Mobile-Cellular Subscriptions, 2000-2012," June 17, 2013, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls.

[28] "The Richest People on the Planet 2013," *Forbes*, April 4, 2013, http://www.forbes.com/billionaires/.

[29] Gekkye, "*Argentina Licita Frecuencias de Telefonia Celular*" [Argentina Bids Cellular Telephony Frequencies], Geekye online, June 6, 2012, http://geekye.infonews.com/2012/06/06/tecnologia-23977-argentina-licita-frecuencias-de-telefonia-celular.php.

[30] Marcelo Canton, "*Ponen en Marcha la Empresa Estatal de Celulares*" [Libre.ar, The State Mobile Company Started Working], Clarin, December 14, 2012, http://www.clarin.com/politica/Ponen-empresa-estatal-celulares-Librear_0_828517184.html; Juan Pedro Tomás, "*Nuevamente Retrasan Licitación de Espectro Móvil*" [Once More, Bid for the Mobile Spectrum is Delayed," *BN Americas*, June 8, 2012, http://bit.ly/1eUxPvl.

[31] Resolution 71/2012, Communications Secretariat, Contabilis, http://contablis.com.ar/legislacion/resoluciones/resolucion-71-2012-sec-comunicaciones.

[32] "*Planificación Anunció que ARSAT Explotará Frecuencias para Telefonía Celular*" [It was Announced that ArSat Will Exploit Cellular Phone Frequncies], TELAM, September 9, 2012, http://www.telam.com.ar/nota/37042/.

[33] "*Estado Administrará 25% del Espectro para Servicios Móviles con ARSAT*"[The State will Administer 25% of the Mobile Services Specter], *Media Telecom*, December 14, 2012, http://bit.ly/15F0VvO.

businesses to resell these services,[34] a development viewed by the cooperatives as an opportunity to gain recognition in the mobile services arena.[35] The new plan is also attractive to foreign investors looking to enter Latin America's mobile services market, such as Chinese telecommunications firm Datang Mobile, which views Argentina as the most profitable point of entry due to its large number of cellphones and potential to embrace 4G services.[36]

The government's proposed mobile service has the potential to catalyze positive change in the industry, especially given that mobile providers currently face harsh criticism related to poor performance and high prices.[37] Accordingly, all three major providers have stated their plans to invest in infrastructure during 2013 in order to expand and improve fixed line and mobile networks.[38] Another positive development in this field concerns a debate currently before the Senate over a law that obligates companies to commercialize cell phones for people with hypoacusis, or partial hearing loss.[39] If passed, this law would define the provision of mobile phones as a public service, a classification which has been subject to national debate, but which would ameliorate the high prices that telecommunications companies currently charge.[40]

Private companies wishing to operate as ISPs must first obtain a license from the communications commission, Comisión Nacional de Comunicaciones (CNC).[41] The CNC functions under the communications secretariat, Secretaría de Comunicaciones, as a decentralized entity. Both operate

[34] Alejandro Alfie, "*El Gobierno Profundiza su Acuerdo con las Telefónicas*" [The Government deepens the agreement with the Cell Phone Companies], Clarin, January 4, 2013, http://www.clarin.com/politica/Gobierno-profundiza-acuerdo-telefonicas_0_841115952.html.

[35] "*Expectativa Entre las Cooperativas Para Poder Dar Servicio de Telefonía Móvil*" [Expectations from the Telephone Cooperatives for the Possibility of Rendering the Mobile Service], Telam, September 9, 2012, http://www.telam.com.ar/nota/38902/.

[36] *"El Negocio de las Telecomunicaciones Atrae el Interés Chino*" [Chinese Interest in National Telecommunications], Telam, October 7, 2012, http://www.telam.com.ar/nota/40165/.

[37] "*Los Celulares Van al Tope del Ranking de Reclamos*" [Mobile Services Rank First on Complaints] *El Dia*, November 5, 2012, http://www.eldia.com.ar/edis/20121105/los-celulares-van-tope-del-ranking-reclamos-laciudad7.htm; "*Argentina Paga la Telefonía Celular Más Cara del Mundo*" [Argentina Pays Most Expensive Mobile Service in the World], *La Capital*, November 1, 2012, http://www.lacapital.com.ar/informacion-gral/Argentina-paga-la-telefonia-celular-mas-cara-del-mundo-20121101-0042.html; Martin Grosz, "*Celulares: Hablar con Tarjeta Cuesta Hasta 6 Veces Más que el Abono Fijo*" [Pre-Paid Plans Are 6 Times More Expensive than Normal Plans], *Clarin*, December 28, 2012, http://www.clarin.com/sociedad/Celulares-hablar-tarjeta-cuesta-abono_0_836916401.html.

[38] "*Personal Avanza con un Plan de Reconversion Tecnologica*" [Personal Plans a Technologic Rationalization], *Terra Noticias*, January 13, 2013, http://noticias.terra.com.ar/personal-avanza-con-un-plan-de-reconversion-tecnologica,ade598ce1e34c310VgnCLD2000000ec6eb0aRCRD.html"*Telefónica Invertirá 2,045 Mdd en Argentina*" [Telefonica Will Invest 2,045 Million Dollars in Argentina], Reuters via *El Economista*, December 18, 2012, http://eleconomista.com.mx/industria-global/2012/12/18/telefonica-invertira-2045-mdd-argentina; José Crettaz, "*Claro Anunció una Inversión de US$ 400 Millones en su Red Móvil, Unilever Invierte $ 1500 Millones*" [Claro Announces a $400 Million Investment in its Mobile Network, Unilever Invests 1.5 Billion], *La Nacion*, November 8, 2012, http://bit.ly/Z3qHCv.

[39] "*El Senado Aprobó Ampliar el Acceso a la Telefonía Móvil para Personas Hipoacúsicas*" [Senate Approved Access to Mobile Network of Persons with Hypoacusis], *Diario Victoria*, November 29, 2012, http://www.diariovictoria.com.ar/2012/11/el-senado-aprobo-ampliar-el-acceso-a-la-telefonia-movil-para-personas-hipoacusicas/.

[40] "*Giustiniani y la Cruzada para que el Celular Sea Servicio Público*" [Giustiniani and the Crusade for the Cellular Telephone as a Public Service], *La Capital*, July 2, 2012, http://www.lacapital.com.ar/la-ciudad/Giustiniani-y-la-cruzada-para-que-el-celular-sea-servicio-publico-20120702-0048.html.

[41] National Communications Commission, , "Decree 764/2000 Annex 1" [in Spanish], accessed March 20, 2012, http://www.cnc.gov.ar/normativa/Dec764_00-AnexoI.pdf.

under the authority of the Ministry of Federal Planning, Public Investment, and Services.[42] Upon receipt of an application, the CNC refers the submission to the Secretariat of Communications, which makes the final decision to grant a license. The applicant is required to pay a relatively modest sum of 5,000 Argentine pesos ($1,100) at the time of submission.[43] The licensing process for mobile phone providers is similar; once approved, no additional fees are charged, however providers are required to pay special taxes, such as those specified under the Universal Service Trust Fund. Cybercafe licenses are processed like those of any other small business; no additional approvals are required.

Although the statutory composition of the CNC offers some degree of independence, per Presidential Decree 521, the executive branch has run the body since 2002 in order to increase efficiency.[44] The decree provides for an ad hoc administrator (*interventor*) appointed by the president, —who fulfills the functions of the CNC president and board of directors and also appoints other commission members at his or her discretion. This arrangement has detracted from the independence of the institution, but there have been few complaints about corruption or unfairness in the CNC's operations. Since 2010, controversy and accusations of political bias have emerged surrounding one case, Fibertel's ISP license, indicating a degree of public mistrust of the regulator.[45] A case relating to these charges has been pending before a federal court since March 2013.

LIMITS ON CONTENT

Argentine internet users have access to a wide array of online content, including international and local news outlets, websites of political parties, and civil society initiatives. The government does not impose automated filtering or restrictions on politically oriented information. However, websites related to pornography are blocked in educational institutions, libraries, and other public locations in Buenos Aires in accordance with Law 2974.[46] In recent years, controversy has emerged over the blocking of allegedly defamatory material, copyright protected content, and injunctions that invoke intermediary liability. A few projects related to these issues were recently taken up in Congress.

Various social media tools, such as the social networking site Facebook, the video-sharing platform YouTube, and the microblogging service Twitter are freely available in Argentina. In August 2011, however, Google's blog-hosting platform Blogger was blocked for nearly one week following a

[42] Ministry of Federal Planning, "Organization Chart" [in Spanish], Public Investment and Services, accessed June 6, 2012, http://institucional.minplan.gov.ar/html/organigrama/.
[43] National Communications Commission,"Guide for License Applications," accessed March 20, 2012, http://www.cnc.gob.ar/infotecnica/archivos/Guide_Licence%20Application[eng].pdf.
[44] National Communications Commission, Presidential Decree N° 521/2002 [in Spanish], March 20, 2002, http://www.cnc.gov.ar/institucional/biblioteca/buscador/Normativa/pdf/Decreto-521_02.pdf.
[45] "Pressed: Argentina's Media," *The Economist,* August 25, 2010, http://www.economist.com/blogs/americasview/2010/08/argentinas_media; "Federal Judge Freezes Order to Cancel Fibertel's License, Govt to Appeal," *Business News Americas*, September 27, 2010, http://www.bnamericas.com/news/telecommunications/Federal_judge_freezes_order_to_cancel_Fibertel*s_license,_govt_to_appeal.
[46] Argentine Federal Government, Law No. 2974, CEDOM; http://www.cedom.gov.ar/es/legislacion/normas/leyes/ley2974.html

court decision to restrict access to two URLs for websites titled *Leaky Mails* functioning as local spinoffs of WikiLeaks, one hosted on Blogspot, a Blogger service which provides domain names.[47] These websites had published the correspondence of government officials, politicians, journalists, and other public figures. Much of the content on the sites appeared to be personal in nature and irrelevant to both public policy and the exposition of malfeasance and corruption.[48] ISPs complied with the court order and blocked access to the IP addresses of the two pages, effectively blocking the entire Blogger platform, including over one million blogs not specified in the judicial order. After criticism from the public and Google, the block was lifted within one week and ISPs shifted to a more precise filtering technique.[49] As of May 2013, the *Leaky Mails* blog remains inaccessible. The Blogger domain has not had any additional site-wide disruptions.

The judicial action taken against the Cuevana website in 2011 and 2012 also garnered public attention. Launched in 2009, the website, which catalogues and connects users to sites that enable the free streaming of movies and television programs, quickly became one of the most visited websites in Argentina and the largest of its kind in Latin America. Since late 2011, various international content producers, including HBO, Turner Argentina, 20th Century Fox, and Disney Enterprises, have filed lawsuits against the site alleging infringement of intellectual property rights.[50] In November 2011, the National Court of First Instance issued a directive requiring ISPs to block certain programs on Cuevana's website.[51] In March 2012, prosecutors opened a criminal case against the site's administrator, alleging that the site had profited from copyrighted materials via financial donations. The administrator denied the charges, claiming that donations were largely voluntary and that profits had been reinvested.[52] If he is found guilty, the administrator could face up to six years in prison. In January 2013, the Buenos Aires Federal Criminal Court of Appeals rejected a request by HBO Ole Partners to completely block the site.[53] The court determined that the measure was disproportionately broad, especially given that no suspect had been formally identified (the administrator was the only person mentioned in the suit) and that the location of the server was still unknown. It has not yet been determined whether Cuevana is an indexation site

[47] National Communications Commission, "*A Todos los Licenciatarios de Telecomunicaciones que Brindan Servicios de Acceso a Internet*" [All Telecom licensees providing Internet Access services], accessed March 20, 2012, http://www.cnc.gov.ar/noticia_detalle.asp?idnoticia=106.

[48] "*La Justicia Bloqueó al 'WikiLeaks' Argentino*" [Justice Blocked the Argentine ´Wikileaks´], *TN Cable*, August 11, 2011, http://tn.com.ar/politica/00062732/juez-pidio-bloquear-al-%E2%80%9Cwikileaks%E2%80%9D-argentino; "*A Todos los Licenciatarios de Telecomunicaciones que Brindan Servicios de Acceso a Internet.*".

[49] "*Google Denuncia un Bloqueo de sus Blogs en la Argentina*" [Google Reports Blockage of Blogs in Argentina], *TN Cable*, August 19, 2012, http://tn.com.ar/tecnologia/00064541/google-denuncia-un-bloqueo-masivo-de-sus-blogs-en-la-argentina.

[50] "*Cuevana Suma Más Problemas*" [Cuevana Has More Problems], Clarin, March 7, 2012, http://www.clarin.com/internet/mundo_web/titulo_0_659334165.html; "*Cuevana: Abren Causa Penal Contra los Dueños del Sitio en Argentina*" [Cuevana: Open Criminal Case Against the Owners of the Site in Argentina], *La Tercera*, March 16, 2012, http://bit.ly/zjW8g3.

[51] Juan Pablo De Santis, "*La Justicia Pidió Bloquear el Acceso a Series en Cuevana*" [Justice Blocks Access to TV Shows in Cuevana], *La Nacion*, November 30, 2011, http://bit.ly/GzsTxc.

[52] Gonzalo Larrea, "Argentina Opens Criminal Case Against Cuevana," TTV Media News, http://www.ttvmedianews.com/scripts/templates/estilo_nota.asp?nota=eng%2FTech%2FInternet%2F2012%2F03_Marzo%2F16_justicia_vs_cuevana; Pablo Sirven, "*Inician Causa Penal Contra Cuevana*" [Criminal Proceedings Initiated Against Cuevana], *La Nacion*, March 16, 2012, http://www.lanacion.com.ar/1456828-inician-causa-penal-contra-cuevana.

[53] "*La Justicia Rechazó Bloquear Acceso a Cuevana*" [Justice rejects the blocking of Cuevana], *InfoBae*, February 6, 2013, http://www.infobae.com/notas/695159-La-Justicia-rechazo-bloquear-el-acceso-a-Cuevana.html.

controlled by users, or if there are identifiable persons responsible for running the site. The name of the administrator, however, was allegedly in the public domain.

To date, there is no legislation which pertains specifically to intermediary liability in Argentina. As such, cases are decided individually and court decisions tend not to be uniform. In the absence of specific regulations adjudicating liability to intermediaries for illegal content posted by third parties, the courts generally apply broad rules pulled from the procedural law and the civil code. Injunctions ordering takedown of content are also based on general rules.

By the end of 2012, multiple cases regarding intermediary liability were presented before the courts,[54] resulting in rulings against Google and Yahoo requiring the removal of sensitive material. The individuals responsible for posting the material in question were in some cases ordered to pay damages to the prominent public figures that had brought the charges. Actress Paola Krum and model Barbara Lorenzo were among the plaintiffs awarded monetary compensation. Court orders also resulted in Google and Yahoo removing the sensitive material from their search results and blocking illicit images of both Krum and Lorenzo. In a more recent case, search engines were asked to block a pornographic video made by well-known actress Florencia Peña before the video was even uploaded. If found guilty of non-compliance, Google and Yahoo could be fined up to half a million pesos (approximately $41,000 USD).[55]

Another controversial case regarding the blocking of indecent material surrounds the death of Jazmín De Grazia, a model who drowned in a hot tub in February 2012 due to an alleged drug overdose.[56] Immediately following the incident, photographs of De Grazia's dead body were published by a newspaper and spread over the Internet. In September 2012, a Federal Court of Appeals asked De Grazia's parents to identify the webpages that had published the photos, indicating to Google those sites which search engines were required to have blocked. The judge subsequently issued a ruling that web pages containing information about the model were protected by the right to freedom of speech, and could not be blocked by law.[57]

According to Google's Transparency Report, from July to December 2012, the Argentine government submitted 51 court orders for content removal encompassing 160 items. Google

[54] CIJ, "*Ordenan a Google y Yahoo! Eliminar Resultados de Búsqueda Vinculados a la Actriz Paola Krum*" [Justice Orders Google and Yahoo! to Block Search Results Related to Actress Paola Krum], September 5, 2012, http://www.cij.gov.ar/nota-9778-Ordenan-a-Google-y-Yahoo--eliminar-resultados-de-busqueda-vinculados-a-la-actriz-Paola-Krum.html; "*La Justicia Ordenó que Google le Pague a una Modelo Cuya Imagen Aparece en Páginas Porno*" [Google Condemned to Pay a Model for Photographs in Porn Webpages], Clarín online, September 7, 2012, http://www.clarin.com/internet/Justicia-Google-imagen-aparece-paginas_0_769723247.html.

[55] "*La Justicia Falló a Favor de Florencia Peña*" [Court rules on behalf of Florencia Peña], *Los Andes Estilo*, January 23, 2013, http://www.losandes.com.ar/notas/2013/1/23/justicia-fallo-favor-florencia-pena-692789.asp.

[56] "*Confirman que Jazmín de Grazia Murió Ahogada*" [Jazmin de Grazia Drowned], *La Nación*, February 6, 2012, http://www.lanacion.com.ar/1446380-investigan-las-causas-de-la-sorpresiva-muerte-de-jazmin-de-grazia.

[57] Ines Tprnabeme, "*Ordenan a Google Eliminar Fotos de Jazmín de Grazia #google #jazmindegrazia #privacidad*" [Google to Delete Jazmin de Grazia Photographs], *Hábeas Data*, September 5, 2012, http://habeasdatacpdp.wordpress.com/2012/09/05/ordenan-a-google-eliminar-fotos-de-jazmin-de-grazia-google-jazmindegrazia-privacidad/.

complied—at least in part—with 82 percent of the requests.[58] Google's breakdown indicates that the majority of content was related to defamation (62 percent of the cases), followed by privacy and security (18 percent), hate speech (4 percent), and national security (2 percent), with the remainder of requests uncategorized.

In this context, many legal initiatives arose in 2012 and 2013. Senator Maria Eugenia Estenssoro led a project concerning net neutrality, which incorporated a variety of civil society demands and international standards followed by organizations such as the OAS and the UN. It applied not only to ISPs, but rather to all telecommunication service providers, both public and private.[59] Other initiatives, however, have been met with reproach from civil society due to lack of clear terms. Representative Julián Obiglio's proposed project relating to intermediary responsibility, 8070-D-2012, faced criticism for disregarding international standards when allowing third parties and administrative bodies to ask ISPs to remove content without judicial order.[60]

Two other projects, 728/12,[61] and 1892-D-12,[62] seek to monitor the web for certain discriminatory and violent content, by surveilling social networks, e-mails and text messages, and requiring businesses to install detection and filtering programs of content unfit for underage persons.[63] Neither of these initiatives has been signed into law. In May 2013, the Senate Freedom of Expression and Technology Commission hosted a session to discuss net neutrality problems and other projects. Initiatives discussed in this session have not yet been made public.

Self-censorship among bloggers and online users is not widespread, and Argentines express a diverse array of views online. Nevertheless, in the interior of the country where the rule of law is weaker than in the capital district, some online journalists and bloggers are cautious about writing about powerful local officials or mining companies due to the possibility of jeopardizing their relationship with private advertisers. Given Argentina's polarized political environment, some writers may adjust their reporting based on the partisan affiliation of their publication.

In fact, the Argentine federal and local governments are known for their discriminatory allocation of official advertising—excluding news outlets whose reporting has been critical of the government

[58] "Google Transparency Report, Argentina," July to December 2012, http://www.google.com/transparencyreport/removals/government/AR/?by=product&p=2012-12.
[59] Argentine Senate. File 3618/12, http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=3618/12&nro_comision=&tConsulta=3.
[60] Argentine House of Representatives, File 8070-D-2012, http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=8070-D-2012; Beatriz Busaniche, "*Responsabilidad de Intermediarios de Internet: El Debate Pendiente*" [Internet Intermediaries' Responsibility: A Pending Debate], *La Nacion*, November 30, 2012, http://www.lanacion.com.ar/1532025-responsabilidad-de-intermediarios-de-internet-el-debate-pendiente.
[61] Argentine Senate, File 728/12, http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=728/12&nro_comision=&tConsulta=3
[62] Argentine House of Representatives, File 1892-D-2012, http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=1892-D-2012.
[63] Carlos Cortes, "Vigilance on the Internet," CELE-iLEI, July 2012, http://www.palermo.edu/cele/pdf/El-deseo-de-observar-la-red.pdf; Beatriz Busaniche, "*Protección de Menores y Libertad de Expresión en Internet*" [Protection of Minors and Freedom of Speech on the Internet], *La Nacion*, August 15, 2012, http://www.lanacion.com.ar/1498094-proteccion-de-menores-y-libertad-de-expresion-en-internet.

and rewarding those who publish supportive media.[64] This phenomenon has had a negative impact on freedom of expression, particularly in the print and broadcast media sectors.[65] While funds allocated to internet activities represent only three percent of the federal advertising budget, during the first semester of 2012, 42 percent of that sum was assigned to only 10 beneficiaries, all with clear ties to the federal government.[66] In March 2011, the Supreme Court ruled unanimously that the government must utilize equitable measures in its distribution of state advertising.[67] Due to the government's non-compliance, the Federal Court of Appeals issued a new request in August 2012 urging the state to abide by the law.[68] To date, the government has faced no penalties for non-compliance.

There are no restrictions on access to national or foreign news sources, and Argentines are able to express themselves freely online. According to some observers, the vigor of the pro-government blogosphere has increased since 2009, although other oppositional political parties have also started to gain ground.[69] A wide range of views are shared online, including those related to potentially sensitive topics such as the recent designation of Pope Francisco despite allegations that he was complicit in abuses carried out by the Argentine Government in 1976.[70] Opinions regarding the controversial Argentina-Iran agreement—which concerns the 1990s terrorist attack of a Jewish Association in Buenos Aires—are also voiced online.[71] Despite such vigorous discussion, journalists have complained about a lack of access to government representatives and a dearth of official press conferences. In 2009, an online portal called *Mejor Democracia* ("Better Democracy"), which provided the public with government-related information, was shut down. When it later reopened,

[64] "*Dimensión de la Publicidad Oficial en la Argentina*" [The Dimension of Official Publicity in Argentina], Poder Ciudadano, accessed March 20, 2012, http://poderciudadano.org/wp/wp-content/uploads/2011/12/Informaci%C3%B3n-preliminar-PO-Poder-Ciudadano.pdf; Asociacion por los Derechos Civiles and Open Society Justice Initiative, "Buying the News: A report on Financial and Indirect Censorship in Argentina," Open Society Institute (2005), http://www.censuraindirecta.org.ar/advf/documentos/48ee57ee263549.92961213.pdf.

[65] Poder Ciudadano, "Dimensión de la Publicidad Oficial en la Argentina."

[66] Juan Pablo de Santis, "*En Internet, el Dinero de la Publicidad Oficial También Queda en Pocas Manos*" [On the Internet, Official Advertising is Also in the Hands of a Few], *La Nacion*, March 21, 2013, http://www.lanacion.com.ar/1564903-en-internet-el-dinero-de-la-publicidad-oficial-tambien-queda-en-pocas-manos.

[67] IFEX, "Supreme Court Urges Government to Avoid Bias in Allocating State Advertising," news release, March 8, 2011, http://www.ifex.org/argentina/2011/03/08/omit_discriminatory_criteria/; Committee to Protect Journalists, "Supreme Court Tells Argentina to Avoid Bias in Allocating Ads," March 4, 2011, http://cpj.org/2011/03/supreme-court-urges-argentina-to-avoid-bias-in-all.php.

[68] "*La Publicidad Oficial*" [The Official Advertising], *Pagina 12*, August 15, 2012, http://www.pagina12.com.ar/diario/elpais/1-201096-2012-08-15.html; *Clarin*, "*Publicidad Oficial: Otro Fallo en Favor de Perfil*" [Official Advertising: Another Ruling Benefits Perfil], *Clarin*, August 15, 2012, http://www.clarin.com/politica/Publicidad-oficial-fallo-favor-Perfil_0_755924464.html; Editorial Perfil SA c/ Federal Government – Chief of Staff of Ministers – SMCs under Law 16.986, March 2011; Editorial Black River [Rio Negro] SA c/ Neuquén Province s/amparo, Fallos 330:3907, September 2007.

[69] Jorge Gobbi, "Argentina: Presidential Elections, a Review of Blogs," *Global Voices*, October 26, 2011, http://globalvoicesonline.org/2011/10/26/argentina-presidential-elections-a-review-of-blogs/.

[70] Mariano Castillo, "Humble Pope Has Complicated Past," CNN, March 16, 2013, http://www.cnn.com/2013/03/14/world/americas/argentina-pope-profile; Luis Majul, "*Francisco le Gana a CFK en Todos los Frentes*" [Francisco Beats CFK on Every Front], *La Nacion*, March 21, 2013, http://www.lanacion.com.ar/1565328-francisco-le-gana-a-cfk-en-todos-los-frentes.

[71] Hernan Cappiello, "*Buscan Anular en la Justicia el Acuerdo con Irán*" [The Jewish Community is Trying to Annul the Treaty with Iran], *La Nacion*, March 1, 2013, http://www.lanacion.com.ar/1558988-buscan-anular-en-la-justicia-el-acuerdo-con-iran.

it did so with reduced transparency, offering notably less information than in its previous incarnation.[72] This is true to the present day.

Most civil society organizations also maintain their own websites, although user engagement in sociopolitical movements is relatively low. Mobile phones, meanwhile, are increasingly being used as a tool for activism; such devices will likely play decisive roles in future political movements.[73] Mobile phone users have also utilized social media in order to protest poor quality of service by orchestrating cellular blackouts, or periods of time when large groups of users refuse to use their cellphones. Such measures have also been applied to social networks such as Twitter (#14N) and Facebook (*Apagón Celular de Facebook*, also known as the Cell Blackout Facebook Group).[74]

The popularity of social media tools has grown overall in recent years. By April 2012, Argentina had over 20 million registered Facebook users, representing almost 50 percent of the population,[75] as well as approximately 1.6 million Twitter users.[76] In late 2012, a major antigovernment protest known as 8N (November 8) was mobilized using social media. The movement, which culminated in thousands of people taking to the streets of Buenos Aires, Mendoza, Cordoba, and other cities to protest corruption, violent crime, diminishing freedom of expression, and inflation, was organized over Twitter (#8N) and Facebook. Throughout the protest, photos, videos, and opinions appeared on Twitter, both in support of the movement (#8NYoVoyPorQue, "I go because") and against it (#8NYoNoVoyPorQue, "I don't go because"). Even those not in favor of protesting were largely in agreement over the problems Argentina is facing, and saw the movement as a catalyst to make use of social media to call for change through various avenues such as reform and voting.[77] The scope of the campaign, which began informally on social networks, was so large that shadow protests occurred outside Argentine embassies in locations as far flung as Rome and Sydney.[78] 8N was the largest protest in Argentina in over a decade, mobilizing at least 30,000 people in Buenos Aires according to local police, a figure which regional media placed closer to 100,000.[79]

---

[72] Asociacion por los Derechos Civiles, "*Califican de 'Retroceso' el Bloqueo de la Web Oficial*" ['Regression' Rating Blocks OFficial Website], October 8, 2009, http://www.adc.org.ar/sw_contenido.php?id=643.
[73] Lourdes Cajrdenas, "*ONG Movilizan a Ciudadanos por Celular*" [NGOs Mobilize Citizenship by Cellphone], CNN Expansion, January 15, 2010, http://www.cnnexpansion.com/expansion/2009/12/11/Mensajes-sin-excusas.
[74] "*Convocan a un Apagon de Celulares el Miercoles*" [Mobile Blackout on Wednesday], *La Nacion*, November 13, 2012, http://www.lanacion.com.ar/1525892-convocan-a-un-apagon-de-celulares-el-miercoles.
[75] Social Bakers, "Argentina: Facebook Statics," accessed February 1, 2013, http://www.socialbakers.com/facebook-statistics/argentina.
[76] New Media Trend Watch, "Markets by Country: Argentina," European Travel Commission (2012) http://www.newmediatrendwatch.com/markets-by-country/11-long-haul/35-argentina.
[77] Laura Schneider, *"#8N: Nueva Protesta Masiva en Argentina*" [#8N: New Massive Protest in Argentina], *Global Voices* , November 9, 2012, http://es.globalvoicesonline.org/2012/11/09/8n-nueva-protesta-masiva-en-argentina/.
[78] "*Bergman: 'Hubo Organización y Logística en la Marcha del 8N'*" [Bergman: Organiztion and Logistic Work for the 8N Mobilization], *El Intransigente*, November 8, 2012, http://www.elintransigente.com/notas/2012/11/8/bergmanhubo-organizacion-logistica-marcha-del-8n-155979.asp; "*Una Multitud se Movilizó en el 8N y Hubo Cacerolazos en Casi Todo el País*" [Big Crowd for the 8N and ´Cacerolazos´in Nearly the Whole Country], *La Nacion*, November 8, 2012, http://www.lanacion.com.ar/1524741-cacerolazo-8n; Conz Preti, "Argentines Take to the Streets to Protest," *ABC News*, November 8, 2012, http://abcnews.go.com/ABC_Univision/News/page/argentines-world-streets-protest-17673951.
[79] Damian Pachter, "Argentines Protest in Huge Anti-Government March," *The Huffington Post*, November 8, 2012, http://www.huffingtonpost.com/huff-wires/20121108/lt-argentina-anti-government-march/.

VIOLATIONS OF USER RIGHTS

The Argentine Constitution and human rights treaties incorporated into the Constitution in 1994 guarantee freedom of expression.[80] Additional laws ensure that citizens have the liberty to express their views without fear of censorship or reprisal. In 2005, constitutional protections were explicitly extended to "the search, reception and dissemination of ideas and information of all kinds via internet services" under Law 26032.[81]

The Argentine judiciary is generally seen as independent, particularly in its higher echelons, such as the Supreme Court of Justice. The Supreme Court has issued several rulings supportive of freedom of expression in recent years. Among these are the aforementioned 2011 decision regarding discriminatory allocation of government advertising, as well as the 2009 suspension of a requirement mandating that service providers retain user data for ten years.[82] The government has also been responsive to decisions of the Inter-American Court of Human Rights and the recommendations of the Inter-American Commission on Human Rights. These procedures have helped accelerate reform of the criminal code's provisions on insult (*desacato*) and defamation. In November 2009, the legislature decriminalized defamatory statements referring to matters of public interest.[83]

No specific laws criminalize online expression related to political or social issues. The 2008 Law on Cybercrime (Law 26388) amended the Argentine Criminal Code to cover offenses such as hacking, dissemination of child pornography, and other online crimes.[84] Some of the amendments have been criticized as overly vague and imprecise in their wording, which could open the door to broad interpretations. Lawyers and human rights groups have also expressed concern over the country's antiterrorism law, arguing that the definition of terrorism provided is overly broad and could therefore be employed to punish legitimate political dissent, social protests, or economic analysis.[85] So far, neither of these laws has been used in practice to punish online expression. As of May 2013, no bloggers, online journalists, or ordinary users were imprisoned for the expression of their views in online forums or via private communications. One website administrator, however, was facing criminal charges and a possible jail term over allegations of profiting from copyrighted material.

---

[80] See Article 14, "Argentine Constitution," Senate of the Argentine Nation, accessed March 20, 2012, http://www.senado.gov.ar/web/interes/constitucion/english.php. The constitution was amended in 1994, and Article 75 (22) now accords numerous international human rights treaties with constitutional status and precedence over national laws.

[81] Law 26032 [in Spanish] (2005), Documentation and Information Center, accessed March 20, 2012, http://www.infoleg.gov.ar/infolegInternet/anexos/105000-109999/107145/norma.htm.

[82] Judgment of Halabi v. P.E.N. Argentine Supreme Court, June 26, 2007; Lorenzo Villegas Carrasquilla, "Personal Data Protection in Latin America: Retention and Processing of Personal Data in the Internet Sphere," Center for Studies in Freedom of Expression and Access to Information, http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/05-Personal_data_protection_Latin_America_Villegas_Carrasquilla.pdf.

[83] Reform Law 26551, See: CELE http://www.lanacion.com.ar/1512551-calumnias-e-injurias-dos-delitos-de-incomoda-vigencia.

[84] Law26.388 [in Spanish] (2008), Documentation and Information Center, accessed March 20, 2012, http://www.infoleg.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm.

[85] Lillie Langtry, "Argentina: Concerns Over New Terrorism Law," *Memory in Latin America*, December 30, 2011, http://memoryinlatinamerica.blogspot.com/2011/12/argentina-concerns-over-new-terrorism.html; "Argentina: Fears Over Terror Law," *New York Times*, December 28, 2011, http://nyti.ms/16QpCiO.

Although violence against online journalists occurs sporadically, it is not nearly as frequent as violence against those working for traditional media outlets. Local press freedom watchdogs recorded approximately 70 cases of physical and verbal attacks against journalists during the first half of 2012. Most attacks were attributed to non-state actors in inland regions against those working for traditional media outlets.[86] However, in some cases, the targeted journalists also maintained websites or contributed to online news outlets. Another report by The Argentine Journalists Forum, known as FOPEA, recorded 172 attacks on reporters during 2012; 11 percent of attacks were against people working for digital media outlets.[87]

In one incident from April 2012, Jorge Peña, a city council president in Candelaria, punched TV journalist and news website editor Daniel Luna, who was arguing against being denied access to cover a city council session; the council president was subsequently charged for injuring the reporter. [88] Shortly after, in May 2012, the city council rejected Peña′s request for restitution. In the same session, Rodrigo Castillo, another online news journalist, was attacked while trying to obtain photographs of a city council member. When alerted about this event, the police disregarded the accusation and made no effort to detain the aggressors.[89]

During 2012, some journalists were also subject to defamatory campaigns and privacy breaches extending to the unauthorized disclosure of their personal information on public websites. Gustavo Sylvestre, a political analyst, journalist, and blogger was targeted with such a smear campaign. His business, family, and tax information, as well as the phone numbers and addresses of his personal contacts, were published online. Days later, a derogatory article was published about him.[90] Sylvestre's work, which is highly political in nature, seems likely to have been the motive behind the virtual attack. Although concerning, as of May 2013, such incidents did not appear to be widespread or on the rise.

There are no restrictions on anonymity for internet users, nor are there restrictions on the use of encryption. Users are able to freely post anonymous comments in a variety of online forums, and neither bloggers nor website owners are required to register with the government. When purchasing a mobile phone or prepaid SIM card, however, users must provide identifying

[86] Committee to Protect Journalists, "Argentina," in *Attacks on the Press 2011,* (New York: February 2012) , http://cpj.org/2012/02/attacks-on-the-press-in-2011-argentina.php.
[87] FOPEA, "Fredoom of Expression Monitor in Argentina," 2012 Report (2013), http://monitoreolde.com.ar/InformeMonitoreo2012FOPEA.pdf.
[88] Liliana Honorato, "Argentine City Council President Punches Journalist in the Face," *Journalism in the Americas*, April 19, 2012, http://knightcenter.utexas.edu/blog/00-9784-argentine-city-council-president-punches-journalist-face.
[89] FOPEA, "*Nueva Agresion a Periodista en Candelaria*" [New Aggression to Journalist in Candelaria], May 9, 2012, http://www.fopea.org/Inicio/Nueva_agresion_a_periodista_en_Candelaria.
[90] FOPEA, "*Solidaridad de FOPEA con el Periodista Gustavo Sylvestre por el Artículo que Revela Datos de su Vida Privada y Familiar*" [FOPEA in Solidarity with Gustavo Sylvestre], August 31, 2012, http://bit.ly/1bXeFE5.

information.[91] In December 2011, the Argentine Network Information Center (NIC.ar) was placed directly under the oversight of the Executive branch of the government. [92]

In late 2012, incidents of domain name denials emerged in cases where the names related in some way to President Cristina Fernandez de Kirchner or to the progovernment youth group La Campora. In such cases, applications were either denied by NIC.ar or applicants were asked to modify their proposed domain names. The sole mention of the President's first or last name was reportedly reason enough for an application to be called into question.[93] Accordingly, domains such as cristinacorazon.com.ar, enlacampora.com.ar, and kirchnerismopasion.com.ar were rejected immediately. Upon asking for clarification, Argentine newspaper *Perfil* was told that such domains were forbidden due to their potential to "affect the morale of the person" in question.[94] Such broad restrictions impact sites critical of the administration as well as those which support the government, complicating efforts to develop online platforms dedicated to discussions of national leadership.

In Argentina, a court order is officially required to intercept private communications, even in cases related to national security.[95] It is believed that these procedures are generally followed in practice, although the government does not publish figures on how many interceptions are implemented annually. According to Google's Transparency Report, between July and December 2012 the Argentine authorities made 114 requests for user data covering 175 accounts; Google complied with the release of some data in 38 percent of cases.[96] Microsoft's 2012 Law Enforcement Request Report states a total number of 769 requests for user data covering 1,279 accounts. Microsoft complied with 85.7 percent of requests and found no system data for the remaining 14.3 percent. All requests were determined to satisfy relevant legal requirements.[97]

Over the past decade, there have been several scandals involving officials on both sides of the political spectrum engaging in illegal surveillance of opponents' telephone communications. In one high-profile scandal, evidence surfaced of navy personnel monitoring former President Nestor

[91] Law 19.798, Resolution 490/97 [in Spanish] (1997), "http://www.cnc.gob.ar/normativa/sc0490_97.pdf; Secretaria de Comunicasiones, "*Apruebase de Relamento General de Clientes de lso Servicios de Comunicaciones Moviles*" [Text of the General Terms for Users of Mobile Communication Services], National Communications Commission, accessed March 20, 2012, http://www.cnc.gob.ar/normativa/sc0490_97.pdf.

[92] Network information centers are responsible for the allocation of domain names and registry administration in different countries.

[93] Eduardo Bertoni and Atilio Grimani, "*Nombres de Dominio: Una Expresion que merece ser Protegida*" [Domain Names: An Expression Worth Protecting], CELE – iLEI, November, 2012, http://bit.ly/1dSs1zC.

[94] , "*El Gobierno Rechaza y se Apropia de Dominios de Internet con Nombres K*" [Government Denies and Owns Internet Domains with K Names on Them], *Perfil*, September 9, 2012, http://www.perfil.com/contenidos/2012/09/05/noticia_0024.html.

[95] Law19.798, *Articles 45 bis, 45 ter and 45 quáter* [in Spanish] (1972), "Law of National Telecommunications," Documentation and Information Center, accessed March 20, 2012, http://infoleg.mecon.gov.ar/infolegInternet/anexos/30000-34999/31922/texact.htm;: Law25.520 [in Spanish] (2001), "Law of National Intelligence," Documentation and Information Center, http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70496/norma.htm.

[96] "Google Transparency Report, Argentina.".

[97] Microsoft, *Microsoft Law Enforcement Requests Report 2012*, http://download.microsoft.com/download/F/3/8/F38AF681-EB3A-4645-A9C4-D4F31B8BA8F2/MSFT_Reporting_Data.pdf.

Kirchner for decades.[98] In another incident, the mayor of Buenos Aires, an opposition politician, and the city's police chief are alleged to have illegally wiretapped civic leaders, politicians, and trade union activists.[99] Most such incidents occurred in 2007 or earlier and there is no clear evidence that such violations of privacy continue. Meanwhile, related prosecutions continue to make their way through the courts.

Cybercrime is perceived as a growing problem in Argentina and new cybercrime legislation has emerged in response to recent news indicating that technical attacks might be more common than typical statistics indicate.[100] In November 2012 the General Prosecutor of Ciudad Autónoma de Buenos Aires activated a one-year pilot project in which he assigned a team of prosecutors to the task of investigating crimes aimed at hacking informational systems and programs, as well as the spreading of pornographic content.[101] Such measures and protocols do not yet appear to exist on the national level.[102] Should such incidents occur, those responsible would be liable for prosecution under the criminal code, as amended by the aforementioned Law 26388.

[98] "Fernandez Shakes Up Argentine Military," UPI, January 6, 2012, http://www.upi.com/Top_News/Special/2012/01/06/Fernandez-shakes-up-Argentine-military/UPI-92341325853530/

[99] Nic Pollock, "Wiretapping Case Continues as Judge Oyarbide Closes Investigation Stage," *Argentina Independent*, May 16, 2012, http://www.argentinaindependent.com/currentaffairs/wiretapping-case-continues-as-judge-oyarbide-closes-investigation-stage/; Maria Magro, "Two Clarin Journalists Testify in Buenos Aires Wiretapping Scandal," *Journalism in the Americas* (blog), November 18, 2010, http://knightcenter.utexas.edu/blog/two-clarin-journalists-testify-buenos-aires-wiretapping-scandal.

[100] Virginia Messi, "*Robos y Estafas: Crecen los Delitos en la Web y las Leyes no se Actualizan*" [Thefts and Cons: Crimes on the Web Go Up and There is No Law Actualization," *Clarin*, February 3, 2012, http://www.clarin.com/policiales/Crecen-delitos-Web-leyes-actualizan_0_859114221.html.

[101] Project authorized by Resolution 501/12 of the General Prosecutor's Office, http://www.mpf.jusbaires.gov.ar/wp-content/uploads/resolucion-fg-nc2ba-501-12-equipo-fiscal-a-uf-este-delitos-y-contravenciones-informaticas-sin-act-int.pdf.

[102] "*Una Fiscalía Dedicada a los Delitos Informáticos*" [A Prosecutor's Office Dedicated to Cyber-Crime], *Clarin*, February 3, 2012, http://www.clarin.com/policiales/fiscalia-dedicada-delitos-informaticos_0_859114224.html.

ARMENIA

	2012	2013
INTERNET FREEDOM STATUS	**N/A**	**FREE**
Obstacles to Access (0-25)	n/a	8
Limits on Content (0-35)	n/a	9
Violations of User Rights (0-40)	n/a	12
Total (0-100)	**n/a**	**29**

* 0=most free, 100=least free

POPULATION: 3.3 million
INTERNET PENETRATION 2012: 39 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Internet access in Armenia significantly increased over the past few years due to decreased cost of connectivity and improved network coverage, though internet use remains somewhat low in comparison to other countries in the region (see **OBSTACLES TO ACCESS**).
- New amendments to the Law on Electronic Communication removed the requirement for internet and mobile phone service providers to obtain a license from the regulatory authority before operating (see **OBSTACLES TO ACCESS**).
- Crowdsourcing websites such as iDitord.org were used to monitor election violations during the 2012 parliamentary elections (see **LIMITS ON CONTENT**).

INTRODUCTION

Access to the internet in Armenia has significantly improved over the past few years, with the internet penetration rate increasing from approximately 6 percent in 2007 to 39 percent in 2012. At the same time, however, there have been minimal efforts to improve community access to the internet and digital literacy remains somewhat low, with television remaining the predominant source by which people receive news and information.

In the wake of riots and protests after the 2008 disputed presidential election, the government declared a state of emergency and imposed a media blackout, forcing the removal of the domain name registration of several websites hosted within Armenia, including several opposition sites and independent news outlets. Since this one incident in 2008, however, the government has engaged in minimal blocking or deletion of online content.

In May 2010, the Armenian National Assembly passed amendments to the administrative and penal code to decriminalize defamation, including libel and insult. The initial result was an increase in civil cases of defamation, often with large fines as penalties. In November 2011, the Constitutional Court ruled that courts should avoid imposing large fines on media outlets in defamation cases, resulting in a subsequent decrease in the number of defamation cases.

OBSTACLES TO ACCESS

Internet access in Armenia has increased substantially, particularly in the past few years. According to the International Telecommunication Union, the internet penetration rate in Armenia stood at 39.2 percent in 2012, compared to 32 percent in 2011 and just 6 percent in 2007.[1] From 2005 to 2007, the Armenian government undertook radical steps toward the liberalization of the information and communications technology (ICT) sector, which involved introducing a new regulatory framework that eliminated the existing telecommunication company's monopoly over the market. Today, the telecommunications sector in Armenia is relatively liberal, but still not mature enough to meet the market demands and communication needs of the entire population. A primary obstacle is the absence of diverse services available in rural areas and small cities, due to operators' lack of interest in the development of unprofitable areas. Nevertheless, access to mobile broadband is available throughout the majority of the country and is affordable for much of the population. Mobile broadband tariffs limitations[2] and less reliable wireless connectivity (compared with landline services) are also problems in the telecommunication infrastructure in Armenia, though to a lesser degree. Landline broadband access provided using ADSL technology is available in most cities and some villages.

[1] International Telecommunication Union (ITU), "Percentage of individuals using the Internet," 2006, 2011 & 2012, accessed June 25, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[2] Known as fair use policy: widely used by mobile operators and provides guaranteed speed for limited data volume (usually 1GB – 10GB) and reduced speed (usually 14.4 Kbit/sec) after exceeding the limit.

The market for internet access in Armenia is concentrated in the capital city of Yerevan, which contains one third of the country's population. ISPs offer bandwidth connections with speeds varying from 512 Kbps to 50 Mbps.[3] All three mobile operators offer 2G and 3G networks (EDGE, UMTS/WCDMA) and one operator offers 4G network services (LTE), but only in the capital city. In contrast to Yerevan's diverse market, only one or two mobile broadband services are usually available in villages and approximately 60 percent of rural towns are covered by landline broadband. According to official information from mobile operators,[4] 3G services are available to almost 90 percent of the population, covering 85 percent of the country. The total number of mobile broadband subscribers in Armenia is about 210,000, in addition to 195,000 landline connections, accounting for approximately 45 percent of households or 13 percent of the population.[5] The number of dial-up connections in Armenia has rapidly decreased during the last five years and by the end of 2012 there were fewer than 2,500 users.

Strong competition among the three primary mobile service providers and internet service providers in Armenia has resulted in fair market prices for both wireless and landline broadband services. ADSL connections with speeds of 1Mbps are available for $11 per month and the price for a minimal volume (3GB) package of mobile broadband service costs $15 per month. Internet costs are relatively high when compared to the minimum salary in Armenia, which is $80 per month. At the same time, considering that the average public utilities bill can vary from $50 to $100 in the summer and $100 to $200 in the winter, the cost of internet access is affordable for the majority of the population, whose average income is approximately $600 per month. Additionally, the availability of free access points in the capital and almost all major cities makes internet services accessible for the majority of the urban population.

From 2005 to 2010, a number of nonprofit and community organizations implemented a series of projects aimed at establishing free public internet access centers. In particular, Project Harmony connected all Armenian schools to the internet with financial support from the U.S. State Department, Open Society Institute, and later from the World Bank.[6] Currently, this project is funded from the state budget. Another large-scale internet connectivity project has been implemented by the UNDP mission in Armenia. Recently, the municipality of Yerevan launched free public internet access points that are available throughout a significant portion of the city, in addition to universities and schools. Mobile operators also provide limited access in public spaces such as cafes and public transportation. Public access centers have now been launched in 11 cities, the centers of each of the Armenia's administrative districts (*marzes*).[7]

In practice, the Armenian government and the telecommunication regulatory authority, the Public Services Regulation Commission (PSRC), do not interfere with or try to influence the planning of

[3] MTS, "Internet Express Tariff Plans," accessed July 30, 2013, http://mts.am/en/individual-customers/internet-and-tv/internet-express-%284g%29/-internet-express-tariff-plan.
[4] This information was derived from reports published on several mobile operators' websites, including MTS (http://www.mts.am), Beeline (http://www.beeline.am), and Orange Armenia (http://www.orangearmenia.am).
[5] This number indicates only large screen (notebooks, netbooks, computers and tablets) service packages and does not include small screen (mobile phones and smart phones) users of broadband connectivity.
[6] Project Harmony, "Armenia School Connectivity Program," accessed July 30, 2013, http://www.ph-int.org/what_we/pr58/.
[7] Armenian territorial divisions include 10 *marzes* and Yerevan, the capital of Armenia, which also has a status of *marz*.

network topology. Operators plan and develop their networks without any coordination with either the government or the regulatory authority. Moreover, the regulatory authority requires service providers to indicate any technological restrictions in their public offers. Armenian internet users enjoy access to internet resources without limitation, including peer-to-peer networks, voice and instant messaging services such as Skype and Google Talk, and popular social networks such as Facebook, YouTube, and LiveJournal.

The regulatory authorities in Armenia primarily focus on companies with significant market power. Armenia was one of the first post-Soviet countries to privatize telecommunication companies. In 1997, the incumbent Armenian operator was sold to a Greek state-owned company with a 13-year monopoly on basic telephone and international data transmission services, including internet. In 2005, however, the Armenian government revised the incumbent's license and granted a second GSM license; by 2007, all exclusive rights of the incumbent had been abolished. Since then, Armenian users can choose from three mobile service operators and more than 100 ISPs, though analysis of service providers' official reports shows that the five leading operators together control approximately 90 percent of the internet market.

Armenian legislation requires that providers obtain a license for either the provision of internet services or the operation of a telecommunication network.[8] Procedures for obtaining licenses differ: a service license is obtained through a simplified licensing procedure (purchased for an amount equivalent to approximately $250), while a network operation license requires verifying the professional and technical capacity of the company and is issued six months after filing the application with the regulatory authority. In 2012, the Armenian government undertook radical reforms of the telecommunication regulatory framework to simplify the market entry procedures of both network operation and services. According to the recently adopted Amendments to the Law on Electronic Communication, service providers will no longer be required to obtain a license but will simply need to notify the regulatory authority.[9]

Public access points such as cafes, libraries, schools, universities, and community centers are not required to obtain a license for offering internet access unless they offer services for a fee. In general, according to the Licensing Law, nonprofit entities are not required to obtain a license for the provision of internet services regardless of their legal status.[10] It is worth noting that both for-profit and nonprofit service providers in Armenia enjoy free use of the low-energy Wi-Fi spectrum: use of 2.4 GHz frequency does not require permission unless it exceeds 0.1 watts of power. However, the use of 2.4 GHz for more powerful devices requires permission granted without auction or tender, but taking into account electromagnetic compatibility with other devices in range.

[8] Article 15 of Law of the Republic of Armenia on Electronic Communication, adopted by the national assembly on July 8, 2005. Public Services Regulatory Commission of the Republic of Armenia, "Law on Electronic Communication," http://psrc.am/en/?nid=69.

[9] Law of the Republic of Armenia on Changes and Amendments to the Law on Electronic Communication. Adopted on April 29, 2013, entered into the legal force on June 15, 2013. Official Bulletin No 05/29(969), June 5, 2013.

[10] Article 43 of the Law of the Republic of Armenia on Licensing. Adopted by the National Assembly of the Republic of Armenia on May 30, 2001 with several amendments from 2002-2012.

Mobile telecommunication companies are granted a license through regular network operation licensing procedures, but are also required to obtain permission for the use of radio frequencies, which is usually granted through an open auction. An exception can be made if no alternative applicant is interested in a particular frequency, or for frequencies and equipment that do not interfere with other operators' activities (such as radio relay communication). For cases in which an entity applies for a non-auctioned frequency, the service provider is required to carry out a test for electromagnetic compatibility.

The concept of an independent regulatory authority was implemented in Armenia in 2006 with the adoption of the Law on Electronic Communication, which was developed with substantial expert contribution from the World Bank, as well from U.S. and European Union consultants. Armenia has chosen a multi-sector regulatory model in which there is one body, the PSRC, which is in charge of the regulation of energy, water supply, and telecommunications services. The PSRC's authority, mechanisms of commissioners' appointments, and budgeting principles are defined under the Law on State Commission for the Regulation of Public Services.[11]

The members or commissioners of the PSRC are appointed by the President of the Republic of Armenia according to the recommendations of the Prime Minister. Once appointed, a commissioner can be dismissed only if he or she is convicted of a crime, fails to perform his or her professional duties, or violates other restrictions in the law, such as obtaining shares of regulated companies or missing more than five PSRC meetings. In cases of dismissal for professional failure, the PSRC makes a decision and reports to the President of the Republic of Armenia for action. The PSRC is accountable to the National Assembly in the form of an annual report, but the parliament merely takes this report into consideration and cannot take any action.

One of the weakest provisions of the Armenian regulatory framework is the absence of term limits for commissioners: every commissioner can be appointed multiple times, making his or her appointment dependent on current political leaders. In practice, the regulatory bodies in Armenia lack independence due to the strong dependence of the commissioners' career on political leadership of the country.[12] For example, in 1995, the broadcasting license of the independent television company A1+ was suspended for refusing to broadcast only pro-government material, and in 2002 its broadcasting frequency was awarded to another company. Despite a ruling by the European Court of Human Rights in 2008 which stated that the regulatory authority's refusal to reinstate the company's broadcasting license amounted to a violation of freedom of information, the license was never reinstated.[13] In September 2012, A1+ began broadcasting on the airwaves of Armnews. During this time, A1+ was nonetheless able to continue publishing news content on its website.

[11] The Law on Public Services Regulation Commission was adopted by the National Assembly of the Republic of Armenia on December 25, 2003.
[12] There are three independent regulatory authorities in Armenia that are part of executive, but not a part of government. These three authorities are the public utilities regulator, the broadcasting regulator, and the competition authority. There is also a civil service commission, which, however, is different from the concept of independent regulatory bodies.
[13] Case No32283/04, Meltex LTD and Mesrop Movsesyan vs. Armenia, June 7, 2008, http://echr.coe.int/Documents/CLIN_2008_06_109_ENG_843572.pdf

The Commission's budget is formed in accordance with the Law on Public Service Regulation Commission and is composed of licensing and regulatory fees that companies pay to the state budget. The amount of regulatory fees is defined by the Commission in accordance with the procedure set up under the relevant provision of the law. The Law on Electronic Communication contains provisions guaranteeing the transparency of the decision-making procedures of the Commission: all decisions are made during open meetings with prior notification and requests for comments from all interested persons posted on the website.[14]

In spite of three well-established ICT-related nonprofit associations, self-regulation of the industry is significantly underdeveloped in Armenia. The oldest nonprofit institution is the Internet Society (ISOC), which is the national chapter of the worldwide ISOC network. At the early stage of internet development in Armenia (1995 through 1998), ISOC Armenia was a primary internet policy advocate and industry promoter. It served as a forum where internet service providers discussed their problems, developed policy agendas, and resolved industry conflicts. However, after the establishment of the independent regulatory authority, ISOC no longer plays a self-regulating role as most industry disputes are filed with the PSRC . Nevertheless, ISOC continues to maintain the registration of domain names, and in spite of lacking formal dispute resolution policies (such as, for example, domain name disputes resolution procedures), it carries out the registry function effectively with minimal influence from government authorities and the regulator.

The Armenian ICT market enjoys a liberal and non-discriminatory domain name registration regime. ISOC Armenia registers domain names according to ICANN recommendations and best practices. Although formally, members of the Armenian Internet Society are individuals, the organization's board is composed of service providers' managers and in general, the Society's policy agenda is strongly influenced by the interests of traditional providers that started their business in the mid-1990s.

Another well-established industry association is the Union of Information Technologies Enterprises (UITE).[15] Though industry self-regulation is one of the main goals of the Union, so far it has not developed any significant policies for industry regulation. Both ISOC Armenia and UITE are founders of a third notable nonprofit institution, the ArmEx Foundation, which was established with the sole purpose of creating a local data traffic exchange point. Other founders include leading ISPs, mobile and landline telecommunication operators.

LIMITS ON CONTENT

The Armenian government does not consistently or pervasively block users' access to content online. The only significant case of internet filtering and blocking was recorded in March 2008 during post-elections events, immediately after clashes between an opposition rally and police

[14] Article 11 of the Law of the Republic of Armenia on Public Service Regulation Commission.
[15] "UITE History," Union of Information Technology Enterprises, accessed July 30, 2013, http://uite.org/en/about-us/uite-history.

resulted in at least eight people killed and hundreds of people injured.[16] The government declared a state of emergency and restricted certain media publications, including independent internet news outlets. The security services demanded that the Armenian domain name registrar suspend the domain names of opposition and independent news sites, and requested that ISPs block certain outside resources, such as some opposition pages on social network platforms (particularly LiveJournal, which was the most popular social network used by opposition and civil society activists for blogging and reporting). Armenian authorities were strongly criticized by international observers for their reaction to the post-elections crisis, including the restriction of the access to internet resources.[17] After the events of 2008, Armenian authorities have been very careful regarding restrictions on internet access and no instances of politically-motivated filtering or blocking have been recorded since that time.

In spite of the fact that according to Article 11 of the Law on Police,[18] law enforcement authorities have the right to block particular content to prevent criminal activity, in practice, such blocking cases have been limited to locally-hosted, illegal content such as illegal pornography and copyright-infringing materials. Service providers involved in the transferring or provision of technical access to illegal resources (such as child pornography, propaganda of crime or cyberterrorism) are not liable for content they make available to their customers provided that they have no prior knowledge of the content. Any decision of a law enforcement body to block particular content can be challenged in court by the resource or content owners, and if the court rules that the measure was illegal or unnecessary, the resource and content owners may claim compensation. Additionally, Armenia is a member of the European Human Rights Convention; therefore, any such decision can also be challenged at the European Court of Human Rights.

Currently, self-censorship is not a widespread practice online. The Armenian government and ruling political elite have avoided the application of any extralegal measures to prevent political opponents or independent internet resources from publishing particular online content. However, similar to traditional media outlets such as television or printed press, Armenian internet news resources are exposed to political pressure. In some cases, for example, journalists of a particular online media outlet are not allowed to deviate from the editorial policy of the outlet, which is often linked to one of the political parties. Such pressure has the potential to affect the overall situation of freedom of speech in the country, but it is worth noting that online publishers and individual bloggers strongly resist self-censorship. Indeed, there is a wide diversity of opinion in social media and virtual battles between pro- and anti-government bloggers are often observed. A variety of independent and opposition web resources provide Armenian internet audiences with politically

[16] Reports on the number of people killed vary; according to the official report from the Council of Europe, eight people were killed. "Special Mission to Armenia," Council of Europe Commissioner for Human Rights, March 12-15, 2008, https://wcd.coe.int/ViewDoc.jsp?id=1265025.

[17] "Observation of the Presidential Election in Armenia," Parliamentary Assembly of the Council of Europe, February 19, 2008, http://www.assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=11961&Language=EN.

[18] According to the Article 11 of the Law of the Republic of Armenia on Police (adopted on 16 April 2001, Official Bulleting No 15(147) of 31 May 2001) the police authorities have a general obligation to undertake measures to prevent crime.

non-biased, neutral, or oppositional opinions, and there are only a few state-owned media enterprises in Armenia.[19]

The Armenian government is very cautious about media freedom issues and tries to avoid direct pressure that may raise criticism from international organizations and local civil society activists. However, both the ruling political elite and the opposition party do have some influence over traditional and new media outlets. According to accounts from media professionals and civil society activists, most media outlets are either linked with a particular political party or periodically receive financial support from politicians, aside from two or three online media resources funded by foreign and international donor organizations.[20] However, the extent to which this has a direct influence over the content of these media outlets cannot be easily assessed.

The financial model of Armenian online news resources is very similar to the model of the traditional print and broadcast media, in that the political elite may lend support to certain outlets through the channeling of advertising of government-loyal businesses. At the same time, websites such as the A1+ news editorial (A1plus.am) and Lragir Daily (Lragir.am), both of which publish articles that are critical of the government, are quite popular and have been able to survive economically. There are neither formal nor practical barriers to receiving domestic or foreign aid or advertisements, but foreign financial support is usually limited to modest grants and foreign advertisers are usually not interested in the Armenian media market. A significant part of advertising comes from mobile operators, car dealers, and consumer electronics sellers.

Armenian telecommunication regulations conform to the principles of technological neutrality, meaning that regulations address legal issues rather than the use of a particular technology, service type, or conditions. Naturally, some laws and regulations contain recommendations or applicable standards, but there are no technology restrictions on bandwidth, protocols, or routing.

The emergence of online media has caused a significant increase in journalistic activities in Armenia. Armenian media has traditionally been economically unsustainable due to the limited audience, high operational costs, and small advertising market. Even at the peak of media production in Armenia, daily newspapers usually published around 5,000 copies per day and few weekly outlets had more than 10,000 readers.[21] The audience for television and radio was larger, but still limited to the leading producers: five of the almost thirty television channels accounted for 76 percent of viewers.[22] Early online news outlets such as A1+ enjoyed significant growth in the number of daily visitors during the first few years of production.

Armenian online news resources started growing from 2001 to 2005 when internet service became relatively affordable. However, the main increase in production of online content—particularly

[19] The only state owned newspaper is *Hayastani Hanrapetutyun* ("Republic Armenia"), which publishes governmental and private announcements and the Official Bulletin (also publishes the Bulletin of Government). There is also a news website for publishing general announcements and procurement information of the government, www.azdarar.am.
[20] Based on interviews carried out with representative of Internews Armenia and the Center for Information Law and Policy.
[21] 1996–1998 could be referred to as a peak of Armenian post-Soviet print press production according to press activities and establishment of new press enterprises. Afterward the development of both television and press slowed down significantly.
[22] AGB Nielsen Media Research, Armenia, 2011, http://www.agbnielsen.am/.

video and audio content—started in 2008 after the liberalization of the market and the decrease in the cost of broadband. Today, there are at least 30 leading online news outlets collecting more than 20,000 daily visitors—four times more than the leading press outlet—and covering political, economic, and social issues. Since 2011, Armenia has seen the emergence of Armenian-language online television programs. Although online video news services are still underdeveloped and underused in Armenia, the public's interest toward online video content is growing, and today at least two leading web resources, Civilnet.am and Azatutyun.am, offer on-demand video news and live-air reporting on major political and social events.

As of May 2013, there were more than 225 online media outlets and traditional media webpages registered in Armenia.[23] Generally speaking, there are no formal or technical restrictions to accessing different internet resources with diverse opinions. However, the extent to which a particular news resource is well-known often depends on the financial support it receives. In other words, despite the ability to access different outlets, choice is often predetermined by the ratings and popularity of a given media outlet, which depend on investments that are usually political in nature.

The majority of the population uses the internet mainly for social networking and as a less-expensive alternative for voice and visual communication with relatives abroad. While those who use the internet in Armenia mainly visit news websites or social networks, given the overall low levels of daily internet use among the Armenian population, most Armenians still receive their news from television programs.[24] Nevertheless, the population's interest toward internet news resources is growing, and the number of visitors to the leading news websites exceeds the number of the leading newspapers' readers.[25] Print copies of the leading Armenian newspapers—*Aravot*, *Hraparak*, and *Iravunk*—usually do not exceed 5,000 issues, whereas online news websites collect more than 50,000 unique visitors per day. At the same time, the audience for television and radio is still larger than that of online news and video programming due to the absence of unified technical solutions.[26]

Armenian online communities, especially blogs, are highly politicized and are likely to respond to most political events. During the last three years, social media—Facebook in particular—has been actively used for political and civil mobilization by the opposition and civil society activists. For example, environmental activists have used internet resources for environmental alerts such as forest cutting or illegal construction in green areas.[27] Another positive example of online mobilization is the iDitord (iObserver) project, a crowdsourced election monitoring project

[23] "Armenian web resources rating," Circle.am, accessed June 26, 2013, http://circle.am/?cat=news&for=today&by=visits.
[24] Most of the top 10 websites in Armenia are either online news services or television news video portals. "Armenian web resource ratings," Circle.am, accessed July 30, 2013, http://circle.am/.
[25] "Armenian web resource ratings," Circle.am.
[26] According to interviews with Armenian media and telecommunication experts, such as the staff at Internews Armenia and the Center for Information Law and Policy, there are two major obstacles for penetration of online video and television: legislative barriers preventing telecommunication operators with foreign capital from carrying out broadcasting activities, and the lack of unified technical solutions for IPTV subscriptions.
[27] "Save the trees: trees without borders," accessed July 30, 2013, http://kanach.am/.

launched in advance of the May 2012 parliamentary elections.[28] The website received more than 1,000 reports from citizens, NGOs, and political parties, mostly related to bribes, problems with the activities of local electoral commissions, violations of advertisement laws, and mistakes in electoral lists. The police and the Central Electoral Commission officially responded to some reports and claimed that others were not confirmed or were misinformed. In contrast, mobile phones (bulk SMS or voice messages) are not used during political campaigns due to the limited peak capacity of networks.

VIOLATIONS OF USER RIGHTS

Article 27 of the Constitution of the Republic of Armenia guarantees freedom of speech irrespective of the source, person, and place. The right to freedom of speech declared in the constitution is universal and applicable to both individuals and media editorials. In 2005, Armenian media legislation changed significantly with the adoption of the Law of the Republic of Armenia on Mass Media[29] (also referred to as the Media Law). One the most positive changes in Armenian media legislation was the adoption of unified regulation for all types of media content irrespective of audience, technical means, and dissemination mechanisms. The Television and Radio Law contains additional requirements toward content delivery, but it does not regulate news delivery and only addresses the issues of broadcasting erotic and horror programs, as well as the time frame for advertising, the mandatory broadcast of official communications, and the rules on election coverage and other political campaigns. Content delivered thorough a mobile broadcasting platform or the internet are not subject to specific regulation.

Armenian criminal legislation grants journalists protection of their professional rights. According to Article 164 of the Criminal Code of the Republic of Armenia, "hindrance to the legal professional activities of a journalist, or forcing the journalist to disseminate information or not to disseminate information, is punished with a fine in the amount of 50-150 minimal salaries, or correctional labor for up to 1 year. The same actions committed by an official abusing one's official position, is punished with correctional labor for up to 2 years, or imprisonment for the term of up to 3 years, by deprivation of the right to hold certain posts or practice certain activities for up to 3 years." [30] However, neither criminal law nor media legislation clearly defines who qualifies as a journalist, whether he or she must be an employee of a media outlet, or if he or she could be an individual or freelance reporter or a blogger.

In 2010, Armenia abolished criminal liability for insult and slander[31] and introduced the concept of moral damage compensation for public defamation.[32] However, even before these amendments, no

[28] "Armenian elections monitoring: Crowdsourcing + public journalism + mapping," Internews, August 28, 2012, https://innovation.internews.org/blogs/armenian-elections-monitoring-crowdsourcing-public-journalism-mapping.
[29] The Law of the Republic of Armenia on Mass Media. Adopted by National Assembly on December 13, 2003. Official Bulletin 29 January 2004 No 29/6(25).
[30] Article 164, Criminal Code of the Republic of Armenia as amended on January 6, 2006.
[31] Official Bulletin of the Republic of Armenia 2 May 2003, No 25(260).
[32] Concept of compensation for moral damage caused by defamation was introduced by adding Article 1087.1 to the Civil Code of the Republic of Armenia. Official Bulletin of the Republic of Armenia 23 June 2010 No 28(762).

criminal cases against journalists were recorded since the adoption of a new criminal code in 2003. Defamation is widely used by Armenian politicians to restrict public criticism, but it has not necessarily been used to combat oppositional viewpoints or media independence. However, the principle of requiring politicians to be more tolerant of public criticism is not a widely adopted legal practice in Armenia.

Since 2003, when the concept of cybercrime was first introduced in the Armenian criminal code,[33] criminal prosecution for crimes such as illegal pornography or copyright infringements on the internet demonstrates that Armenian law enforcement authorities follow the best practices of the European legal system, and neither service providers nor hosting service owners have been found liable for illegal content stored on or transmitted through their system without their actual knowledge of such content. Armenia is a signatory to the Council of Europe's Convention on Cybercrime and further development of Armenian cybercrime legislation has followed the principles declared in the Convention.

Armenian criminal legislation also prohibits the dissemination of expressions calling for racial, national, or religious enmity, as well as calls for the destruction of territorial integrity or the overturning of legitimate government or constitutional order.[34] Libeling or insulting an official has not been criminally prosecuted since 2008, when the relevant provision of the criminal code was excluded. As mentioned previously, the Armenian legal system is based on the principle of universality, meaning that laws are applicable online as they are offline. Therefore, all crimes conducted on the internet are prosecuted similarly to those that are conducted elsewhere. Regarding liability for content published on websites hosted in other jurisdictions, Armenian legal theory and practice follows the principle of "place of presence," meaning that the person is liable if he or she acts on the territory of that country.

So far no cases have been recorded of imprisonment or other criminal sanctions or punishments for individuals accessing or disseminating information online. However, cases of civil liability, such as moral damages compensation for defamation, have been recorded several times.[35] The downloading of illegal materials or copyrighted publications is not prosecuted under Armenian legislation unless it is downloaded and stored for further dissemination, and the intention to disseminate must be proved.

Anonymous communication is not prohibited in Armenia; however, it is up to the website administrator to allow or prohibit anonymous communication to or from a resource. No registration is required for bloggers and online media outlets, though tax authorities may question bloggers or media outlets on revenue-related issues (advertisements or paid access). The use of encryption software by individuals or corporate users is not prohibited. However, the use of proxy

[33] Cybercrime was defined under the new Criminal Code of the Republic of Armenia, adopted on April 18, 2003. The first prosecution case for the dissemination of illegal pornography via the internet was recorded in 2004.
[34] Articles 226 and 301 of the Criminal Code of the Republic of Armenia.
[35] "Demanding Financial Compensation from Armenian News Outlets is Becoming Trendy," Media.am, March 3, 2011, http://media.am/en/media-attacks.

servers is not that common, due to the fact that since 2008, internet users have not faced significant problems with website blocking and traffic filtering.

The collection of an individual's personal data by the government is allowed only in accordance with a court decision in cases proscribed by the law. The monitoring and storing of customers' data is illegal unless it is required for the provision of services. Personal data can be accessed by law enforcement bodies only in accordance with a court decision; however, in most cases courts usually support requests from law enforcement bodies for data retention. Law enforcement bodies usually file motions on data retention while investigating crimes; however, motions must be justified, and if not, the defense attorney may insist on the exclusion of evidence obtained as a result of such action.

Armenian legislation does not require access and hosting service providers to monitor transmitted traffic or hosted resources. Moreover, the Law on Electronic Communication allows operators and service providers to store only data required for correct billing. Cybercafes and other access points are not required to identify clients, or to monitor or store their data and traffic information.

Cases of physical violence towards online journalists or other staff have not been recorded, though such cases have happened with journalists from traditional media outlets.

DDoS attacks were not prevalent in Armenia until the start of the campaign period for the 2012 parliamentary elections. Blognews.am, an Armenian blogosphere aggregator, was attacked on the morning of April 20, 2012. Later, the iDitord.org website that covered election violations suffered from a DDoS attack. As a result, iDitord.org went down for several hours on the day of polling; however, as a result of external DDoS mitigation services, the website was able to resume normal functioning after four hours of inaccessibility while attacks continued. The culprits of the DDoS attack are still unknown. Interestingly, during election day, iDitord was the only Armenian web site which came under DDoS attack.[36] Additionally, during the presidential election on February 18, 2013, the opposition media website Galatav.am suffered from a DDoS attack.[37]

[36] "DDoS attacks becoming customary in Armenia?" Media.am, May 8, 2012, http://m.media.am/en/DDos-attacks-on-websites.
[37] "Website of Gala TV undergoes DDoS attack," ArmInfo, February 18, 2013, http://arminfo.am/index.cfm?objectid=A313ACE0-79EA-11E2-83EBF6327207157C.

AUSTRALIA

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	2	2
Limits on Content (0-35)	5	5
Violations of User Rights (0-40)	10	11
Total (0-100)	17†	18

* 0=most free, 100=least free

POPULATION: 22 million
INTERNET PENETRATION 2012: 82 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Broadband access continued to expand for online users as the National Broadband Network reached more rural and remote communities (see **OBSTACLES TO ACCESS**).
- Concerns over ISP filtering practices continued, as it was revealed that a number of legitimate websites were accidentally blocked by ISPs who were trying to limit access to a fraudulent website with the same IP address (see **LIMITS ON CONTENT**).
- Australia's accession to the Council of Europe's Convention on Cybercrime in 2012 raised concerns about additional requirements in the Australian legislation for ISPs to monitor and store user data, especially in regard to the requirement to comply with foreign preservation notices (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Australia enjoys affordable, high-quality access to the internet and other digital media, and this access has continued to expand over the past few years with the rollout of the National Broadband Network. However, recent amendments to surveillance legislation and proposals to implement censorship through directives to internet service providers (ISPs) have raised concerns about privacy and freedom of expression.[1] Although not currently law, there have been a number of proposals put forward on data retention, surveillance, and filtering in the course of the last two years.

Additionally, in late 2012 Australia acceded to the Council of Europe's Convention on Cybercrime, which brought into effect a number of obligations for ISPs to monitor, preserve, and store user data. However, the Australian legislation goes beyond the requirements set out in the Convention by requiring longer retention timelines for foreign preservation notices, and requiring ISPs to cooperate with any serious crime being investigated in Australia or overseas.

OBSTACLES TO ACCESS

In 1989, Australia's Academic and Research Network (AARNet) made the country's first internet connection with a 56 Kbps satellite link between the University of Melbourne and the University of Hawaii.[2] Today, the same connection to the United States is 200,000 times faster, and with the development of the high-speed National Broadband Network (NBN) in 2012,[3] all Australians, including those in more remote areas, will soon have access to an internet connection with a peak speed of at least 12 Mbps for its mixed network (fiber, wireless and satellite technology), while the fiber product will offer speeds from 100 Mbps to 1 Gbps.[4]

Australia has an internet penetration rate of approximately 82 percent as of December 2012, according to the International Telecommunication Union.[5] There were 12.2 million internet subscribers in Australia in December 2012 (excluding internet connections enabled through mobile phone handsets) and 17.4 million mobile handset subscribers.[6] The internet penetration rate is

† The 2012 rating for Australia was adjusted on the basis of updated scoring guidelines to best convey changes over time.

[1] For a comprehensive overview of the legislative history of censorship in Australia see Libertus.net, "Australia's Internet Censorship System," accessed June 2010, http://libertus.net/censor/netcensor.html. See also Australian Privacy Foundation, accessed June 2010, http://www.privacy.org.au.

[2] Australia's Academic and Research Network (AARNet), "AARNet Salutes the 20th Anniversary of the Internet in Australia," news release, November 26, 2009, http://www.aarnet.edu.au/Article/NewsDetail.aspx?id=173;
Roger Clarke, "A Brief History of the Internet in Australia," May 5, 2001, http://www.rogerclarke.com/II/OzIHist.html;
Roger Clarke, "Origins and Nature of the Internet in Australia," January 29, 2004, http://www.rogerclarke.com/II/OzI04.html.

[3] Australian Government, Department of Broadband, Communications and the Digital Economy, "National Broadband Network," accessed March 2012, http://www.dbcde.gov.au/broadband/national_broadband_network.

[4] NBN Co., "National Broadband Network," accessed January 10, 2013, http://bit.ly/16U3Qvt.

[5] International Telecommunication Union, "Percentage of Individuals Using the Internet," accessed July 15, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[6] Australian Bureau of Statistics, "Internet Activity, Australia," December 2012, http://bit.ly/18eYL3I.

expected to steadily increase with the implementation of the NBN, which includes expanded wireless and satellite services in rural communities. Although internet access is widely available in locations such as libraries, educational institutions, and internet cafes, Australians predominantly access the internet from home, work, and increasingly through mobile phones.

Access to the internet and other digital media is widespread in Australia. Australians have a number of internet connection options, including ADSL, ADSL 2+, wireless, cable, satellite, and dial-up.[7] Wireless systems can reach 99 percent of the population, while satellite capabilities are able to reach 100 percent. While the internet service provided by these systems can be slow, the expansion of the NBN means that all Australians will have access to high internet speeds. Major ISPs such as Telstra offer financial assistance for internet connections to low-income families.[8] The phasing out of dial-up continues, with nearly 90 percent of internet connections now provided through other means. Once implemented, the NBN will eliminate the need for any remaining dial-up connections and make high-speed broadband available to Australians in remote and rural areas.[9]

Age is a significant indicator of internet use, with 69 percent of Australians between the ages of 18 and 24 accessing the internet at home on a daily basis and 75 percent of people 15 years or over reporting having used the internet over a 12 month period.[10] By contrast, only 31 percent of those 65 years and over had used the internet in the same 12 months.[11]

Approximately 50 percent of Aboriginal and Torres Strait Islanders living in discrete indigenous communities (i.e. not major cities) have access to the internet, with 36 percent having internet access in the home.[12] In remote indigenous communities, 63 percent of the population had taken up mobile phone services in 2004.[13] However, not all indigenous communities have mobile phone coverage; the overall mobile phone penetration rate in Aboriginal communities is unknown.

Australia has a mobile phone penetration rate of 106 percent, with many consumers using more than one SIM card or mobile phone.[14] Third generation (3G) mobile services are the driving force behind the recent growth, with 24.3 million mobile subscriptions operating in 2012.[15]

---

[7] Australian Communications and Media Authority (ACMA), *Communications Report, 2008–09* (Canberra: ACMA, 2009), http://www.acma.gov.au/webwr/_assets/main/lib311252/08-09_comms_report.pdf.
Australian Communications and Media Authority (ACMA), *Communications Report, 2010-11* (Canberra: ACMA, 2011), http://www.acma.gov.au/webwr/_assets/main/lib410148/communications_report_2010-11.pdf.
[8] Telstra, *Telstra Sustainability Report 2011,* accessed March 2013, http://bit.ly/1dPRUQw.
[9] Australian Government National Broadband Network, "NBN Key Questions and Answers," accessed June 2010. http://www.nbn.gov.au/content/nbn-key-questions-and-answers-faqs.
[10] Australian Bureau of Statistics, "Online @ Home," accessed March 2012, http://bit.ly/mnrJiG.
[11] Ibid.
[12] Australian Bureau of Statistics, "Internet Access at Home," accessed October 2010, http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4102.0Chapter10002008. For a comprehensive report on indigenous internet use and access, see ACMA, Telecommunications in Remote Indigenous Communities (Canberra: ACMA, 2008), accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311397.
[13] Australian Communications and Media Authority (ACMA), *Communications Report, 2008-2009* (Canberra: ACMA, 2008-2009), http://www.acma.gov.au/webwr/_assets/main/lib311252/08-09_comms_report.pdf. There is no equivalent data on indigenous communities in the more recent 2011-2012 report.
[14] International Telecommunication Union, "Mobile-cellular telephone subscriptions," accessed July 15, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Internet access is affordable for most Australians. The government subsidizes satellite phones and internet connections for individuals and small businesses in remote and rural areas, where internet affordability is not comparable to that in metropolitan areas.[16]

The government has adopted a strong policy of technological neutrality, also referred to as net neutrality. There are no limits to the amount of bandwidth that ISPs can supply. While the government does not place restrictions on bandwidth, ISPs are free to adopt internal market practices of traffic shaping. Some Australian ISPs and mobile service providers practice traffic shaping (also known as data shaping) under what are known as fair-use policies. If a customer is a heavy peer-to-peer user, the internet connectivity for those activities will be slowed down to free bandwidth for other applications.[17]

Like most other industrialized nations, Australia hosts a competitive market for internet access, with 81 medium-to-large ISPs as of June 2012, as well as a number of smaller ISPs.[18] Many of the latter are "virtual" providers, maintaining only a retail presence and offering end users access through the network facilities of other companies; these providers are carriage service providers and do not require a license.[19] Larger ISPs, which are referred to as carriers, own network infrastructure and are required to obtain a license from the Australian Communications and Media Authority (ACMA) and submit to dispute resolution by the Telecommunications Industry Ombudsman (TIO).[20] Australian ISPs are co-regulated under Schedule 7 of the 1992 Broadcasting Services Act (BSA), meaning there is a combination of regulation by the ACMA and self-regulation by the telecommunications industry.[21] The industry's involvement consists of developing industry standards and codes of practice.[22]

The ACMA is the primary regulator for the internet and mobile telephony, and is responsible for enforcing Australia's anti-spam law.[23] Its oversight is generally viewed as fair and independent, though there are some transparency concerns with regard to the classification of content. Small businesses and residential customers may file complaints about internet, telephone, and mobile-phone services with the TIO,[24] which operates as a free and independent dispute-resolution service.

---

[15] Australian Communications and Media Authority (ACMA), *Communications Report, 2011-2012* (Canberra: ACMA, 2001-2012), http://www.acma.gov.au/webwr/_assets/main/lib550049/comms_report_2011-12.pdf . The Report was tabled to Parliament and released on Dec. 1, 2012.
[16] Rural Broadband, "Welcome," accessed June 2010, http://www.ruralbroadband.com.au.
[17] Telstra, 19.
[18] Australian Bureau of Statistics, "Internet Activity, Australia, June 2012," http://bit.ly/R9RsDo.
[19] Australian Bureau of Statistics, "Internet Activity, Australia, Dec. 2009.", http://bit.ly/1fRWQpZ.
[20] Australia Communications and Media Authority, "Carriage & Service Provider Requirements, accessed March 2013, http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_1622.
[21] Australian Communications and Media Authority Act 2005, http://bit.ly/16U44mm;
Broadcasting Services Act 1992, http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214/;
ACMA, "Service Provider Responsibilities," accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_90157.
[22] Chris Connelly and David Vaile, "Drowning in Codes: An Analysis of Codes of Conduct Applying to Online Activity in Australia," Cyberspace Law and Policy Centre, March 2012, http://cyberlawcentre.org/onlinecodes/report.pdf.
[23] ACMA, "The ACMA Overview," accessed March 2012, http://www.acma.gov.au/WEB/STANDARD/pc=ACMA_ORG_OVIEW;
ACMA, "About communications & media regulation," accessed March 2012,
http://www.acma.gov.au/WEB/STANDARD/pc=PUB_REG_ABOUT.
[24] Telecommunications Industry Ombudsman, accessed March 2012, http://www.tio.com.au.

LIMITS ON CONTENT

Australian law does not currently provide for mandatory blocking or filtering of websites, blogs, chat rooms, or platforms for peer-to-peer file sharing. Access to online content is far-reaching, and Australians are able to explore all facets of political and societal discourse, including information about human rights violations. The ability to openly express dissatisfaction with politicians and to criticize government policies is not hindered by the authorities, and complaints may be sent directly to the Telecommunications Industry Ombudsman.[25] However, the legal guidelines and technical practices by which ISPs filter illegal material on websites have raised some concerns in the past year.

In 2010, the government proposed implementing a mandatory filtering system run through ISPs.[26] Draft legislation was proposed under the Rudd Labour government, and then put aside during the election in August 2010 when a minority government with Julia Gillard of the Labour Party came to power. While the Gillard government had stated that they might introduce legislation on this topic, there have been no formal proposals, bills, or further discussion on the matter since the election. Another election was planned for September 2013, but has been cancelled due to Kevin Rudd winning the Labour Party leadership vote, after which Gillard resigned and Rudd was sworn in as Prime Minister. So far, there have not been any claims by either party to introduce mandatory filtering. Despite the lack of mandatory filtering, ISPs still voluntarily block content from websites that are on Interpol's blacklist and that contain child pornography.

Controversy struck, however, in May 2013 when it was revealed that a number of legitimate Australian websites not hosting any type of illegal or even controversial material had been blocked. Investigations revealed that the Australian Security and Investment Commission was using an obscure provision (section 313) of the Telecommunications Act to request that a fraudulent website be blocked.[27] The notice by ASIC to the ISPs specified an IP address that contained the fraudulent website along with a number of legitimate websites, including that of Melbourne Free University. This is the first known incident of ASIC using s.313 to issue notices to ISPs to block non-Interpol material. The use of section 313 in this matter is highly contentious.

In addition, there are two systems in place that regulate internet content and place some restrictions on what can be viewed online. Under the first system, material deemed by the ACMA to be "prohibited content" is subject to take-down notices. The relevant ISP is notified by the ACMA that it is hosting illicit content, and it is then required to take down the offending material.[28] Under the Broadcasting Services Act, the following categories of online content are prohibited:

---

[25] Ibid.
[26] Alana Maurushat, Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009); ACMA, "Service Provider Filtering", http://www.acma.gov.au/scripts/nc.dll?WEB/STANDARD/1001/pc=PC_90157
[27] LeMay, R., "Interpol Filter Scope Creep: ASIC Ordering Unilateral Website Blocks" (May, 15, 2013), accessed July 16, 2014, http://delimiter.com.au/2013/05/15/interpol-filter-scope-creep-asic-ordering-unilateral-website-blocks/
[28] Internet Society of Australia, "Who Is an Internet Content Host or an Internet Service Provider (and How Is the ABA Going to Notify Them?" accessed June 2010, http://www.isoc-au.org.au/Regulation/WhoisISP.html;

- Any online content that is classified Refused Classification (RC) by the Classification Board, including real depictions of actual sexual activity; child pornography; depictions of bestiality; material containing excessive violence or sexual violence; detailed instruction in crime, violence, or drug use; and material that advocates the commission of a terrorist act.
- Content that is classified R 18+ and not subject to a restricted access system that prevents access by children, including depictions of simulated sexual activity; material containing strong, realistic violence; and other material dealing with intense adult themes.
- Content that is classified MA 15+, provided by a mobile premium service or a service that provides audio or video content upon payment of a fee and that is not subject to a restricted access system, including material containing strong depictions of nudity, implied sexual activity, drug use, or violence; very frequent or very strong coarse language; and other material that is strong in impact.[29]

To date, there have not been any problems with this system of take-down notices being applied to videos, films, literature, or similar material with information of political or social consequence. In addition, the government's general disposition is to allow adults unfettered access to R 18+ materials while protecting children from exposure to inappropriate content.

Under the second system, the ACMA may direct an ISP or content service provider to comply with the Code of Practice developed by the Australian Internet Industry Association (IIA) if the regulator decides that the provider is not already doing so. Failure to comply with such instructions may draw a maximum penalty of AUD 11,000 (approximately USD 11,500) per day. Other regulatory measures require ISPs to offer their customers a family-friendly filtering service.[30] This practice is known as voluntary filtering, since customers must select it as an option.

RC content, including many forms of adult pornography, is generally not unlawful to use, access, possess, or create in Australia merely by virtue of its RC status. Only material that is otherwise legislatively criminalized, such as material depicting child abuse and certain terrorism-related content, is unlawful. Moreover, Australia has no X 18+ or R 18+ category for video and computer games. This means that extremely violent video games beyond the MA 15+ classification level are necessarily categorised as RC.[31] The 1995 Classification Act and the 1992 Broadcasting Services Act were amended in 2012 to now include an R 18+ category for video games. The laws entered into force on January 1, 2013. In the past, the lack of an R 18+ classification for video games led to some peculiar results with games such as *Aliens vs. Predators* initially given an RC classification which

Internet Industry Association, "Guide for Internet Users," March 23, 2008, http://bit.ly/1hfYKP7.

[29] ACMA, "Prohibited Online Content," accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90102.

[30] Internet Industry Association (IIA), *Internet Industry Code of Practice: Content Services Code for Industry Co-Regulation in the Area of Content Services (Pursuant to the Requirements of Schedule 7 of the Broadcasting Services Act 1992), Version 1.0*, 2008, http://www.acma.gov.au/webwr/aba/contentreg/codes/internet/documents/content_services_code_2008.pdf

[31] Libertus.net, "Australia's Internet Censorship System," http://libertus.net/censor/netcensor.html.

was later amended to M 15+.[32] When a game is classified as RC, often the developer will slightly modify the game to ensure it receives either an R 18+or an M 15+ ranking.[33]

The classification system suffers from a lack of transparency; the ACMA does not inform Australian content owners when it issues a take-down notice, and there is no mechanism available for owners or creators to challenge the classification of RC content. Only the ISP or similar intermediary hosting the material may bring a challenge to the Administrative Appeals Tribunal (AAT). In February 2012, the Australian Law Reform Commission released their report on the introduction of a new classification scheme, with recommendations as to how the classification scheme should be amended and clarified.[34] However, none of the report's recommendations are currently being considered by Parliament, and legislation is not expected to be introduced in 2013.

There are no examples of online content manipulation by governments or partisan interest groups. Journalists, commentators, and ordinary users are not subject to censorship so long as their content does not amount to defamation or breach criminal laws, such as those against hate speech or racial vilification.[35] Nevertheless, the need to avoid defamation and, to a lesser extent, contempt of court has been a driver of self-censorship by both the media and ordinary users (see "Violations of User Rights"). For example, narrowly-written suppression orders are often interpreted by the media in an overly broad fashion so as to avoid contempt of court charges.[36]

Aside from the restrictions on prohibited content, the incitement of violence, racial vilification, and defamation, Australians have access to a broad choice of online news sources that express diverse, uncensored political and social viewpoints. Individuals are able to use the internet and other technologies both as sources of information and as tools for mobilization. In August and September of 2012, Australians vocalized their opinions about the Attorney-General's proposal regarding data retention and the introduction of surveillance mechanisms that would store users' online and mobile phone communications for two years. The proposal was immensely unpopular with the industry, civil liberties groups, and general consumers. Groups such as *Getup!* encouraged Australians to send e-mails and twitter messages to Nicola Roxon, the Attorney-General, to voice their concerns over the proposal. As a result of the immense unpopularity of the data retention proposal, Roxon released a video on YouTube in which she attempted to clarify some of the key aspects of the proposal that had been criticized.[37]

---

[32] Australian Government – Classification Review Board 2009, *Alien vs. Predator – Review Board Decision Reasons,* accessed March 2013, http://www.classification.gov.au/About/Documents/Review%20Board%20decisions/DecisionReasons-AliensvsPredator-Final-4January2010.pdf.

[33] See generally Andy Chalk, "OFLC reveals changes to Australian *Fallout 3*,"*The Escapist*, 13 August 2000, http://www.escapistmagazine.com/news/view/85646-OFLC-Reveals-Changes-To-Australian-Fallout-3.

[34] Australian Law Reform Commission Report 118, "Classification-Content Regulation and Convergent Media" February 2012, http://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_118_for_web.pdf.

[35] *Jones v. Toben* [2002] FCA 1150 (17 September 2002), http://www.austlii.edu.au/au/cases/cth/FCA/2002/1150.html.

[36] Nick Title, "Open Justice – Contempt of Court" (paper presentation, Media Law Conference Proceedings, Faculty of Law, The University of Melbourne, February 2013).

[37] Delimiter, "Roxon Makes Plea on YouTube," September 11, 2012, http://delimiter.com.au/2012/09/11/data-retention-roxon-makes-youtube-plea/.

Advanced web applications like the social-networking sites Facebook and MySpace, the Skype voice-communications system, and the video-sharing site YouTube are neither restricted nor blocked in Australia. Digital media such as blogs, Twitter feeds, Wikipedia pages, and Facebook groups have been harnessed for a wide variety of purposes ranging from elections, to campaigns against government corporate activities, to a channel for safety-related alerts where urgent and immediate updates were required.[38]

VIOLATIONS OF USER RIGHTS

While online users in Australia are generally free to access and distribute materials online, free speech is limited by a number of legal obstacles, such as broadly applied defamation laws and a lack of codified free speech rights. Australia's accession to the Council of Europe Convention on Cybercrime on November 30, 2012, while putting the country in line with international legal standards, also raised concerns because of the broader requirements under the Australian legislation for ISPs to monitor user activities.

Australians' rights to access internet content and freely engage in online discussions are based less in law than in the shared understanding of a fair and free society. Legal protection for free speech is limited to the constitutionally-implied freedom of political communication, which only extends to the limited context of political discourse during an election.[39] There is no bill of rights or similar legislative instrument that protects the full range of human rights in Australia, and the courts have less ground to strike down legislation that infringes on civil liberties. Nonetheless, Australians benefit greatly from a culture of freedom of expression and freedom of information, further protected by an independent judiciary. The country is also a signatory to the International Covenant on Civil and Political Rights (ICCPR).

The Australian press, however, has consistently expressed concerns about a "culture of secrecy" that continues to inhibit reporting.[40] A 2007 report commissioned by Australia's Right to Know (ARTK), a coalition of media companies formed to examine free press issues, found that there were over 350 pieces of legislation containing "secrecy" provisions to restrict media publications.[41] There are two significant secrecy laws that have a far-reaching impact on the media. The first is a lack of federal legislation to protect whistleblowers. The second is a lack of shield laws in many Australian states, which means that journalists are not shielded from having to disclose their sources in a court proceeding. In cases where journalists do not disclose their sources, they are subject to

[38] Digital media, for example, is readily used for political campaigning and political protest in Australia. See Terry Flew, "Not Yet the Internet Election: Online Media, Political Content and the 2007 Australian Federal Election,"(2008) *Media International Australia Incorporating Culture and Policy*, pp. 5-13. Also available at http://eprints.qut.edu.au/39366/1/c39366.pdf

[39] Alana Maurushat, Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009).

[40] David Rolph, Matt Vitins, and Judith Bannister, *Media Law: Cases, Materials and Commentaries* (South Melbourne: Oxford University Press, 2010): 44.

[41] Australia's Right to Know, "Submission to the Australian Law Reforms Commission's Review of Secrecy Laws" (2007) http://www.australiasrighttoknow.com.au/files/docs/ALRC-Secrecy-Submission.pdf.

liability and possible criminal sanction.[42] In October 2012, Independent Member of Parliament Andrew Wilke introduced the Public Interest Disclosure (Whistleblower Protection) Bill. The bill is consistent with past recommendations and committee outcomes recommending that whistleblower protection be introduced at the federal level. The bill, if enacted, provides much needed protection for those federal public sector employees who leak information about corrupt practices. At this time there is no evidence to support whether leaking information occurs more often via online communication as opposed to traditional media such as print or broadcast.

The Anti-Terrorism Act 2005 (Cth) revived laws against sedition and unlawful association. The unlawful association provisions have been used widely since their enactment to ban several organizations perceived to be potentially dangerous in terms of their links to violent acts.[43] The sedition provisions, however, have not been used. Further, insults against government institutions or officials would not fall within the sedition provisions.[44]

Australian defamation law has been interpreted liberally and is governed by legislation passed by the states as well as common law principles.[45] Civil actions over defamation are common and form the main impetus for self-censorship,[46] though a number of cases have established a constitutional defense when the publication of defamatory material involves political discussion.[47] Court costs and stress associated with defending against suits under Australia's expansive defamation laws have caused organizations to leave the country and blogs to shut down.[48]

Under Australian law, a person may bring a defamation case to court based on information posted online by someone in another country, providing that the material is accessible in Australia and that the defamed person enjoys a reputation in Australia. In some cases, this law allows for the possibility of libel tourism, in which individuals may take up legal cases in Australia because of the more favorable legal environment regarding defamation suits. The right to reputation is generally afforded greater protection in countries like Australia and the United Kingdom than the right of freedom of expression. In Australia this is especially so as freedom of expression is limited to political speech. While the United States and the United Kingdom have recently enacted laws to restrict libel tourism, Australia is not currently considering any such legislation.

Social-networking companies such as Twitter and Facebook are finding themselves in Australian courts under Australia's defamation laws. Recently, television actress and producer Marieke Hardy

---

[42] Irene Moss, *Report of the Independent Audit into the State of Free Speech in Australia* (Surry Hills, New South Wales: Australia's Right to Know Coalition, 2007), http://www.smh.com.au/pdf/foIreport5.pdf.. See also LexMedia Australia, "Journalist Shield Laws in Australia" (2010) http://www.lexmedia.com.au/2010/10/journalist-shield-laws.html#.UTfUOHnh2F8.
[43] Andrew Lynch and George Williams, *What Price Security?* (UNSW Press: Sydney, 2006), 41-59.
[44] Ibid.
[45] Principles of online defamation stem from the High Court of Australia, *Dow Jones & Company Inc v. Joseph Gutnick*, [2002] HCA 56.
[46] Moss, 42.
[47] Human Rights Constitutional Rights, "Australian Defamation Law," http://www.hrcr.org/safrica/expression/defamation.html, accessed June 2010.
[48] Asher Moses, "Online Forum Trolls Cost me Millions: Filmmaker," *Sydney Morning Herald*, July 15, 2009, http://www.smh.com.au/technology/technology-news/online-forum-trolls-cost-me-millions-filmmaker-20090715-dl4t.html.

wrongly named Melbourne resident Joshua Meggitt as the author of a hate blog.[49] Hardy tweeted the defamatory comment, which was then retweeted by some of Hardy's followers. In 2011, Meggitt sued Hardy for defamation and reached a confidential settlement out of court. Then in 2012, Meggitt took further legal action against Twitter as the publisher of Hardy's defamatory tweet. Hardy has reached a confidential settlement out of court. There is no reported outcome yet in the Twitter matter.

Users do not need to register to use the internet, nor are there restrictions placed on anonymous communications. The same cannot be said of mobile phone users, as verified identification information is required to purchase any prepaid mobile service. Additional personal information is required for the service provider before a phone may be activated. All purchase information is stored while the service remains activated, and it may be accessed by law enforcement and emergency agencies providing there is a valid warrant.[50]

Law enforcement agencies may search and seize computers, and compel an ISP to intercept and store data from those suspected of committing a crime. Such actions require a lawful warrant. The collection and monitoring of the content of a communication falls within the purview of the Telecommunications (Interception and Access) Act 1979 (TIAA). Call-charge records, however, are regulated by the Telecommunications Act 1997 (TA).[51] It is prohibited for ISPs and similar entities, acting on their own, to monitor and disclose the content of communications without the customer's consent.[52] Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions.[53] The TIAA and TA expressly authorize a range of disclosures, including to specified law enforcement and tax agencies, all of which require a warrant. ISPs are currently able to monitor their networks without a warrant for "network protection duties," such as curtailing malicious software and spam.[54]

On August 22, 2012, the Australian Senate passed the Cybercrime Legislation Amendment Bill, allowing Australia to accede to the Council of Europe Convention on Cybercrime.[55] Unlike that of many other countries that have already ratified the convention, Australia's legislation goes beyond the treaty's terms by calling for greater monitoring of all internet communications by ISPs. Under the Convention, an ISP is only required to monitor, intercept, and retain data when presented with a warrant, and only in conjunction with an active and ongoing criminal investigation restricted to the areas in the Convention: child pornography, online copyright (intellectual property), online

[49] Michelle Griffin, "Man Sues Twitter over Hate Blog" *Sydney Morning Herald*, February 17, 2012, http://www.smh.com.au/technology/technology-news/man-sues-twitter-over-hate-blog-20120216-1tbwg.html.
[50] ACMA, "Pre-paid Mobile Services—Consumer Information Provision Fact Sheet," accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/pc=PC_9079.
[51] Telecommunications Act 1997, Part 13, http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/.
[52] Part 2-1, section 7, of the Telecommunications (Interception and Access) Act 1979 (TIAA) prohibits disclosure of an interception or communications, and Part 3-1, section 108, of the TIAA prohibits access to stored communications. See Telecommunications (Interception and Access) Act 1979, http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.
[53] Criminal offenses are outlined in Part 2-9 of the TIAA, while civil remedies are outlined in Part 2-10. See Telecommunications (Interception and Access) Act 1979, http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.
[54] Alana Maurushat, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Obfuscation Crime Tools?" (2010) *University of New South Wales Law Journal* 16, no. 1.
[55] Council of Europe, Convention on Cybercrime, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

fraud and forgery, and computer offenses. The new Australian legislation compels ISP cooperation for any serious crime being investigated in Australia or overseas; it is not limited to the crimes set out in the Convention.

The Convention also requires expeditious preservation of data by the person in possession or control of data, which means ISPs will often be the ones called upon to preserve data. Articles 16 and 17 of the Convention state that ISPs can be compelled to preserve internet traffic data logs for a maximum period of 90 days, whereas the Australian legislation mandates that ISPs store data for 180 days for foreign preservation notices. However, the Convention does not compel ISPs to monitor stored communications, only traffic data. In the case of an active criminal investigation, the Convention obligates an ISP to preserve the data that is already stored but would otherwise be deleted. This could include preservation of what IP addresses connect to and from other IP addresses, or what phone numbers connect to a Voice over Internet Protocol (VoIP) number. This may also include information about what types of protocols a customer uses, the size and use of packets, and so forth. Data preservation remains a controversial point but most notably in relation to the obligation to provide mutual assistance to a foreign entity.

In July 2012, the Commonwealth Attorney-General's Department released a discussion paper titled "Equipping Australia against emerging and evolving threats."[56] Under the proposal, Australian ISPs would be required to monitor, collect, and store information pertaining to all users' communications, including storing communications for a period of two years. This activity would be done without a warrant and enforced against all users regardless of whether there is a criminal investigation.[57] A similar data retention law is in place in Europe.[58] Many European courts, however, have struck down the data retention provisions on the grounds that they are a gross violation of privacy, inconsistent with domestic law, and unconstitutional.[59] The Attorney-General has failed to discuss the significant differences between the EU and Australian legal environments. In EU countries, including the United Kingdom, citizens' human rights are protected under a Bill of Rights or a Charter of Human Rights and Freedoms. Like the U.S. courts, European courts can strike down laws or directives which offend these guarantees of fundamental human rights and civil liberties. There is no Bill of Rights or Charter of Human Rights and Freedoms in Australia. As such, the courts have no effective means to strike down proposals that violate civil liberties. Once a proposal is enacted, the only way to have it changed is through legislation, which often requires a change of government. This compulsory data-retention policy, if enacted, could become a significant threat to online freedom in Australia. The proposal is not yet official policy in Australia, nor has it evolved to a bill. At this point in time it remains a proposal only.

---

[56] Commonwealth Attorney-General's Department's Discussion Paper, *Equipping Australia against emerging and evolving threats*, 2012, accessed February 1, 2013, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/discussion%20paper.pdf.

[57] Asher Moses, "Web Snooping Policy Shrouded in Secrecy," *The Age*, June 17, 2010, http://www.theage.com.au/technology/technology-news/web-snooping-policy-shrouded-in-secrecy-20100617-yi1u.html.

[58] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006

[59] Countries that have annulled, modified, or ruled the provisions unconstitutional include: Germany, Czech Republic, Romania, Bulgaria, and the Republic of Cypress. Constitutional challenges continue in Ireland, Hungary, and Slovakia.

There have been several cases in the states of New South Wales and Victoria of individuals being sentenced to jail terms for publishing explicit photos of women, typically former girlfriends or boyfriends. By way of example, Australian citizen Ravshan Usmanov pled guilty to publishing an indecent article and was originally sentenced to six months of home detention after he posted nude photographs of an ex-girlfriend on Facebook.[60] The sentence was appealed and the court commuted the original sentence in favor of a suspended sentence.

The group Anonymous has commenced a series of "hacktivist" attacks in response to the data retention proposal put forth by the Attorney-General. In July 2012, the movement took down a number of government websites as a form of protest after a Q&A session with Julia Gillard in which details of many cybersecurity initiatives were outlined.

[60] Heath Astor, "Ex-Lover Punished for Facebook Revenge," April 22, 2012, *Sydney Morning Herald*, http://www.smh.com.au/technology/technology-news/exlover-punished-for-facebook-revenge-20120421-1xdpy.html.

AZERBAIJAN

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	13	13
Limits on Content (0-35)	16	17
Violations of User Rights (0-40)	21	22
Total (0-100)	**50**	**52**

* 0=most free, 100=least free

POPULATION: 9.3 million
INTERNET PENETRATION 2012: 54 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Some websites were temporarily blocked during protests or other anti-government events (see **LIMITS ON CONTENT**).
- In addition to the dominance of state-owned media outlets, the government further manipulated the online sphere through intimidation tactics like requiring students to "like" government policies on Facebook, and threatening those who support anti-government political causes online (see **LIMITS ON CONTENT**).
- New regulations were implemented in 2013 that required all mobile phones to be registered according to their IMEI identification code (see **VIOLATIONS OF USER RIGHTS**).
- Authorities broadly applied existing laws to prosecute journalists and citizens for their online activities (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Over the course of the last few years, Azerbaijan has acquired a vibrant and rapidly growing online community. The internet in Azerbaijan has not only become a platform for information sharing, but as the country's traditional media outlets continue to fall under strict government control, it has become a medium for alternative voices and popular political dissent. Its limited, though growing, community of users has yet to see any major restrictions imposed on the technical level, given the country's ongoing commitment and eagerness to promote itself as a leader of information and communication technology (ICT) innovation in the region.

When it comes to the internet, the Azerbaijani government is practicing what some have called "networked authoritarianism"[1]—a middle path between open access and censorship, where online content remains relatively uncensored, and most often the state lets users discuss the country's problems and sometimes openly call for action. On the surface, such an approach generates a relatively democratic image for the country at home and abroad. However, behind the scenes, those who speak out on the internet are more likely to face intimidation, threats, arrests, and fines from the state.

Exemplifying this model, Azerbaijani authorities engage little in filtering and direct censorship. Nonetheless, they discourage the use of online technology in three ways: demonizing technology through the practice of media framing, as in the case with the state psychiatrist who called users of social media mentally ill;[2] gradually instilling a sense of fear and inevitably self-censorship in users of online media through constant monitoring and surveillance; and putting online activists behind bars, such as the case in 2009 of the arrests of two prominent bloggers, Emin Milli and Adnan Hajizade.[3]

While the internet was first introduced in Azerbaijan in 1994 and became available for all citizens in 1996, it was not until the late 2000s that the internet became a more widely-used tool. Despite an increase in internet penetration, the lowering of costs, and the growth of various internet service providers (ISPs), the overall quality of internet access has remained low, especially outside the capital, where many users still rely on dial-up services. Since 2005, authorities have sporadically blocked access to certain antigovernment websites (including satirical ones). The crackdown intensified in 2011 with bloggers and online activists joining the usual group of targeted suspects—outspoken journalists and opposition party members. The uprisings of the Arab Spring created further grounds for fear, turning the government's attention to social networks in search of "violators" of public order.

[1] Katy E. Pearce, Sarah Kendzior, "Networked Authoritarianism and Social Media in Azerbaijan," Journal of Communication ISSN 0021-9916, 2013, http://www.academia.edu/1495626/Networked_Authoritarianism_and_Social_Media_in_Azerbaijan
[2] "Social network users have 'mental problems'," trend.az, March 7, 2011, http://en.trend.az/news/society/1841409.html
[3] Adam Hug, "Spotlight on Azerbaijan," *Information and Communication Technology in Azerbaijan*, The Foreign Policy Center, 2012, fpc.org.uk/fsblob/1462.pdf

In 2012, Azerbaijan hosted two major international events: the Eurovision Song Contest in May and the Internet Governance Forum in November. In the wake of these events, once international attention had been diverted, the government continued to crack down on protestors and suppress antigovernment media coverage. From 2012-2013, the number of attacks on opposition websites and arrests of online activists increased, alongside an increase in the use of ICTs to mobilize protests against the government.

OBSTACLES TO ACCESS

Indicators for Azerbaijan's internet penetration vary based on available sources, although most would agree that the number of internet users has risen significantly in recent years. Figures reported by the Ministry of Communication and Information Technologies (MCIT) indicate an internet penetration rate of 70 percent for 2012; these statistics include mobile internet users as well as anyone who has accessed the internet, including one-time users.[4] The International Telecommunication Union (ITU), on the other hand, estimates Azerbaijan's internet penetration rate at 54 percent for 2012,[5] while research conducted by academics suggest that the penetration figure could be as low as 25 percent.[6]

Despite a growing penetration rate, diversifying ISPs, and gradually declining costs, access to the internet remains highest in the capital and lowest in rural areas, where there is a scarcity of providers. The quality of access also remains low, with paid prices not corresponding to advertised speeds and with many users still relying on slow dial-up connections. An ambitious state program (worth $131 million in total) is underway to build a broadband internet infrastructure, particularly in rural regions. The plan intends to provide users across the country with 10 Mbps speed and generate an internet penetration rate of 85 percent by 2017.

At present, the cost of internet access at an average speed of 1 Mbps is a minimum of AZN 12 (approximately $15.30), which is equivalent to 3 percent of the average monthly wage, according to official data distributed by the Ministry of Communication and Information Technologies.[7] The ministry intends to further decrease prices; however, no specific amounts were mentioned in any of the recent statements that the ministry issued.[8]

Privately owned but government controlled Delta Telecom (previously known as AzerSat) is the primary ISP in the country, holding an 88 percent share of the overall internet market and selling

[4] "Internet penetration rate reaches 70% in Azerbaijan," ann.az, January 16, 2013, http://ann.az/en/?p=109281
[5] International Telecommunications Union (ITU), "Percentage of Individuals Using the Internet, 2012," accessed July 3, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
[6] İşdən sonra- Azərbaycanda internet statistikası, azadliq.org, November 7, 2012, http://www.azadliq.org/audio/broadcastprogram/635687.html [in Azerbaijani/English]
[7] "Minister: In Azerbaijan, the cost of connection to the Internet at speeds of 1Mbit/s is about 3% of the average monthly wage", apa.az, January 16, 2013, http://en.apa.az/news/186053
[8] "Azərbaycanda mobil danışıq qiymətləri və internet tarifləri ucuzlaşacaq", Kanal13AZ via youtube.com, January 9, 2013, http://www.youtube.com/watch?v=nCtwmMv0CRo [in Azerbaijani]

traffic to almost all other ISPs. [9] It was the first company to implement a WiMAX technology project in the country in February 2010, laying the foundation for the use of wireless, broadband, and unlimited internet access. The largest ISP operating outside of Baku is the state-owned AzTelekom, with ownership ties to the Ministry of Communication and Information Technologies (MCIT).[10] Azertelecom, owned by Azerfon, completed its fiber-optic network in 2011 and is now competing for Delta Telecom's business.[11]

Up until 2000, ISPs in Azerbaijan were required to obtain a license; however, in 2000 this licensing procedure was no longer required. As a result, according to the information provided by the Ministry of Communication and Information Technologies, today there are over 40 ISPs operating in the country with only three—Aztelekomnet, Bakinternet, Azdatakom—being state owned.[12] Delta Telecom and Azertelecom are two private companies that provide access to the international internet.

With Azertelecom's growing role in the internet business, government control over ICTs has become more apparent, particularly after it was uncovered in 2011 that Azerfon is largely owned by President Ilham Aliyev's daughters.[13] Furthermore, there is a lack of transparency over the ownership of other ICT resources. While there are no specific legal provisions or licensing requirements for ISPs in Azerbaijan, the MCIT refuses to answer inquiries regarding the ownership of license holders.[14]

According to clause 4.2(a) of the "Rules for Using Internet Services," internet providers can unilaterally suspend services provided to subscribers in cases that violate the rules stipulated in the law "On Telecommunications." Furthermore, a provider can suspend the delivery of internet services in certain circumstances including in times of war, events of natural disasters, and states of emergency, though none of these legal provisions were employed in 2012-2013.[15]

Usage of mobile phones in Azerbaijan has continued to grow steadily. There are three mobile service providers using the Global System for Mobile Communications (GSM) standard: Azercell, Azerfon, and Bakcell. In 2009, Azerfon, in a partnership with Britain's Vodafone, was the only company with a license for 3G service; however, in response to a number of critical media reports, Azercell and Bakcell were issued licenses in 2011, breaking Azerfon's monopoly over the 3G market. Azercell and Bakcell reduced prices to increase demand for mobile internet when they launched 3G services.[16] As a result, the number of mobile internet users on the Azercell network—

[9] "Azerbaijan country profile," Open Net Initiative, November 17, 2010, http://opennet.net/research/profiles/azerbaijan.
[10] Yashar Hajiyev, "Azerbaijan," European Commission, accessed August 30, 2012, http://bit.ly/1fz6jF9.
[11] "Azerbaijan Network," Azertelecom.az, accessed September 5, 2012, http://www.azertelecom.az/en/aznetwork/.
[12] Ministry of Communications and Information Technologies of the Republic of Azerbaijan, http://www.mincom.gov.az/activity/information-technologies/internet/
[13] Khadija Ismayilova, "Azerbaijani President's Daughter's Tied to Fast-Rising Telecoms Firm," Radio Free Europe/Radio Liberty, June 27, 2011, http://www.rferl.org/content/azerbaijan_president_aliyev_daughters_tied_to_telecoms_firm/24248340.html.
[14] Response of the Ministry of Communication to a written request for information.
[15] "Searching for Freedom: Online Expression in Azerbaijan", The Expression Online Initiative, November 2012, http://www.irfs.org/wp-content/uploads/2012/12/Report_EO_1.pdf
[16] "Azercell reduces prices for mobile internet services (Azerbaijan)," Wireless Federation, November 28, 2011, http://wirelessfederation.com/news/90875-azercell-reduces-prices-for-mobile-internet-services-azerbaijan/.

the country's largest mobile communication provider with 55 percent of the market[17]—increased 300 fold in 2011, according to a company representative.[18]

Introduction of 3G services and changes in mobile phone data packages provided by the phone companies brought down the average costs of mobile internet from AZN 40.5 (approximately $50) in 2011 to AZN 7.75 (approximately $10) in 2012. The connection speed improved significantly in 2011, increasing from 3.48 Mbps to 7.05 Mbps.[19]

Azerbaijan does not have an independent regulatory body for the telecommunications sector, and the MCIT performs the basic regulatory functions pursuant to the 2005 Law on Telecommunications. The MCIT also has a monopoly over the sale of the ".az" domain, which cannot be obtained online and requires an in-person application and Azerbaijani citizenship, subjecting the process to bureaucratic red tape and possible corruption.

On February 14, 2013, the Azerbaijani Press Council established a commission under the government-controlled National Television and Radio Council to handle citizen's complaints about ethical violations online, hacking attacks on web pages, and other issues related to online media.[20] This is another alarming development, as the Press Council is known for its progovernment stance. Already last year, the council restricted the activities of several critical newspapers by describing them as "rackets" and putting them on a "black list."[21] As a result, these papers are banned from publishing. Aflatun Amashov, chair of the Press Council, argues that since the number of internet news outlets is growing, the situation calls for the council to take concrete action in this direction.[22]

In another worrisome development, on February 20, 2013, the National Television and Radio Council announced the introduction of possible licensing measures for online television channels, seeing free operation of these outlets as "unfair" when compared to traditional TV channels.[23] Proponents of free speech and free access to information describe this move as the government's attempt to "gag freedom of expression and deprive people of alternative sources of information" through new forms of control.[24]

---

[17] "About us," Azercell, accessed September 5, 2012, http://company.azercell.com/en/.
[18] Nijat Mustafayev, "Number of mobile internet users of Azercell increased sharply over the past year," APA-Economics, November 18, 2011, http://en.apa.az/news.php?id=159794.
[19] "Mobile internet tariffs in Azerbaijan and explanations", mobiz.az, October 2012, http://mobiz.az/n909/Azerbaycanda-mobil-internet-tarifleri-+-tehlil [in Azerbaijani]
[20] "Press Council created commission for internet media," mediaforum.az, February 14, 2013, http://bit.ly/18eZnGI [in Azerbaijani]
[21] "Statement: The Online Expression is Under Assault in Azerbaijan," Expressiononline.net, http://expressiononline.net/pressreleases/statement-the-online-expression-is-under-assault-in-azerbaijan-2
[22] "Aflatun Amasov: commission on internet portals is not censorship", proses.az, February 21, 2013, http://proses.az/?m=xeber&id=8014 [in Azerbaijani]
[23] "Nushirvan Maharramli: 'We should license Internet TV'," contact.az, February 20, 2013, http://contact.az/docs/2013/Economics&Finance/011000024138en.htm#.USyg-uhhNAD
[24] "Statement: Expression Online Demands Azerbaijani Government Keep Hands Off the Internet," irfs.org, February 15, 2013, http://expressiononline.net/pressreleases/statement-expression-online-demands-azerbaijani-government-keep-hands-off-the-internet-5

LIMITS ON CONTENT

From 2012-2013, the government did not engage in widespread blocking or filtering of websites, preferring instead to exert control over the online sphere through intimidation and arrests of users. However, some sites were temporarily blocked, usually in connection to protests in specific areas of the country. In addition, the government continued its attempt to influence users' online activities by threatening students who criticize the government online, and causing indirect self-censorship and intimidation of users through high-profile arrests of online activists.

A few websites and social media platforms were sporadically blocked from 2012-2013. For example, the popular image-sharing website Imgur was temporarily blocked in early 2013.[25] On January 19, 2013, hackers from Anonymous obtained and released 1.7 GB worth of documents from the Special State Protection Service of Azerbaijan, posting the material as images on Imgur, after which the entire platform was temporarily blocked for users in Azerbaijan.[26] Websites such as Musavat, Azadliq, Bizim Yol, Turan News Agency, and Radio Free Europe/Radio Liberty's Azerbaijan service, were also subject to occasional blocking. Other websites, such as Tinsohbeti.com, a website with satirical articles, caricatures, and videos about government and government corruption, and Susmayaq.biz, a website for public campaigning, were both shut down.[27]

There is still no established process through which affected entities can appeal in cases where opposition websites or other materials have been censored. Sporadic filtering has also become a problem for opposition websites from the Azerbaijani diaspora, such as Azdiaspora.org. Meanwhile, both the MCIT and the Ministry of Education run a hotline program to uncover allegedly illegal and dangerous content.[28]

Another concern is the possible introduction of a new bill that will grant the government broad powers to restrict online content, allegedly in order to protect children from pornography and other inappropriate material. On February 23, 2013, the chairman of the Azerbaijani Parliament's Social Policy Committee, Hadi Rajabli, told the local press service that a draft law is likely to be developed to limit children's access to the internet. In his statement, Rajabli assured that the law would not mean restrictions on content, but rather the introduction of limitations based on age groups.[29] However, according to Emin Huseynov, the Director of the Institute for Reporters'

[25] "Imgur.com blocked in Azerbaijan?", advocacy.globalvoicesonline.org, February 7, 2013, http://advocacy.globalvoicesonline.org/2013/02/07/imgur-com-blocked-in-azerbaijan/
[26] "1.7GB Documents leaked from Special State Protection Service of Azerbaijan", cyberwarmews.info, January 19, 2013, http://www.cyberwarnews.info/2013/01/19/1-7gb-documents-leaked-from-special-state-protection-service-of-azerbaijan/
[27] "Focus on Internet and Human Rights in Azerbaijan: Interview with Vugar Gojayev", Global Information Society Watch, giswatch.com, http://www.giswatch.org/en/focus-internet-and-human-rights-azerbaijan-interview-vugar-gojayev
[28] Yaman Akdeniz, "Freedom of Expression on the Internet," Organization for Security and Cooperation in Europe, 2010, http://www.osce.org/fom/80723.
[29] "Children's access to internet may be limited in Azerbaijan", APA.az, February 23, 2013, http://en.apa.az/news/188419

Freedom and Safety (IRFS), this is merely an attempt to start censoring the internet and is likely to lead to additional restrictions.[30]

There are limited deletions of online content based on a takedown notice system, primarily related to personal data. Subject to Articles 5.7 and 7.2 of the law "On Personal Data," personal data published without the consent of an individual must be removed from websites following a written demand from the individual concerned, a court, or the executive branch.

Access to social media applications such as Facebook and Twitter is unrestricted, and such sites are increasingly used to disseminate content critical of the government. Facebook, in particular, has become a key source of information on rallies, protests, and social issues such as housing demolitions. The number of registered Facebook users grew from approximately 700,000 in December 2011 to over 1,000,000 users in 2013,[31] with the largest age group between the ages of 18-24. The second biggest age group of Facebook users consists of young people between the ages of 25-34. The majority of Facebook users in Azerbaijan are male, at 64 percent.[32]

Blogging in Azerbaijan began gaining popularity in 2007. With the introduction of Azerbaijani-language blogging platforms, active bloggers writing in the native language provide an alternative source of information on many subjects that are ignored or distorted by the traditional media. Together with microblogs, there are over 150,000 bloggers and microblog users in Azerbaijan.[33] Most of these blogs are written in the Azerbaijani language, and only about 1,000 blogs are written in English, Russian, and other languages. Many bloggers, such as Ali Novruzov, Emin Milli, Emil Bagirov, Etibar Salmanli, Arzu Geybullayeva, and Zaur Gurbanly, are well known for their independent views, and an estimated 50,000 to 70,000 users read blogs online. Additionally, according to the head of the Press Council in Azerbaijan, more than 10 internet radio stations and television channels operate in the country's virtual space, and over 100,000 users watch television online. There are also more than 40 online news websites.[34]

As journalists, activists, and those critical of the government have increasingly turned to the internet to express their views, the Azerbaijani authorities have amplified their efforts to clamp down on online activities and stifle opposition voices through tactics such as internet cafe raids, netizen arrests, and other extralegal intimidation (see "Violations of User Rights"). Some state universities warn students that they will encounter problems, including threats of bad grades or detention, if they participate in online political activism. Students are instead urged to be very active in defending the government and its positions in their posts and comments on Facebook and other social media. These efforts have had a chilling effect on internet users who may be practicing self-censorship out of fear of government reprisals, although the extent of self-censorship is not as

[30] "Statement: Internet censorship in Azerbaijan ready to go live," irfs.org, February 27, 2013, http://www.irfs.org/news-feed/statement-internet-censorship-in-azerbaijan-ready-to-go-live/
[31] "Facebook Statistics Azerbaijan," Socialbakers, accessed February 2013, http://bit.ly/qVuzuT.
[32] "Facebook Statistics Azerbaijan," Socialbakers, accessed February 2013.
[33] "Bloggers are passive: in Azerbaijan blog users are not active", video, YurdTV, March 5, 2013, http://yurd.tv/yurdxeber/20130302085717673.html [in Azerbaijani]
[34] "The number of Internet users in Azerbaijan is 45% of the population," Regnum News Agency, February 3, 2011. http://regnum.su/news/fd-abroad/azeri/1379705.html [in Russian].

widespread as in the traditional media. Furthermore, government-friendly online media outlets are the main beneficiaries of the advertisement market. As is the case in the traditional media sphere, state-owned and private companies tend to refrain from advertising their products in independent or opposition online media.

To further discourage young Azerbaijanis from using the internet and social networks, a number of different tactics were introduced. Early in 2011, the country's chief psychiatrist, Garay Geraybeyli, described "people who prefer communication on social networks [as] having mental problems."[35] Not surprisingly, the statement came four days prior to the March 11 Great People's Day in Azerbaijan, an online initiative organized through Facebook calling people join in the struggle for freedom and democracy in Azerbaijan in a civil way, without provocations, in villages and cities across the country.[36] In another attempt, a television program featured stories of "severe Facebook trauma" and "illness" as a result of use of social media. On April 2, 2013, an article published online on Xezerxeber.com described social networks as "cholera of the 21st century." The paper claims that social networks create jealousy among its users.[37]

Despite these manipulative efforts, youth activists, organizations, and political movements are widely represented in social media, providing information, organizing activities and events, and arranging flash mobs via the internet. Inspired by the Arab Spring uprisings in early 2011, young activists in Azerbaijan continue to use social media to organize demonstrations against the government's authoritarian rule, calling for democratic reforms and an end to pervasive government corruption.[38]

Beginning in September 2012, Elshad Abdullayev, the former director of the now-defunct Azerbaijan International University, began uploading videos to YouTube that exposed corruption on the part of Gular Ahmedova, a high-ranking figure and member of the ruling party.[39] The first video footage of this scandal, referred to as "GularGate," exposed Ahmadova attempting to sell a parliamentary seat to Abdullayev for AZN 500,000 (approximately $636,000). Ahmadova was stripped of her parliamentary mandate, expelled from the ruling party, and placed under house arrest. On February 13, 2013, the Prosecutor General's Office announced that Ahmadova had been charged under Article 178.3.2 for fraud (embezzlement) and Article 307.2 for concealment of a serious crime without agreement.[40]

On January 12, 2013, a large, unsanctioned rally was organized through the Facebook page "Əsgər Ölumlərinə SON" (End soldiers' deaths)[41] and held in Baku to protest against the death of military

[35] "Social network users have 'mental problems'," trend.az, March 7, 2011, http://en.trend.az/news/society/1841409.html
[36] https://www.facebook.com/events/192209267477787/
[37] "Social networks create jealousy", Xezerzeber.com, April 2, 2013, http://xezerxeber.com/XeberOxu.aspx?id=55717#.UV33UxlhOaI [in Azerbaijani]
[38] Natasha Schmidt, "Freedom of expression online," Chapter 8, *Running Scared: Azerbaijan's Silenced Voices*, Article 19: Global Campaign for Free Expression, 2012, http://www.article19.org/data/files/medialibrary/3003/12-03-26-azerbaijan.pdf.
[39] As of February 2013, eight videos have been released.
[40] "Azerbaijani Politician Arrested on Corruption Charge," rferl.org, February 14, 2013, http://www.rferl.org/content/azerbaijan-corruption/24901860.html
[41] https://www.facebook.com/Esger.olumlerine.son?ref=ts&fref=ts

conscript Ceyhun Qubadov. According to local reports, hundreds to thousands of people gathered at the Fountain Square holding signs with slogans about the mistreatment of military conscripts in Azerbaijan. While there were no arrests, police issued fines to 29 protestors. Facebook was quickly put to use once again to organize an online fundraiser through the "5 Gəpik" (5 Cents) Campaign. The campaign managed to raise 12,500AZN (approximately US$16,000) from seven thousand people over a two week period. Thirteen activsts paid their fines from this amount, while the rest was donated to the family of the concsript. Those who refused to pay their fines began a civil disobedience campaign.[42]

Most likely related to this campaign, as well as the upcoming presidential election in October 2013, a new subarticle was added to the Code on Administrative Offenses, based on which anyone providing or donating monetary assistance of more than AZN 200 (approximately $255) to political parties, civil society organizations, or international NGOs must register the donation with the Ministry of Justice.[43] Those who fail to do so will receive fines ranging from AZN 250 to AZN 7,000 (approximately $300-9,000).[44] The article divides "providers" into three categories: individuals, officials, and legal entity representatives. Institutions that accept these donations are also subject to fines, ranging from a minimum of AZN 1,000 to a maximum of AZN 10,000 (approximately $1,300-13,000).

VIOLATIONS OF USER RIGHTS

In 2012–2013, there were seven lawsuits against various opposition newspapers and their journalists, and five of these cases were related to their online activity. The government continued to restrict online activity through surveillance, monitoring of independent blogs, and extralegal intimidation of users. Additionally, new regulations were implemented in 2013 that require all mobile phones to be registered according to their IMEI identification code.

Articles 47 and 50 of the constitution guarantee freedom of thought and speech, provide the right to distribute information, and prohibit state censorship of the mass media.[45] In addition, as a member of the Council of Europe, the OSCE, and the UN, and as a signatory of the International Covenant on Civil and Political Rights (ICCPR), Azerbaijan is obliged to respect the right to freedom of expression. In practice, however, the authorities aggressively use various forms of legislation to stifle free speech in print and broadcast media. The judiciary lacks independence and is largely subservient to the executive branch.

[42] https://www.facebook.com/notes/khadija-ismayil/civil-disobedience-campaign-read-and-share/10151477615056535
[43] Mina Muradova, "Azerbaijan Restricts NGO Funding," The Central Asia-Caucasus Analyst, February 20, 2013, http://www.cacianalyst.org/publications/field-reports/item/12654-azerbaijan-restricts-ngo-funding.html
[44] "Those who give cash to political parties and NGOs in Azerbaijan will receive high fines," apa.az, February 8, 2013, http://az.apa.az/news/287879 [in Azerbaijani]
[45] The constitution is available in English at http://en.president.az/azerbaijan/constitution.

Libel is the most common criminal offense used by the authorities against journalists in Azerbaijan.[46] Under the Law on Mass Media of 1999, the internet is designated as a form of mass media, thus all rules applied to traditional media can be used to regulate the online sphere as well.[47] In November 2010, it was announced that the government-controlled Press Council would start monitoring online news sources for their compliance with the rules of professional journalism.[48]

While there are no laws that specifically criminalize online expression in Azerbaijan, there has been a growing trend in recent years of the authorities broadly applying existing laws to prosecute journalists and citizens for their online activities. In an effort to clamp down on free expression and silence critical voices in both the traditional media and online, the Azerbaijani authorities have increasingly detained critics on tenuous charges not directly related to their work. In many cases, arrests have been made based on politically motivated allegations of criminal defamation, fabricated accusations of illegal drug possession, or other such trumped-up charges.[49]

There have been numerous cases over the past few years of individuals being arrested or detained for their online activities. As of April 2013, seven journalists and two human rights defenders were in jail, and five of these cases are linked to their online criticism of authorities. Among these is Nijat Aliyev, the editor of the website Azadxeber.org. He has been in detention since May 2012 on drug-related charges and is facing up to three years in prison. Prior to his arrest, Aliyev publicly criticized the government's policies on religion and LGBT rights, and questioned the high costs of hosting the Eurovision song contest in 2012. On January 26, 2013, Aliyev was additionally charged with the sale and distribution of religious material without authorization; infringement of territorial integrity; and inciting national, racial and religious hostility.

On April 5, 2013, Araz Guliyev, the editor of the Islamist news website Xeber44.com, was sentenced by the Lankaran Court on Grave Crimes to eight years in prison. Guliyev was convicted of illegal possession of firearms; organizing and participating in a public order disturbance; inciting national and religious hatred; resisting the authorities; and insulting the republic's flag and insignia. Guliyev had originally been arrested on charges of hooliganism while he was reporting on a protest. Multiple rights organizations have expressed the view that these charges were fabricated and that the arrest was likely linked to Guliyev's activities as an online journalist.[50]

On May 9, 2013, Reshad Ramazanov, an online activist known for his outspokenness on Facebook in particular, was arrested and accused of illegal possession and/or sale of a large amount of

[46] "Azerbaijan Criminal Code: Article 147. Defamation," Conseil de l'Europe, December 12, 2003, accessed August 30, 2012, http://www.coe.int/t/dghl/standardsetting/media/Doc/DH-MM(2003)006rev_fr.asp#P281_18801.
[47] "Law of the Republic of Azerbaijan 'About Mass Media,'" Azerbaijan National Academy of Sciences, December 7, 1999, http://ict.az/en/index.php?option=com_content&task=view&id=477&Itemid=95.
[48] "Control Over Online Sources and Facebook-like sites in Azerbaijan," Today.az, November 27, 2010, http://www.today.az/view.php?id=77287.
[49] "International community must act on Azerbaijan crackdown," Amnesty International, November 16, 2011, http://www.amnesty.org/en/news/international-community-must-act-azerbaijan-crackdown-2011-11-16.
[50] "Editor of religious news website faces lengthy jail term in Azerbaijan," IFEX, April 8, 2013, http://www.ifex.org/azerbaijan/2013/04/08/editor_prison/; "Islamist website editor sentenced to eight years in prison," Reporters Without Borders, April 8, 2013, http://en.rsf.org/azerbaijan-islamist-website-editor-sentenced-08-04-2013,44332.html

narcotics. On May 10, 2013, he was sentenced to three months of pretrial detention. If convicted, Ramazanov faces up to 12 years of imprisonment.

Ramin Deko, a reporter for the newspaper *Azadliq*, was kidnapped in April 2011, held for eight hours, and warned to stop using social media to criticize the government.[51] On March 7, 2012, Deko was again detained while covering a protest near the Elmlar Akademiyasi metro station. The protest was held in response to reported abuses committed against prisoners of conscience Mahammad Majidli and Babak Hasanov. Deko was taken to the police station where all his photographs from that day were deleted from his memory card.

Following mass demonstrations in the remote town of Guba on March 1, 2012, which were prompted by the circulation of an online clip featuring the regional governor Rauf Habibov allegedly insulting the local population, two editors of Khayal TV were detained. Vugar Gonagov and Zaur Guliyev, who were held on charges of organizing mass disorder and abuse of office for posting video material online, were released on February 15, 2013, after they were given a probationary sentence of three years.[52] The circulation of the video posted by Gonagov and Guliyev prompted thousands of protestors to take to the streets and demand the governor's resignation.[53] In response to the unrest, the authorities searched several internet cafes in Guba to identify the individual responsible for posting the video. The authorities also tried to determine the authors of comments posted on social-networking websites that called for the demonstrations.[54] The governor was dismissed shortly after this unrest.

On January 26, 2013, after a series of protests and riots broke out in the town of Ismayilli, in which police used water cannons, rubber bullets, and tear gas to deter the protestors, supporters used Facebook to organize a solidarity protest in Baku. Residents gathered downtown and called for an immediate end to the use of weapons against unarmed civilians. Despite their calls, however, protestors were tackled, kicked, and slapped.[55] In total, 75 protestors were detained, and of those detained, five received administrative detention. Emin Milli was among these five. He received the longest sentence of 15 days of administrative detention. The fines handed out that day totaled AZN 15,250 (nearly $20,000),with the highest fine given to Turgut Gambar, the son of Isa Gambar, who is the leader of the Musavat Party.

In December 2011, the Cabinet of Ministers endorsed a plan—without parliamentary approval—that would require registration for all mobile devices. The plan requires the registration of IMEI codes (the unique serial number given to each phone), SIM cards, and mobile network numbers.

[51] "Journalist Ramin Deko: kidnapped yesterday, beaten today", Azadliq.org, April 4, 2011, http://www.azadliq.org/content/article/3546794.html [in Azerbaijani]
[52] "The Individual Cost of Freedom of Expression in Azerbaijan", International Partnership Group for Azerbaijan, March 26, 2013, http://milaz.info/en/news.php?id=8919
[53] Shahin Abbasov, "Report: Clashes in Azerbaijan Prompt Dismissal of Regional Government Official," Eurasianet.org, March 1, 2012, http://www.eurasianet.org/node/65068.
[54] Shahin Abbasov, "Azerbaijan: Is Guba Protest Response a Harbinger of a Political Shift in Baku?" Eurasianet.org, March 6, 2012, http://www.eurasianet.org/node/65092.
[55] "In Baku a rally was held in support of Ismayilli," azadliq.org, January 26, 2013, http://www.azadliq.org/media/video/24884524.html [in Azerbaijani]

Unregistered devices will be listed on a "black page" and mobile service providers will be required to limit service to all devices under this category.[56] The registration process began on March 15, 2013, and a statement from the Deputy Minister of Communication and Information Technologies indicated that service would be affected for phones on the "black page" beginning May 1, 2013.[57]

It is unclear to what extent security agencies monitor ICT activity or track user data in Azerbaijan. Most users do not have licenses for the software on their computers, which leaves them vulnerable to security threats such as viruses and other malicious programs that could be implanted to monitor their activity. While the law explicitly prohibits the arbitrary invasion of privacy and court orders are required for the surveillance of private communications, the law "On operative-search activity" (Article 10, section IV) authorizes law enforcement agencies to conduct surveillance without a court order in cases regarded as necessary "to prevent serious crimes against the person or especially dangerous crimes against the state."[58] The unclear parameters for what constitutes preventive action leave the law open to abuse. As such, it has long been believed that the Ministry of National Security and Ministry of Internal Affairs monitor the phone and internet communications of certain individuals, especially foreigners, known activists, and business figures.[59]

Such suspicions were confirmed by many of those detained for their involvement in the March 2011 protests, who reported that the authorities had referred to their Facebook activities and private communications during interrogations. This surveillance continues today, with arrested activists reporting seeing their Facebook message exchanges printed out. On February 27, 2013, Turkel Alisoy, a member of Popular Front Party's youth branch, was taken from his home to the Khatai District Police Office no. 35. From there he was taken to the Baku City Main Police Office, where the head of the criminal investigation department showed him screenshots of his Facebook post in support of the Students' Day of Boycott Facebook event page. Alisoy reported that he was accused of intentionally calling students and other citizens to protest. During his temporary detention, Alisoy was threatened with criminal prosecution if he continued to call for protests on Facebook.[60]

In April 2012, a month before Azerbaijan was set to host the Eurovision Song Contest, a Swedish investigative documentary revealed evidence of a blanket mobile phone surveillance system employed by the telephone company Azercell.[61] With help from the Stockholm-based telecom TeliaSonera, Azercell has reportedly installed "black box" devices on its networks that allow government security services and the police to monitor all mobile phone communications—including text messages, internet traffic, and phone calls—in real time without any judicial

[56] "Azerbaijan tightens control of mobile telephones," News.Az, December 30, 2011, http://www.news.az/articles/51997
[57] "IMEI-codes registration system to be applied in Azerbaijan," News.Az, March 15, 2013, http://www.news.az/articles/tech/77977
[58] "Article 10. Operative-search measures," Law of the Azerbaijan Republic, On operative-search activity, accessed September 5, 2012, http://taxes.caspel.com/qanun/728_eng.pdf.
[59] U.S. Department of State, "Azerbaijan," Country Reports on Human Rights Practices for 2011, Bureau of Democracy, Human Rights and Labor, http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper.
[60] "Monthly Internet Freedom Report February 20, 2013- March 15, 2013," Expressionline.net, http://expressiononline.net/monitoringresearch/monthly-internet-freedom-report-february-20-2013-march-15-2013
[61] "Video: The Black Boxes," SVT.se, April 26, 2012, http://www.svt.se/ug/video-the-black-boxes-3.

oversight. In addition, insider reports described how Azercell has set aside special offices in their headquarters for government authorities to conduct surveillance activities. While it is unclear exactly when the monitoring system was installed and put into practice, one source working for TeliaSonera noted that "the Arab Spring prompted the regimes to tighten their surveillance….There's no limit to how much wiretapping is done, none at all."[62]

Netizens and their family members have also been subject to instances of extralegal intimidation and harassment through surprise police visits to their homes, summons to local branches of the Ministry of National Security for questioning, and arbitrary job losses.[63] In one instance, the investigative journalist Khadija Ismayilova became the victim of a blackmail campaign in March 2012 that attempted to silence her by publishing private personal footage aimed at damaging her reputation. Known for her reporting on corruption in the country, including investigations into the president's conduct and business activities, Ismayilova had been regularly disseminating her reports on social-networking sites such as Facebook, where she has a wide following. The threats against her included intimate photographs of her being taken and then sent to her with a warning to "behave." Refusing to be silenced, Ismayilova instead went public with the blackmail attempt, and in retaliation, an intimate video of Ismayilova filmed by hidden camera was distributed over the internet.[64]

On March 26, 2013, 22-year-old activist and a member of the Azerbaijani Popular Front Party, Dashgin Malikov was arrested following a number of Facebook posts in which Malikov openly criticized the government. During a search at the police station, drugs were planted into Malikov's wallet. He was forced to sign a confession, which he later retracted. Malikov suffered from a medical condition that required him to undergo bi-annual medical checks, none of which indicated any instances of previous drug use.

On March 31, 2013, Taleh Bagirov, a religious scholar and activist, was arrested. Bagirov is known to be critical of the Azerbaijani government in his sermons (some of his sermons are available on YouTube. His final video received over 36,000 hits).[65] He was charged with illegal drug possession with an intention to sell under Article 234.1 of the Azerbaijani criminal code. According to Bagirov's lawyer, Anar Gasimli, he was unable to see his client for a week. When Gasimli finally did see Bagirov, the activist told him he was abused and beaten while in custody. During their meeting, the defendant was heavily bruised and unable to move three of his fingers. Requests for immediate medical examination were never met. In March, Bagirov was sentenced to two months in pre-trial detention. His sentenced was extended on May 24.

On April 3, 2013, a story appeared on a local online news portal, Haqqin.az, about a case in which a university had prepared a list of students with accounts on social networks. According to Alkhas

[62] Ryan Gallagher, "Your Eurovision Song Contest Vote May Be Monitored: Mass Surveillance in Former Soviet Republics," Slate.com, April 30, 2012, http://slate.me/IQPhyO.
[63] U.S. Department of State, "Azerbaijan," Country Reports on Human Rights Practices for 2011, Bureau of Democracy, Human Rights and Labor, http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper.
[64] Robert Coalson, "Azerbaijani Journalist Defiant in Face of Blackmail Bid," Radio Free Europe/Radio Liberty, March 9, 2012, http://www.rferl.org/content/azerbaijan_ismailova_blackmail_rferl_journalists_threats/24509372.html.
[65] Haci Taleh Bagirzade arrested following this speech, March 24,2013, https://www.youtube.com/watch?v=KUmEb7O43-A

Ismaylov, the author of the article, a fourth year student of Technical University stated that students were directly warned by the deputy deans to close their profiles if they wanted to remain students of the university.[66]

In April 2013, Azerbaijani TV channels aired voice recordings of arrested NIDA members (a young opposition movement) Bakthiyar Guliyev and Mahammad Azizov,[67] confessing their intentions to resort to violence against the police by using Molotov cocktails during the planned March 10 protests. Many supporters and human rights defendants believed the young men were coerced or threatened into making these confessions during detention, as none of them were allowed to see their lawyers following their arrests.

Wrongful access to a computer, such as through the implantation of viruses or security breaches, is punishable under Chapter 30 of the criminal code.[68] Internet security is also dealt with in the Law on National Security of 2004 and the Law on Protection of Unauthorized Information of 2004. Hacking attacks aimed at Azerbaijani internet users and websites often come from Armenian internet protocol (IP) addresses, and the timing of such attacks typically coincides with politically sensitive dates related to the unresolved territorial conflict between the two countries. Sometimes attacks occur after high-profile political statements. The ostensibly Armenian-based attacks have targeted the websites of entities such as the MCIT, the National Library, and the public television broadcaster. The Anti-Cybercriminal Organization is the main body working against cyberattacks in Azerbaijan, and the country ratified the Council of Europe's Convention on Cybercrime in March 2010, which took effect in July 2010.

Throughout 2011, some opposition news websites, including *Yeni Musavat*, Radio Azadliq, and the personal blog of the Popular Front Party's chairman Ali Kerimli, were subject to constant attacks that resulted in temporary shutdowns.[69] The newspaper *Yeni Musavat* speculated that the cyberattack against it could have been launched by the Ministry of Defense as a response to its critical reporting, but the ministry denied the allegations.[70] In June 2011, the Popular Front Party issued a statement also accusing the government of cyberattacks against its website.[71] Nevertheless, the sites of state bodies and state-controlled media have also been subject to an increasing number of cyberattacks over the past year, with hackers targeting and defacing sites belonging to the Interior Ministry, the State Security Service, the Ministry of Education, and the ruling New Azerbaijan party, among others.[72]

---

[66] Alkhas Ismaylov, "Student users of Facebook, get out of Universities", April 3, 2013, http://haqqin.az/news/4827 [in Russian]
[67] In total 7 NIDA members are currently in detention facing up to 8 years in prison if convicted
[68] An unofficial English translation of the criminal code is available at http://bit.ly/MY3HK.
[69] "Two more Azerbaijani websites undergo hacker attacks," Azerbaijani News Network, April 9, 2012, http://ann.az/en/?p=70943.
[70] "Azərbaycan Müdafiə Nazirliyi "Yeni Müsavat" qəzetini məhkəməyə verir," APA Economics, September 16, 2011, http://az.apa.az/news.php?id=234649 [in Azerbaijani].
[71] Fatima Karimli, "AXCP hakimiyyəti kibercinayətdə suçladı" [Front Party cybercrime], Qafqazinfo, June 22, 2011, http://qafqazinfo.az/AXCP_HAKIMIYY%C6%8FTI_KIBERCINAY%C6%8FTD%C6%8F_SU%C3%87LADI-923-xeber.html.
[72] Institute for Reporters' Freedom and Safety (IRFS), "Chapter Four: Freedom of Expression Online," *Azerbaijan's Critical Voices in Danger – Semi-annual Azerbaijan freedom of expression report, January 01-July 01, 2012*, http://www.ifex.org/azerbaijan/2012/08/16/irfs_freedom_of_expression_report.pdf.

BAHRAIN

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	12	11
Limits on Content (0-35)	25	26
Violations of User Rights (0-40)	34	35
Total (0-100)	**71**	**72**

* 0=most free, 100=least free

POPULATION: 1.3 million
INTERNET PENETRATION 2012: 88 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- After an intense government crackdown, more users have begun to exercise a degree of self-censorship when speaking about sensitive issues owing to fears of government reprisals (see **LIMITS ON CONTENT**).
- Eight online users were given prison sentences during the coverage period, with numerous others arrested or intimidated for Twitter posts amid authorities' increased intolerance towards government criticism on social media (see **VIOLATIONS OF USER RIGHTS**).
- Cyberattacks and government surveillance were increasingly employed to disrupt or monitor online activities of prominent dissidents (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

In the absence of a representative government, many Bahrainis look to the internet as an outlet for expressing political, economic, and social frustrations in the country. Unfortunately, as the importance of online tools has grown, so too has the desire of the Bahraini authorities to extend censorship and government repression practices from the real world into the online domain. In 1997, only two years after the internet was introduced in the country, a Bahraini internet user was arrested for the first time after sending information to a political opposition group outside of the country.[1] The Ministry of Information made its first official attempt to block websites containing content critical of the government in 2002, and today over 1,000 websites are blocked, including individual pages on certain social-networking sites.[2]

Crackdowns on Bahraini internet users escalated in 2011, following widespread protests against the ruling family of King Hamad bin Isa al-Khalifa. The authorities engaged in mass arrests, military trials, torture, and widespread intimidation tactics in an attempt to silence popular demands for greater political rights and democratic freedoms, including a new constitution and an elected government.[3] One online activist died from torture while in police custody in April 2011.[4]

Over the past year, a combined total of over 47 months of prison sentences have been passed down on eight Bahraini citizens as a result of their online activities, while many other cases are pending trial. The continued crackdown and oppressive online environment is pushing more users toward self-censorship. Surveillance of online activity and phone calls is widely practiced, and officers at security checkpoints actively search mobile phones for suspicious content.[5] Numerous users have reportedly been subject to physical or psychological torture while held by authorities, often for Twitter posts. Finally, online activists are subject to consistent cyberattacks as overzealous security forces aim to collect personal information for use during interrogations.

OBSTACLES TO ACCESS

From a technological perspective, Bahrain is one of the most highly connected countries in the world. In 2012, Bahrain ranked among the top five countries in the Western Asia region on the

[1] Initiative For an Open Arab Internet, "Bahrain," *Implacable Adversaries: Arab Governments and the Internet*, December 2006, http://old.openarab.net/en/node/350.
[2] "Bahrain: Government orders over 1,000 websites blocked," Index on Censorship, September 25, 2009, http://www.indexoncensorship.org/2009/09/bahrain-government-orders-over-1000-websites-blocked/.
[3] "Document – Bahrain: Two die as protests are violently repressed: 'Ali 'Abdulhadi Mushaima', Fadhel 'Ali Matrook," Bahrain Center for Human Rights, February 15, 2011, http://bahrainrights.org/en/node/3731.
[4] "Journalists Killed in Bahrain," Committee to Protect Journalists, April 9, 2011, http://cpj.org/killed/2011/zakariya-rashid-hassan-al-ashiri.php.
[5] "Political media in Bahrain: From the murals and publications to the online forums" [in Arabic], Bahrain Mirror, January 7, 2012, http://bhmirror.hopto.org/article.php?id=2712&cid=117.

United Nations Telecommunications Infrastructure Index.[6] Internet access is widely available at schools, universities, shopping malls, and coffee shops, where Bahrainis often gather for work and study.[7] The number of internet users has risen rapidly, from a penetration rate of 28 percent in 2006 to 88 percent in 2012.[8] There are approximately 413,000 internet subscriptions in the country, of which 60 percent were mobile broadband, 28 percent were fixed-wireless, and the remaining were ADSL.[9] Dial-up connections have disappeared since 2010 and ADSL use has declined with the growth of mobile broadband. Approximately 78 percent of broadband subscribers in 2011 were on plans with speeds of at least 1Mbps, while 58 percent enjoyed speeds of 2Mbps or higher.[10] Broadband prices fell by nearly 40 percent between 2010 and 2011, and are among the lowest in the region for mobile broadband. However, prices remain relatively high by international standards[11] and in comparison to countries in the Organization for Economic Cooperation and Development (OECD).[12]

Bahrain also has one of the highest mobile phone penetration rates in the region at 156 percent as of the end of 2012, representing over 2.1 million subscribers.[13] However, in an effort to halt the rapid dissemination of information, authorities banned BlackBerry users from sending news bulletins through text messages in April 2010.[14] BlackBerry phones are popular among young people and the business community and account for around 12.5 percent of mobile subscribers.[15] Similarly, while Web 2.0 applications such as the video-sharing site YouTube, social-networking site Facebook, and the micro-blogging site Twitter are available, the government often blocks individual pages on each of those platforms if they violate the country's strict laws on political expression. (See "Limits on Content")

Mobile phone services and ISPs are regulated by the Telecommunications Regulation Authority (TRA) under the 2002 Telecommunications Law. The TRA is responsible for licensing telecommunication providers and for "promoting effective and fair competition among established

[6] The index is a measure of the population's connectivity in fixed telephony, mobile, internet, online, personal computing and television. "E-Government Survey 2012," United Nations Department of Economic and Social Affairs, (New York: United Nations, 2012),http://www2.unpan.org/egovkb/global_reports/12report.htm.
[7] Telecommunications Regulatory Authority (TRA*), Annual Report 2011,* (Manama: TRA), slide 38, http://tra.org.bh/EN/pdf/TRAAnnualReport2011English.pdf.
[8] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2012, accessed June 24, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[9] Telecommunications Regulatory Authority (TRA), *Telecommunications Market Indicators in the Kingdom of Bahrain* (Manama: TRA, December 2012), slide 32, http://tra.org.bh/EN/pdf/2012TelecommunicationsmarketsindicatorsvFforpublic.pdf.
[10] Telecommunications Regulatory Authority (TRA), *Telecommunications Market Indicators in the Kingdom of Bahrain* (Manama: TRA, December 2012), slide 34, http://tra.org.bh/EN/pdf/2012TelecommunicationsmarketsindicatorsvFforpublic.pdf.
[11] Telecommunications Regulatory Authority (TRA*), Annual Report 2011,* (Manama: TRA), slide 33, http://tra.org.bh/EN/pdf/TRAAnnualReport2011English.pdf.
[12] Telecommunications Regulatory Authority (TRA), "Broadband Prices fall by up to 40% while Mobile Prices fall by up to 25%," press release, September 14, 2011, http://www.tra.org.bh/en/pdf/2011PriceBenchmarkingPressRelease_en.pdf.
[13] International Telecommunication Union (ITU), "Mobile-cellular subscriptions" 2012, accessed June 26, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[14] "Authorities Ban Blackberry Users from Sending News Bulletins," IFEX, April 15, 2010, http://ifex.org/bahrain/2010/04/15/blackberry_ban/.
[15] TRA, *Telecommunications Market Indicators in the Kingdom of Bahrain*, December 2012, slide 19, http://tra.org.bh/EN/pdf/2012TelecommunicationsmarketsindicatorsvFforpublic.pdf.

and new licensed operators."[16] In this vein, the TRA fined the leading telecommunications company Batelco BHD 5 million (US$13 million) in 2009 for monopolizing access to the country's international data lines, ordering the company to share its facilities with MENA Telecom and other licensed operators. The TRA has also issued several regulations that have not been welcomed by consumers, including measures that violate individual privacy.[17] (See "Violations of User Rights")

Although the TRA is theoretically an independent organization, in practice its members are appointed by the government and its chairman reports to the Minister of State for Telecommunications. Up until June 2013, this minister also occupied the post of President of the Information Affairs Authority (IAA).[18] In turn, the IAA, which replaced the Ministry of Information in 2010, oversees both traditional and online media outlets in Bahrain and is responsible for decisions to block websites, which are then enforced by internet service providers (ISPs).

In a positive development, more ISPs have recently been introduced to the Bahraini market, improving Bahrainis' access to the internet.[19] Indeed, over 31 licenses have been granted since 2003, with 16 providers currently in business.[20] There have been no reported instances of ISPs being denied registration permits. The major providers are Batelco, Zain, MENA Telecom, and VIVA. The latter two are also licensed to provide the increasingly popular WiMAX technology for accessing wireless broadband from one's computer through a USB device.

Batelco, Zain, and VIVA also serve as Bahrain's three mobile phone operators. The government has a controlling stake in Bahrain's largest telecommunications company, Batelco, while other ISPs are owned by investors from the private sector, including non-Bahraini investors. Although there is no centralized internet backbone in Bahrain, all ISPs are indirectly controlled by the government through orders from the TRA. This tight control over the country's ICT sector has allowed the Bahraini authorities to enforce strict limits on online content.

LIMITS ON CONTENT

Over the past year, the overall scale and sophistication of censorship has remained stable, with many websites blocked since the February 14, 2011 protests. The popular uprising, which was called for and heavily covered by online channels, resulted in a significant rise of blocking and filtering measures by the Bahraini authorities. Throughout late 2012 and early 2013, prominent platforms for the live-streaming of events and chat applications used to conduct online seminars remained blocked as the government sought to hinder online mobilization through legal and

[16] TRA Homepage, accessed March 19, 2013, http://www.tra.org.bh/EN/Home.aspx.
[17] Geoffrey Bew, "'Big Brother' Move Rapped," Gulf Daily News, March 25, 2009, http://www.gulf-daily-news.com/Print.aspx?storyid=246587.
[18] In June 2013, Mohamed al-Rumaihi was named President of the IAA, replacing Fawaz al-Khalifa who remained Minister of State for Telecom.
[19] TRA, *Telecommunications Market Indicators in the Kingdom of Bahrain*, December 2012, slide 10, http://tra.org.bh/EN/pdf/2012TelecommunicationsmarketsindicatorsvFforpublic.pdf.
[20] TRA, "Market Information: Number of Licenses Issued," accessed February 1, 2012, http://www.tra.org.bh/en/marketstatistics.asp.

administrative means. The crackdown on online speech has also resulted in an increase in self-censorship among social network users.

The IAA officially blocks websites that violate Articles 19 and 20 of the country's Press Rules and Regulations. This includes material judged as "instigating hatred of the political regime, encroaching on the state's official religion, breaching ethics, encroaching on religions and jeopardizing public peace or raising issues whose publication is prohibited by the provisions of this law."[21] As such, any site that criticizes the government, the ruling family, and the country's status quo is targeted by the IAA and promptly blocked. According to statistics provided by an online community-based survey, 39 percent of all sites reportedly blocked in Bahrain are related to politics, while 24 percent are related to the use of various internet tools, such as anonymizers and web proxies.[22] According to some estimates, the IAA has blocked or shut down more than 1,000 websites, including human rights websites, blogs, online forums, and individual pages from social media networks.[23] For example, the websites of the Arab Network for Human Rights Information (ANHRI) and the Bahrain Center for Human Rights (BCHR) have been blocked since 2006. The website of the opposition Bahrain Justice and Development Movement, which was established abroad, has been blocked since 2011.[24]

Although there are a number of news websites providing a plurality of viewpoints distinct from the narrative of Bahraini state media, most of these are blocked by the government and require circumvention tools to access. The websites of international television channels that continue to report on the unrest in Bahrain, such as Al-Alam,[25] Press TV,[26] and Lualua TV, remain blocked.[27] The news site Bahrainmirror.com, which is published from abroad,[28] and the website of the London-based *Al-Qudus Al-Arabi* newspaper have been blocked since 2011 for publishing views that are critical to the Bahraini government.[29] Bahrainonline.org, the country's prominent online forum, has been blocked since its launch in 1998, though its moderators have continuously generated and distributed new links to bypass the block.[30] The Arabic web portal and blog-hosting

[21] Please see "Decree-by-Law No. (47) for the year 2002 regarding organizing the press, printing and publishing," available at: http://www.iaa.bh/policiesPressrules.aspx.
[22] "Herdict: At a Glance - Bahrain" Herdict, accessed on March 19, 2013, http://www.herdict.org/explore/indepth?fc=BH.
[23] "Countries Under Surveillance: Bahrain," 2011, Reporters Without Borders, accessed July 16, 2012, http://en.rsf.org/surveillance-bahrain,39748.html.
[24] "Violence, blocked websites and prosecutions – Anti-media offensive continues," Reporters Without Borders, August 20, 2011, http://en.rsf.org/bahrain-violence-blocked-websites-and-20-08-2011,40811.html.
[25] "Channel block site of the world in Bahrain" [in Arabic], Islam Times, March 8, 2011, http://www.islamtimes.org/vdcfcmdt.w6dcxaikiw.html.
[26] "Press TV's website blocked in Bahrain," PressTV, March 5, 2011, http://www.presstv.ir/detail/168269.html.
[27] LualuaTV also had its satellite broadcast jammed in Bahrain. Source: Simon Atkinson, "Bahrain TV station struggles as signal blocked," BBC News, November 14, 2011, http://www.bbc.co.uk/news/business-15699332.
[28] "Crackdown continues in Bahrain, Bloggers go on trial in Emirates," Reporters Without Borders, June 16, 2011, http://en.rsf.org/bahrain-crackdown-continues-in-bahrain-16-06-2011,40467.html.
[29] "Bahrain: 'Internet' the biggest victim of the war launched by the authorities on the general freedom ANHRI condemns blocking Al-Quds Al-Arabi newspaper website following its publishing of an editorial article criticizing the Saudi intervention in Bahrain," The Arabic Network for Human Rights Information, May 24, 2011, http://www.anhri.net/en/?p=2544.
[30] Ben Birnbaum, "Bahrain continues crackdown on Shi'ite opposition," The Washington Times, September 14, 2010, http://www.washingtontimes.com/news/2010/sep/14/bahrain-shiites-fear-arrests-detention-torture/?page=2 and "WebStatsDomian - Mail.bahrainonline.org," WebStatsDomain, accessed March 19, 2013, http://www.webstatsdomain.com/domains/mail.bahrainonline.org/.

service Al-Bawaba has also been blocked since 2006. Online newspapers have been banned from using audio and video reports on their websites since 2010, apart from the state-owned Bna.bh, which publishes video reports taken from state television.[31] Website administrators face the same libel laws that apply to print journalists and are held jointly responsible for all content posted on their sites or chat rooms.

YouTube, Facebook, Twitter, and international blog-hosting services are freely available. However, certain Web 2.0 tools are permanently blocked and specific content on social networks can be inaccessible. For example, since February 2011, most live-broadcasting websites[32] that were popular among protesters have been blocked.[33] PalTalk, a chatting service that was used to conduct political seminars for wide online audiences, has been blocked since June 2011.[34] In September 2012, authorities briefly blocked the United Nations broadcast website in anticipation of the Bahrain Universal Periodic Review session.[35] It was unblocked shortly after, following a large online pressure campaign. A crowdsourcing application implemented by a Bahraini blogger used to track the locations of flash security checkpoints was blocked a few days after its launch in August 2012.[36] Furthermore, all websites displaying the "abusive video of Prophet Mohamed" were blocked after an order from the Ministry of Interior in September 2012.[37] Although the video was officially blocked, it remained accessible using certain mobile phone applications.

Following the March 2011 crackdown on protestors, authorities also used extralegal measures to forcibly remove online content. Through the use of arrests,[38] detentions, and torture,[39] security forces coerced many online forum moderators into permanently shutting down their sites.[40] This resulted in the loss of a large amount of information on Bahrain's history that had been documented by online users and made available only through local forums and websites.

---

[31] "Ban on audio programs on daily newspaper Al-Wasat's website," Bahrain Center for Human Rights, September 9, 2010, http://www.bahrainrights.org/en/node/3327.

[32] These sites include bambuser.com, ustream.tv, justin.tv, and other websites that stream directly to Twitter like twitcasting.tv and twitcam.livestream.com. See, "Attacks on media continue across Middle East," Committee to Protect Journalists, February 16, 2011, http://cpj.org/2011/02/attacks-on-media-continue-across-middle-east.php.

[33] "Despotic regimes continue to obstruct coverage of revolutions," Reporters Without Borders, September 1, 2011, http://en.rsf.org/bahrain-despotic-regimes-continue-to-01-09-2011,40886.html.

[34] "Crackdown continues in Bahrain, Bloggers go on trial in Emirates," Reporters Without Borders, June 16, 2011, http://en.rsf.org/bahrain-crackdown-continues-in-bahrain-16-06-2011,40467.html.

[35] "Bahrain: blocked UN website after Oral Intervention given by Prominent Human Rights Activist at the Human Rights Council," Bahrain Youth Society for Human Rights, September 14, 2012, http://byshr.org/?p=1170.

[36] "#Bahrain's blocks the police checkpoints map two days after launch," Bahrain Freedom Index,accessed March 19, 2013, http://bahrainindex.tumblr.com/post/30577509879/bahrains-blocks-the-police-checkpoints-map-two-days.

[37] "Interior Minister directs to speed work on blocking," [in Arabic], September 14, 2012, Al Wasat, http://www.alwasatnews.com/3660/news/read/701627/1.html.

[38] Non exhaustive list of forum moderators who were subject to arrest found at: https://spreadsheets.google.com/pub?hl=en&hl=en&key=0ApabTTYHrcWDdEk0Q0pWYnlSa3JmbS1RbThtUkZrNkE&output=html; accessed via: "Bahrain: After destruction of the actual protesting site at "the Pearl," the government shifts to eliminate virtual protests," Bahrain Center for Human Rights, May 17, 2011, http://bahrainrights.hopto.org/en/node/4101.

[39] http://globalvoicesonline.org/2011/12/05/bahrain-twitter-user-jailed-for-66-days-for-tweeting/

[40] Moderator of the AlDair Forum talks about his detention, saying he was forced to show the interrogation officer how to close the website: "Ahmed al-Dairi Moderator of AlDair Forums in the first episode of his testimony: thus eased voice of Zakaria AlAsheeri forever" [in Arabic], Bahrain Mirror, January 4, 2012, http://bhmirror.no-ip.org/article.php?id=2678&cid=117.

In Bahrain, websites are filtered based on keyword density, the manual entry of URLs, and certain website categories. An updated list of blocked websites is regularly sent to ISPs, which are instructed to "prohibit any means that allow access to sites blocked by the ministry."[41] Through notification to the TRA, the IAA can revoke the license of any operator that does not cooperate with its blocking orders.[42] Batelco, Bahrain's main ISP, filters the web using McAfee SmartFilter software and Blue Coat technology.[43] In March 2011, plans were announced to switch to technology from Palo Alto Networks that can block certain elements and activities within websites, such as video or photo uploading, and make it more difficult for users to circumvent censorship.

The decision-making process and government policies behind the blocking of websites are not transparent. The list of all blocked websites is not available to the public and the IAA can order the blocking of a website without referring the case to a court. In addition, webmasters do not receive notifications or explanations when their websites are banned. When trying to access a blocked site, users are presented with the message, "This web site has been blocked for violating regulations and laws of Kingdom of Bahrain," with no particular laws specified. Although the law does technically allow affected individuals to appeal a block within 15 days, no such case has yet been adjudicated.

The government crackdown in March 2011 led many regular internet users to exercise a higher degree of self-censorship, particularly after investigations of users' online activities were launched at work places and universities.[44] Today, the majority of users on Twitter and online forums, and even those who leave comments on online editions of newspapers, still use pseudonyms over fears of being targeted by the authorities.[45] Many have modified their privacy settings on social media or 'protected' their Twitter pages. There has been a drop in the level of tweets related to the #Bahrain hashtag since November 2012, following the prosecution of four internet users.[46] Some Twitter users have even announced that they have been temporarily forced to stop tweeting after receiving threats to their personal safety.[47]

While websites that express criticism of the government are blocked, authorities also manipulate the online content that is accessible in order to fabricate greater public support. Hoax journalists[48] linked to public relations (PR) agencies have been employed by the government to spread

[41] Reporters Without Borders, "Authorities Step Up Offensive Against Journalists and Websites," news release, May 14, 2009, http://en.rsf.org/spip.php?page=article&id_article=33042.
[42] Reporters Without Borders, "Authorities Step Up Offensive Against Journalists and Websites," news release, May 14, 2009, http://en.rsf.org/spip.php?page=article&id_article=33042. A copy of the law can be seen on [Arabic] http://www.legalaffairs.gov.bh/viewpdf.aspx?ID=RCLIF0109
[43] Paul Sonne and Steve Stecklow, "U.S. Products Help Block Mideast Web," Wall Street Journal, March 27, 2011, http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html.
[44] Simeon Kerr, "Manama fights back in cyberspace," Financial Times, May 23, 2011, http://www.ft.com/intl/cms/s/0/7bce94b8-8560-11e0-ae32-00144feabdc0.html#axzz1lLZwkuOF.
[45] Nancy Messieh, "Online anonymity: A gateway to freedom or abuse?" The Next Web, August 14, 2011, http://thenextweb.com/me/2011/08/14/online-anonymity-a-gateway-to-freedom-or-abuse/.
[46] See http://bahrainindex.tumblr.com/post/41025930298/a-drop-in-level-of-tweets-on-bahrain-hashtag
[47] See http://bahrainindex.tumblr.com/post/35897159633/bahraini-doctor-bahraindoctor-threatened-with-arrest
[48] Marc Owen Jones, "Hoax Journalist Liliane Khalil Returns, This Time as Habiba Dalal," MarcOwenJones, (blog), January 29, 2012, http://marcowenjones.wordpress.com/2012/01/29/the-return-of-liliane-khalil/.

propaganda on Twitter and progovernment blogs such as BahrainViews and Bahrain Independent.[49] At least one agency was contracted to provide "web optimization and blogging" services to the Bahraini government,[50] while other PR agencies are known to have been contracted for online reputation management through the creation of fake blogs and websites.[51] Multiple Wikipedia entries linked to Bahrain were also changed in favor of the government.[52] In general, the independent group Bahrain Watch lists 18 PR firms known to have been hired by the Bahraini government for various promotional campaigns since February 2011, representing at least $32 million in contracts.[53]

Similarly, an "army of trolls" has been active on Twitter[54] since February 2011, when hundreds of accounts suddenly emerged to collectively harass and intimidate online activists,[55] commentators, and journalists who voiced support for protests and human rights.[56] International figures and organizations are also targeted, including Marietje Schaake, a Member of the European Parliament from the Netherlands.[57] The government trolls have been moderately effective in silencing or reducing the activity of opposition voices inside Bahrain[58] and abroad.[59] The trolls have also played a vital role in spreading information that is controversial, offensive, or false,[60] in order to distort the image of protesters, spread hate and conflict, or discredit information posted on social networks.[61] These troll accounts usually have few followers (or sometimes none at all) and tend to appear and disappear in coordination with one another.

---

[49] Marc Owen Jones, "Busted! Journalist Liliane Khalil Exposed," MarcOwenJones, (blog), August 2, 2011 http://www.marcowenjones.hostbyet2.com/?p=364 and Media Jihad: If Ya Can't Beat 'Em, Sue 'Em! http://bahrainipolitics.blogspot.com/2011/06/media-jihad-if-you-cant-beat-em-sue-em.html# Dr Majeed AL Alawi, Twitter post, January 2, 2012, 2:51am, https://twitter.com/#!/DrMajeedAlalawi/status/153790396231716865.

[50] "Trippi & Associates Manipulate Internet Content on Behalf of Bahrain Government," Bahrain Freedom Index (blog), July 20, 2011, http://bahrainindex.tumblr.com/post/15188201300/trippi-associates-manipulate-internet-content-on.

[51] Marcus Baram, "Lobbyists Jump Ship in Wake of Mideast Unrest," Huffington Post, March 25, 2011, http://www.huffingtonpost.com/2011/03/24/lobbyist-mideast-unrest-departures_n_840231.html;

[52] Marc Owen Jones, "Truth Massages & the Intelligence Unknown," MarcOwenJones, (blog), December 7, 2011 http://www.marcowenjones.hostbyet2.com/?p=401.

[53] "PR Watch – keeping an eye on the Kingdom's PR," Bahrain Watch, http://bahrainwatch.org/pr/.

[54] "Bahrain's Troll Army," Web 3.0 Lab (blog), February 17, 2011, http://web3lab.blogspot.com/2011/02/bahrains-troll-army.html.

[55] Brian Dooley, "'Troll' Attacks on #Bahrain Tweets Show Depth of Government Attempts to Silence Dissent," Huffington Post (blog), November 17, 2011, http://www.huffingtonpost.com/brian-dooley/troll-attacks-on-bahrain_b_1099642.html.

[56] J. David Goodman, "'Twitter Trolls' Haunt Discussions of Bahrain Online," The Lede (blog), *New York Times*, October 11, 2011, http://thelede.blogs.nytimes.com/2011/10/11/twitter-trolls-haunt-discussions-of-bahrain-online/.

[57] See https://twitter.com/MarietjeD66/status/292223867274022913

[58] iManamaa, Twitter post, May 13, 2011, 7:39am, http://twitter.com/imanamaa/status/69049206215684097; Sultan Al-Qassemi, "Pioneer Bloggers in the Gulf Arab States," Jadaliyya, December 20, 2011, http://www.jadaliyya.com/pages/index/3643/pioneer-bloggers-in-the-gulf-arab-states; "Disturbing Drop in Tweeting in Bahrain," Web 3.0 Lab (blog), March 22, 2011, http://web3lab.blogspot.com/2011/03/disturbing-drop-in-tweeting-in-bahrain.html.

[59] Jillian York, "Twitter Trolling as Propaganda Tactic: Bahrain and Syria," JillianCYork.com (blog), December 10, 2011, http://jilliancyork.com/2011/10/12/twitter-trolling-as-propaganda-tactic-bahrain-and-syria/.

[60] Marc Owen Jones, "So Many Trolls but so Few Leaders: The Information War in Bahrain," MarcOwenJones (blog), March 14, 2011 http://www.marcowenjones.hostbyet2.com/?p=176.

[61] David Wheeler, "In the Arab Spring's Wake, Twitter Trolls and Facebook Spies," The Chronicle of Higher Education, November 29, 2011, http://chronicle.com/blogs/planet/2011/11/29/in-the-arab-springs-wake-twitter-trolls-and-facebook-spies/.

Despite these numerous attempts to manipulate the online information landscape, government restrictions on online advertising have not forced the closure of any opposition websites. While it is difficult for government-blocked websites to secure advertising, popular sites such as bahrainonline.org have not faced significant financial pressures. This is due to the fact that most Bahraini opposition websites are run with limited and sometimes personal resources. Furthermore, the websites continue to receive large amounts of traffic from users within Bahrain through the use of proxy services, dynamic IP addresses, and virtual private network (VPN) applications. However, the government does regularly block access to circumvention tools, including techniques such as using Google Page Translate, Google cached pages, and online mobile emulators. Adaptive and internet savvy Bahrainis tend to find ways around these restrictions.

Bahrain's online community has grown rapidly in recent years, especially in social media. The number of Bahraini users on Facebook reached 377,620 as of March 2013, representing a penetration rate of 51.2 percent,[62] and there are more than 3,500 local entities (both government and civil society) with a Facebook page.[63] Around 72,468 Bahraini users were active on Twitter as of June 2012.[64] Despite the recent drop in activity, the "#bahrain" hashtag consistently remains one of the most popular topics on Twitter across the Arab region.[65]

Given restrictions on press freedom, the lack of international media coverage, and the inability of many prominent journalists to enter the country,[66] activists have turned to the internet to continue to bring attention to ongoing protests and human rights violations in Bahrain.[67] Indeed, the internet is also the main source of information and news for many Bahrainis, particularly those active on Twitter. The resilient social protest movement titled the "Coalition of February 14 Youth" continues to use social networks such as Facebook and Twitter[68] to organize different forms of protests.[69] YouTube videos are uploaded to document police attacks on civilians and torture testimonies,[70] though many are promptly blocked.[71] Overall, by uploading videos and sharing

[62] "Bahrain Facebook Statistics," Socialbakers, accessed March 6 , 2013, http://www.socialbakers.com/facebook-statistics/bahrain.
[63] "To prevent its use in the buildup to the issues related to public affairs, Bahrain is considering the legalization of the use of Facebook similar to Arab countries" [in Arabic], Alwasat News, February 4, 2011, http://www.alwasatnews.com/3073/news/read/525216/1.html.
[64] Dubai School of Government, "Mapping Twitter: Twitter Users," Arab Social Media Report, Issue 4, July 2012, http://www.dsg.ae/en/Publication/Pdf_En/82620121121220934784 9.pdf
[65] Dubai School of Government, "Twitter in the Arab Region," *Arab Social Media Report*, accessed September 4, 2013, http://www.arabsocialmediareport.com/Twitter/LineChart.aspx?&PriMenuID=18&CatID=25&mnu=Cat.
[66] "Access Denied," a project of the independent research and advocacy organization Bahrain Watch, chronicles the many journalists, researchers, academics, and NGO workers that were expelled from or denied access to Bahrain from the 2011 uprising until now. Available at: http://bahrainwatch.org/access/.
[67] Amira al Hussaini, "Bahrain: Tweeting Appalling Conditions at Jaw Prison," Global Voices, July 19, 2013, http://globalvoicesonline.org/2012/07/19/bahrain-tweeting-appalling-conditions-at-jaw-prison/.
[68] See https://twitter.com/COALITION14
[69] Toby C. Jones and Ala'a Shehabi, "Bahrain's revolutionaries," Foreign Policy, January 2, 2012, http://mideast.foreignpolicy.com/posts/2012/01/02/bahrains_revolutionaries and "Demonstration Notice 3 – January 17, 2013, " U.S. Embassy Bahrain, January 17, 2013, http://photos.state.gov/libraries/adana/5/2013PDFfiles/CONS-DemonstrationNotice3-13.pdf .
[70] "Blocking the Documentary 'Systematic Torture in Bahrain' on YouTube," Bahrain Center for Human Rights, February 8, 2011, http://bahrainrights.hopto.org/en/node/3710.
[71] Jillian York, "Bahrain Blocks YouTube Pages and More," Global Voices, February 14, 2011, http://advocacy.globalvoicesonline.org/2011/02/14/bahrain-blocks-youtube-pages-and-more/.

images on social media, protesters have maintained the spotlight on their struggle and in some cases succeeded in placing pressure on the government.[72]

For example, in December 2012, a video of a police officer slapping a man in the course of an identity check went viral with over 200,000 views within 24 hours, receiving international attention and mainstream media coverage. Acting upon international pressure, Bahraini authorities announced that the policeman was arrested. Nonetheless, many observers were skeptical about the sincerity of the government's intentions and whether any disciplinary action would be taken against the officer.[73] In the end, he was handed a two-month sentence in June 2013.[74] The victim in the video also revealed that he was questioned by police authorities about the identity of the cameraman who took the video.[75]

VIOLATIONS OF USER RIGHTS

While censorship has remained somewhat stable since the post-uprising crackdown in 2011, the past year has witnessed an increase in violations of user rights. In particular, authorities have stepped up arrests of Twitter users for expressing criticism of the government. Also increasing is the practice of targeting activists with surveillance malware in order to monitor their online activities and collect personal information. The legal environment remains an impediment to freedom online, although authorities also make use of extralegal measures such as arbitrary detention and torture to intimidate and prosecute users. Bahraini authorities have continuously called for more restrictions on internet freedom in recent years.

Bahrain's legal environment presents many obstacles to internet freedom in its current form. According to Article 23 of the Bahraini constitution, freedom of expression is guaranteed, "provided that the fundamental beliefs of Islamic doctrine are not infringed, the unity of the people is not prejudiced, and discord or sectarianism is not aroused."[76] Article 26 states that all written, telephonic, and electronic communications "shall not be censored or their confidentiality be breached except in exigencies specified by law and in accordance with procedures and under guarantees prescribed by the law."[77] Similarly, the Press and Publications Law of 2002 promises free access to information "without prejudice to the requirements of national security and defending the homeland." Bahraini journalists have argued that these qualifying statements and loosely-worded clauses allow for arbitrary interpretation and, in practice, the negation of the many

[72] Marc Owen Jones, "Viral Justice: The MOI's Continued Failure to Hold Police Accountable Despite Evidence," Blog by Marc Owen Jones, December 11, 2012, http://marcowenjones.wordpress.com/2012/12/11/social-media-viral-justice-the-mois-continued-failure-to-hold-police-accountable-despite-evidence/
[73] "Bahrain: police 'slap' video goes viral," France24, January 3, 2013, http://www.france24.com/en/20121227-2012-12-27-2049-wb-en-webnews?page=11.
[74] "Officer is sent to prison for slapping man," Gulf Daily News, June 20, 2013, http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=355704.
[75] Malik Abdullah, "Almcefua Haider Rasool," [in Arabic] Al Wasat, January 5, 2013, http://www.alwasatnews.com/3773/news/read/728036/1.html .
[76] Constitution of the Kingdom of Bahrain, available at http://www.shura.bh/en/InformationCenter/Pages/Documents.aspx.
[77] Constitution of the Kingdom of Bahrain, available at http://www.shura.bh/en/InformationCenter/Pages/Documents.aspx.

rights they seek to uphold.[78] In addition, there is no law that defines clear penalties for violating the privacy of internet users, a concern shared by many bloggers who believe the absence of a law allows for greater abuse.[79]

The numerous proposals that are currently under review signal a negative trend in the country's legal environment. In September 2011, the Chief of Public Security issued a statement declaring that "the mere fact of posting instigative calls is a penal crime punishable by the law," even if those calls are made through social networks and internet websites.[80] Bahrain's Minister of State for Information Affairs announced in June 2012 that the government is preparing to introduce tough new laws to combat the "misuse" of social media.[81] The Interior Ministry also stated that it would crack down on offences and smear campaigns targeting national and public figures on social media networks.[82] These were followed by an October 2012 announcement that the Ministry of Justice will seek to enact further legislation to restrict the use of social networks, the internet, and mobile technologies.[83] These calls were linked to the spread of information online about the identities of security officers involved in human rights violations.[84] As of April 2013, no law had been officially proposed or issued. A proposed cybercrimes law that criminalizes unauthorized access to computer systems has been under review since 2005 and is scheduledto be discussed by the Council of Representatives during the current term of the lower house of parliament. The bill was approved by the Shura Council, or upper house, in June 2012.[85]

Censorship of online media is currently implemented under the 2002 Press and Publications Law[86] and was extended to mobile telephones in 2010.[87] The law allows for prison sentences of at least six months (and up to five years for repeat offenders) for publishing material that criticizes Islam, its followers, or the king, as well as content that instigates violent crimes or the overthrow of the

[78] "Bahrain," in *Media Sustainability Index 2008* (Washington, DC: IREX, 2009), http://irex.org/programs/MSI_MENA/2008/MSIMENA_bahrain.asp.
[79] "Ali al-Moussawi, "On the occasion of the World Day to combat electronic surveillance," [in Arabic], Al Wasat, March 12, 2012, http://www.alwasatnews.com/3474/news/read/642338/1.html.
[80] "Public Security/Statement," Bahrain News Agency, September 21, 2011, http://www.bna.bh/portal/en/news/473522.
[81] Matt J. Duffy, "Bahrain shouldn't pass new laws to regulate social media," Gulf News, June 26, 2012, http://gulfnews.com/opinions/editorials/bahrain-shouldn-t-pass-new-laws-to-regulate-social-media-1.1040382.
[82] Habib Toumi, "Ministry pledges cyber defamation crackdown," Gulf News, September 10, 2012, http://gulfnews.com/news/gulf/bahrain/ministry-pledges-cyber-defamation-crackdown-1.1072373.
[83] Mariam Ahmed, "Justice Minister declares: a new law to address the misuse of networking," [translated] Akhbar al-Khaleej, October 10, 2012, http://www.akhbar-alkhaleej.com/12619/article/54540.html.
[84] "Minister of Justice Uses Coercive Force against Preachers and Looms Further Procedures that Affect Freedom of Expression," Bahrain Center for Human Rights, October 17, 2012, http://www.bahrainrights.org/en/node/5476.
[85] "«Cyber crimes» and «money laundering» at the committee table" Alwatan News [in Arabic], October 14, 2012 http://alwatannews.net/NewsViewer.aspx?ID=mzj733337WsnRK6ipKD7V9T833338SEg933339933339
[86] For cases where the authorities have used the 2002 press law to censor online websites, see "Website accused of violating press code, BCHR concerned that move is aimed at silencing critical voices," Bahrain Center for Human Rights, October 1, 2008, http://www.bahrainrights.org/en/node/2446 and "Closing a blow to freedom of opinion and eexpression," [Arabic] Al Wasat, April 25, 2010, http://www.alwasatnews.com/2920/news/read/472942/1.html and "Blocking users 'Twitter' caused by a violation of the Copyright Act," [Arabic] Al Wasat, January 3, 2010, http://www.alwasatnews.com/2676/news/read/358169/1.html.
[87] Habib Toumi, "Bahrain imposes blackout on BlackBerry news sharing," habibtoumi.com (blog), April 8, 2010, http://www.habibtoumi.com/2010/04/08/bahrain-imposes-blackout-on-blackberry-news-sharing/.

government.[88] In addition, the 2002 Telecommunications Law contains penalties for several online practices such as the transmission of messages that are offensive to public policy or morals.[89] However, sentences can be longer if more severe penalties are called for by the penal code or terrorism laws. For instance, under the penal code, any user who "deliberately disseminates a false statement" that may be damaging to national security or public order can be imprisoned for up to two years.[90] The government has used these vague clauses to question and prosecute several bloggers and online commentators.

After the March 2011 crackdown on street protesters, the government conducted a mass arrest campaign of online activists and bloggers. More than 20 online activists were arrested and held for periods ranging from a few days to several months.[91] Arrests and prosecutions continued throughout 2012 and early 2013. Collectively, more than 47 months of prison sentences were passed on to eight Bahraini users in cases directly related to online posts between May 2012 and April 2013. As photos and videos of police brutality continue to emerge online, more measures are being taken against citizens who are seen holding cameras (including smart phones) in areas of protest. In November 2012, a Saudi blogger said she was told on two separate occasions to delete photos of protests and anti-government graffiti she had taken with her smartphone.[92] Bloggers, moderators, and online activists are systematically detained and prosecuted by authorities for expressing views the government regards as controversial.

One of Bahrain's most prominent human rights defenders, Nabeel Rajab, has been subject to repeated arrests and interrogations for publicly criticizing government figures. Rajab is the president of the Bahrain Center for Human Rights, a non-governmental organization that remains active despite a 2004 government order to close it.[93] He was first arrested on May 5, 2012 and held for over three weeks for "insulting a statutory body" in relation to a criticism directed at the Ministry of Interior over Twitter.[94] On June 9, 2012, he was arrested again after tweeting about the unpopularity of the Prime Minister (also a member of the royal family) in the city of Al-Muharraq, following the sheikh's visit there.[95] A group of citizens from the city promptly sued Rajab for libel in a show of obedience to the royal family. On June 28, 2012, he was convicted of

[88] Press and Publications Law of 2002 of the Kingdom of Bahrain (No.47 of 2002). A copy can be found at: http://www.legalaffairs.gov.bh/viewhtm.aspx?ID=L4702 or http://www.iaa.bh/policiesPressrules.aspx.
[89] Telecommunications Law of the Kingdom of Bahrain, http://www.tra.org.bh/en/pdf/Telecom_Law_final.pdf.
[90] Bahrain Penal code, 1976, article 168, http://bahrainrights.hopto.org/BCHR/wp-content/uploads/2010/12/Bahrain-Penal-Code.doc.
[91] List of arrested Bahraini journalists: https://docs.google.com/spreadsheet/ccc?key=0ApabTTYHrcWDdFZocWpBRlp6ell6RkNWeGh5YXAtUFE#gid=0, accessed via bahrainrights.org.
[92] Rana Jarbou, "A thousand weapons," Rana Jarbou, November 15, 2012, http://ranajarbou.blogspot.com/2012/11/a-thousand-weapons.html.
[93] "About BCHR," Bahrain Center for Human Rights, http://www.bahrainrights.org/en/about.
[94] "Nabeel Rajab granted bail but not released," Bahrain Center for Human Rights, May 19, 2012, http://www.bahrainrights.org/en/node/5256.
[95] Addressing the Prime Minister, Rajab tweeted: "Khalifa: Leave the al-Muharraq alley ways, their sheikhs and their elderly, everyone knows that you have no popularity there; and if it was not for their need for money they would not have come out to welcome you - when will you bow out?" "Bahrain: Call for 'immediate release' of activist Nabeel Rajab, jailed for tweet," Amnesty International, July 11, 2012, https://www.amnesty.org.uk/news_details.asp?NewsID=20223 and

charges related to his first arrest and ordered to pay a fine of 300 Bahraini dinars ($800).[96] Shortly after he was released on bail, he was re-arrested on July 9, 2012 after a court sentenced him to three months imprisonment for the Al-Muharraq incident. The court of appeals later acquitted Rajab, although he had already served most of his sentence.[97] However, he is currently serving a two-year sentence for "calling for illegal gatherings over social networks."[98] Rajab, who tweets under the name '@NabeelRajab,' was ranked the "most connected" Twitter user in Bahrain according to a survey, with over 150,000 followers at the time of his arrest in May 2012.[99] He continues to issue calls to protest over Twitter, even from prison.[100] By May 2013, Rajab's followers had reached 206,075 and the tweet that led to his arrest had been retweeted at least 2,000 times.[101]

In another case, a 19-year-old blogger was sentenced to two years imprisonment for reportedly posting abusive comments about the Prophet Mohamed's wife Aisha on a Bahraini online forum in June 2012.[102] That month another blogger, Mohamed Hasan, was interrogated by police authorities for "writing for websites and newspapers without a license, protesting, and tweeting,"[103] although there is no law in Bahrain that requires a license for blogging. A few days earlier, one of his tweets had appeared on the Al-Jazeera television show 'The Stream.'[104] No further legal action has yet been taken against Hasan.

In August 2012, the 21-year-old blogger Shaheen Al-Junaid was summoned by police authorities for tweeting about an attack by members of the royal family on a Bahraini citizen who worked for their cousin. The employee was beaten after he refused the royal family members entry onto their cousin's premises, which his employer had instructed him to do following a dispute between the family members.[105] The summons was later cancelled.[106]

Four Twitter users were arrested and had their electronic devices confiscated after their houses were raided on the night of October 16, 2012. Abdullah Alhashemi, Salman Darwish, Ali

---

[96] "BAHRAIN: Arrest of Mr. Nabeel Rajab," fidh, July 22, 2012, http://www.fidh.org/BAHRAIN-Arrest-of-Mr-Nabeel-Rajab.
[97] Sara Yasin, "Bahrain activist acquitted of Twitter charges but remains in prison," Index on Censorship, http://www.indexoncensorship.org/2012/08/bahraini-activist-acquitted-of-twitter-charges-but-remains-in-prison/
[98] "Updates: Bahrain, emboldened by international silence, sentences Nabeel Rajab to 3 years imprisonment," Bahrain Center for Human Rights, August 20, 2012, http://www.bahrainrights.org/en/node/5387.
[99] "How the Middle East Tweets: Bahrain's Most Connected," Wamda, December 3, 2012, http://www.wamda.com/2012/12/how-the-middle-east-tweets-bahrain-s-most-connected-report.
[100] "Bitter protests in Bahrain," Movements.org, January 28, 2013, http://www.movements.org/blog/entry/bitter-protests-in-bahrain/.
[101] "Khalifa: Leave the al-Muharraq alley ways, their shaikhs and their elderly, everyone knows that you have no popularity there; and if it was not for their need for money they would not have come out to welcome you - When will you bow out?" https://twitter.com/nabeelrajab/status/208853736494350336.
[102] "Bahrain blogger charged with blaspheming Islam," Bahrain Freedom Index, 2012, accessed September 4, 2013, http://bahrainindex.tumblr.com/post/25638178036/bahrain-blogger-charged-with-blaspheming-islam.
[103] See https://twitter.com/safybh/status/210005542406598657 (@safybh)
[104] "Bahrain blogger @safybh interrogated about his 'goodnight tweets'," Bahrain Freedom Index, 2012, accessed September 4, 2013, http://bahrainindex.tumblr.com/post/25638691193/bahraini-blogger-safybh-interrogated-about-his.
[105] "Investigation with Shaheen Junaid for 'victory' marginal offended by members of the ruling family," Manama Voice, August 11, 2012, http://manamavoice.com/news-news_read-10274-0.html.
[106] "Cancel call to expose the assault on a citizen by the King's cousins," [in Arabic] Bahrain Mirror, December 8, 2012, http://www.bahrainmirror.com/article.php?id=5434&cid=73.

Mohamed Watheqi, and Ali Alhayki, who are not known public figures, were charged with "insulting the king of Bahrain over Twitter." In November 2012, they received sentences ranging from one to six months.[107] At least one of the men has revealed that he was coerced into making a forced confession.[108]

On December 11, 2012, a fifth Twitter user received a four-month sentence for the same charge.[109] According to activists, the identities of these anonymous users were discovered using a technique known as "spear phishing," in which surveillance software was secretly embedded in seemingly innocent private messages to the users, enabling the hackers to remotely access the victims' computers.[110] One of those arrested was a progovernment Twitter user who had criticized the king for not being harsh enough in punishing protestors.[111]

Another wave of arrests took place on March 11 and 12, 2013, when six users, including one lawyer and one minor, were detained over charges of defaming the king over social media.[112] None of the users had a large base of followers; instead, it seemed that the authorities selected them in order to instill fear locally without provoking criticism from the international community.

After months of living in hiding, award-winning photographer Ahmed Humaidan was arrested by 15 undercover policemen on December 29, 2012. Humaidan was accused of participating in an attack on a police station in the district of Sitra,[113] though it is believed that his arrest is in fact due to him photographing protests.[114] Following his arrest, Humaidan was interrogated, blindfolded for two days, and placed in solitary confinement for a week[115] at the General Directorate of Criminal Investigation while being denied access to a lawyer.[116] He was subject to psychological torture and made to believe that a bomb had been placed in his hand that would imminently detonate if he did not produce a confession.[117] Humaidan has been one of many photographers documenting the

[107] "Bahrain: Twitter users sentenced to prison as authorities seek to extend their crack-down on social media websites," Bahrain Center for Human Rights, November 8, 2012, http://www.bahrainrights.org/en/node/5507.
[108] See http://twitter.com/freedomprayers/status/261928988274991104.
[109] "4 months in prison accused of insulting the king via Twitter" [in Arabic], Al Wasat, December 12, 2012, http://www.alwasatnews.com/3749/news/read/722589/1.html.
[110] "Bahrain: How the identities of the tweeps were tracked," Bahrain Freedom Index (Tumblr), accessed December 2012, http://bahrainindex.tumblr.com/post/35839544837/bahrain-how-the-identities-of-the-tweeps-were-tracked.
[111] See https://twitter.com/freedomprayers/status/258927207286722560 and https://twitter.com/jehadabdulla/status/257445077457190912.
[112] The detainees include 17-year-old Ali Faisal Al-Shufa, 33-year-old Hassan Abdali Isa, 26-year-old Mohsen Abdali Isa, 36-year-old Ammar Makki Mohammed Al-Aali, 34-year-old Mahmood Abdul-Majeed Abdulla Al-Jamri, and 25-year-old Mahdi Ebrahim Al-Basri. See "Bahrain: The Authorities Celebrate the World Day against Cyber-censorship by Arresting 6 Twitter Users," Bahrain Youth Society For Human Rights, March 12, 2013, http://byshr.org/?p=1324.
[113] "Public Prosecution / Statement," Bahrain News Agency, January 5, 2013, http://www.bna.bh/portal/en/news/540555.
[114] "Bahrain arrests photographer who documented dissent," Committee to Project Journalists, January 9, 2013, http://www.cpj.org/2013/01/bahrain-arrest-photographer-who-documented-dissent.php.
[115] See https://twitter.com/BHRS2001/status/287932501744304128.
[116] See https://twitter.com/BHRS2001/status/287924826797125634.
[117] "Fake bomb in the hands of photographer Humaidan in order to extract confessions" [in Arabic], Bahrain Mirror, January 12, 2013, http://www.bahrainmirror.com/article.php?id=7363&cid=73.

protests through social media websites such as Flickr and Instagram.[118] He was reportedly sentenced to three years in prison on June 18, 2013.[119]

The Bahraini authorities are remarkably responsive when enforcing the country's tight online restrictions. Human rights activist Said Yousif Al-Muhafdha (@SaidYousif) was arrested only 23 minutes after a photo of a protester's shotgun injury was posted on his Twitter account. The photo identified the injury as having taken place that same day in Manama, though in reality it was taken several days earlier.[120] Al-Muhafdha was indeed monitoring a protest in Manama prior to his arrest, tweeting media and information about attacks on the demonstrators by the police; however, he has denied publishing that particular picture. He was charged under Article 168 of the Penal Code with "willfully disseminating false news" that "resulted in protests and riots that disrupted security and order on the same day."[121] He was detained for one month before being released on bail, pending a trial. On March 11, 2013 the court acquitted him of the charges, stating there was "no proof of [a] connection between the riots and the picture he had posted."[122] However, the public prosecution has appealed against the acquittal and a second trial will start on July 1, 2013, in which Al-Muhafdha could face a prison sentence.[123]

In January 2013, the higher court of cassation upheld a series of harsh sentences originally passed by a military court in June 2011, in which two bloggers were charged with possessing links to a terrorist organization aiming to overthrow the government.[124] They were also accused of disseminating false news and inciting protests against the government. The two users, Abduljalil al-Singace and Ali Abdulemam, had already been detained for six months between September 2010 and February 2011. According to their own court testimonies[125] and media interviews, both were also subject to torture while held.[126] Al-Singace, a prominent human rights defender, has been held in detention since March 17, 2011 and his blog has been blocked since February 2009.[127] He was sentenced to life imprisonment for "plotting to topple" the government in late 2011 and remains in prison.[128] He was not allowed to testify before the court until his appeal, when he revealed that he

[118] See: http://instagram.com/ahmedhumaidan/, http://www.flickr.com/photos/86494560@N05, and http://500px.com/AhmedHumaidan.
[119] See https://twitter.com/FreedomPrayers/status/349607068916924416.
[120] "Bahrain: Light speed investigation leads to arrest of a tweep 23 minutes after sending his criminal tweet!" Manama (Blogspot), December 22, 2012, http://manamacoac.blogspot.com/2012/12/bahrain-light-speed-investigation-leads.html.
[121] "Bahrain: Charges Against Rights Defender Raise Concerns," Human Rights Watch, January 3, 2012, http://www.hrw.org/news/2013/01/03/bahrain-charges-against-rights-defender-raise-concerns.
[122] "Activist cleared of Twitter post," Gulf Daily News, March 12, 2013, http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=349145.
[123] "'Public Prosecution' appeals against the acquittal of AlMuhafdha in the 'false news broadcast' " , Alwasat news, April 13, 2013, http://www.alwasatnews.com/3871/news/read/763690/1.html
[124] "Detained blogger Abduljalil Al-Singace on hunger strike," Reporters Without Borders, September 6, 2011, http://en.rsf.org/bahrain-one-blogger-sentenced-to-life-22-06-2011,40507.html. [125] "Terrorist network first hearing – Trial Testimonies – 28th October, 2010," Bahrain Center for Human Rights, October 29, 2010, http://bahrainrights.hopto.org/en/node/3540.
[125] "Terrorist network first hearing – Trial Testimonies – 28th October, 2010," Bahrain Center for Human Rights, October 29, 2010, http://bahrainrights.hopto.org/en/node/3540.
[126] Ali Abdulemam describes the way he was tortured (minute 09:37), "People & Power – Bahrain: Fighting for change," Al Jazeera English, March 9, 2011, http://www.youtube.com/watch?v=IZdyiK-Z5Do.
[127] http://www.bahrainrights.org/en/node/2752. Alsingace's blog is http://alsingace.katib.org.
[128] "Bahrain upholds lengthy prison terms for journalists," Committee to Protect Journalists, September 28, 2011, http://cpj.org/2011/09/bahrain-1.php.

had been subject to torture.[129] Ali Abdulemam, the owner of Bahrain's most popular online forum, Bahrainonline.org, had been in hiding since March 17, 2011 during which time he was sentenced (in absentia) to 15 years of prison.[130] However, he suddenly re-emerged in May 2013, having escaped Bahrain to the United Kingdom through Saudi Arabia, Kuwait, and Iraq.[131]

Five policemen were put on trial for the death of the online journalist and moderator of the Al-Dair online forum, Zakaryia Al-Ashiri, who died from torture while in police custody on April 9, 2011.[132] However, after a lengthy trial that lasted from January 2012 until March 2013, the court acquitted all of those accused, furthering the widely held belief that members of Bahrain's security apparatus enjoy impunity for crimes against protestors.[133]

Students and employees have received disciplinary action for comments they have communicated via private text messages and social media. In May 2012, a student of the University of Bahrain was suspended for a semester after writing 'phrases that insult His Majesty the King' on her mobile phone and sending them to her colleagues. She was reported to the university management by one of the recipients of her message.[134]

Given that users can be prosecuted for being identified with an offending post or text, many users are concerned about restrictions on using ICT tools anonymously. The TRA requires users to obtain licenses to use Wi-Fi and WiMAX connections,[135] and the government prohibits the sale or use of unregistered (anonymous) prepaid mobile phones. The country's cybercafes are also subject to increasing surveillance. Oversight of their operations is coordinated by a commission consisting of members from four ministries, who work to ensure strict compliance with rules that prohibit access for minors and require that all computer terminals are fully visible to observers.[136]

Since March 2009, the TRA has mandated that all telecommunications companies must keep a record of customers' phone calls, e-mails, and website visits for up to three years. The companies are also obliged to provide the security services access to subscriber data upon request.[137] Since the application of "National Safety Status" (emergency law) in March 2011, citizens have been forced to

[129] The full testimony of Dr Abduljalil AlSingace before the higher court of appeal on 29 May 2012 (Arabic) http://bahrainrights.hopto.org/BCHR/wp-content/uploads/2012/06/AJ.docx.
[131] Peter Beaumont, "Bahrain Online founder Ali Abdulemam breaks silence after escape to UK," The Guardian, May 10, 2013, http://www.guardian.co.uk/world/2013/may/10/bahrain-online-ali-abdulemam-escape.
[131] Peter Beaumont, "Bahrain Online founder Ali Abdulemam breaks silence after escape to UK," The Guardian, May 10, 2013, http://www.guardian.co.uk/world/2013/may/10/bahrain-online-ali-abdulemam-escape.
[132] "Zakariya Rashid Hassan al-Ashiri," Committee to Protect Journalists, April 9, 2011, http://cpj.org/killed/2011/zakariya-rashid-hassan-al-ashiri.php.
[133] "After a year-long show trial: no one is found guilty for killing blogger under torture in police custody," Bahrain Center for Human Rights, March 13, 2013, http://www.bahrainrights.org/en/node/5673.
[134] Brian Dooley, "Bahrain Student Suspended for Phone Message," Human Rights First, June 4, 2012, http://www.humanrightsfirst.org/2012/06/04/bahrain-student-suspended-for-phone-message/.
[135] Geoffrey Bew, "Technology Bill Rapped," Gulf Daily News, July 20, 2006, http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=149891.
[136] Reporters Without Borders, "Countries Under Surveillance: Bahrain."
[137] "'Big Brother' Move Rapped," Geoffrey Bew, *Gulf Daily News*, March 25, 2009, http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=246587.

allow security personnel to search their mobile phones at checkpoints. Recent instances of this behaviour continue to be documented on YouTube.[138]

In May 2011, new units were created within the IAA to monitor social media and foreign news websites. According to the IAA's director of publishing, the initiative aims to "further help project the kingdom's achievements and respond to false information that some channels broadcast."[139] Although Bahraini cyberspace is highly monitored, no actions have been taken against the dozens of progovernment users who continue to spread online threats against activists.[140] Some of these users have publically defamed citizens by using social media to identify the faces of protestors and circulate lists of "traitors."[141] It is common for users tied to the opposition movement to receive these types of extralegal attacks in a bid to disrupt their activities.

In July 2012, researchers discovered malicious software concealed in seemingly innocent emails sent to Bahraini activists in April and May 2012. The surveillance software, named "FinFisher," is developed by the Munich-based Gamma International GmbH and distributed by its U.K. affiliate, Gamma Group. One aspect of the software, "FinSpy," can remotely and secretly take control of a computer, taking screen shots, intercepting Voice-over-Internet-Protocol (VoIP) calls, and transmitting a record of every keystroke.[142] The company has denied that it has sold its products to the Bahraini government, claiming that the version of FinSpy deployed on activists was "old" and for demonstration purposes only. However, evidence compiled by internet watch groups shows that a newer version of the FinSpy software is also in use in Bahrain, suggesting the government is receiving paid updates from the company.[143] Since 2010, evidence has also emerged surrounding the use of spy gear maintained by Nokia Siemens Networks (NSN) and its divested unit, Trovicor GmbH, to monitor and record phone calls and text messages.[144]

Cyberattacks against both opposition and progovernment pages, as well as other websites, are common in Bahrain. For example, in June 2012 a Facebook news page that belongs to opposition

[138] See video: http://bahrainindex.tumblr.com/post/39738010314/policeman-checking-the-private-mobile-content-of-a.
[139] Andy Sambridge, "Bahrain sets up new units to monitor media output," Arabian Business, May 18, 2011, http://www.arabianbusiness.com/bahrain-sets-up-new-units-monitor-media-output-400867.html?parentID=401071.
[140] "Bahrain: Death threats against Messrs. Mohammed Al-Maskati, Nabeel Rajab and Yousef Al-Mahafdha," World Organization Against Torture, December 7, 2011, http://www.omct.org/human-rights-defenders/urgent-interventions/bahrain/2011/12/d21549/.
[141] See https://twitter.com/Jalad_Almajoos/status/292638655217020929. For a well-documented account of the defamation of opposition activists, please refer to Mahmoud Cherif Bassiouni et al., "Report of the Bahrain Independent Commission of Inquiry," Bahrain Independent Commission of Inquiry (BICI), November 23, 2011, paragraph 1597, http://files.bici.org.bh/BICIreportEN.pdf.
[142] Vernon Silver, "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma," Bloomberg, July 25, 2012, http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html and "From Bahrain With Love: FinFisher's Spy Kit Exposed," CitizenLab, July 25, 2012, http://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/.
[143] "You Only Click Twice: FinFisher's Global Proliferation," CitizenLab, May 13, 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.
[144] Vernon Silver and Ben Elgin, "Torture in Bahrain Becomes Routine With Help From Nokia Siemens," Bloomberg, August 22, 2011, http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.

activists was taken over by a progovernment group.[145] Similarly, a progovernment website, b4bh.com, was hacked in August 2012 for the second time by opposition activists.[146] Government-associated websites are frequently targeted with distributed denial of service (DDoS) attacks, with the most recent instance occurring on May 17, 2012 following the arrest of activist Nabeel Rajab. The main perpetrator of such attacks has been the group "Anonymous," which launched "Operation Bahrain" through a press release published on February 17, 2011.[147]

[145] See Bahrainforums.com, June 8, 2012, https://bahrainforums.com/vb/%E5%E4%C7-%C7%E1%C8%CD%D1%ED%E4/978431.htm .
146 "Opponenets of Bahrain infiltrate locations belonging to the government," [in Arabic], Jurnaljazira.com, August 11, 2012, http://www.jurnaljazira.com/news.php?action=view&id=4834.
[147] "Anonymous hits Bahrain after arrest of human rights activist Nabeel Rajab," Examiner, May 5, 2012, http://www.examiner.com/article/anonymous-hits-bahrain-after-arrest-of-human-rights-activist-nabeel-rajab.

BANGLADESH

	2012	2013
INTERNET FREEDOM STATUS	N/A	PARTLY FREE
Obstacles to Access (0-25)	n/a	13
Limits on Content (0-35)	n/a	12
Violations of User Rights (0-40)	n/a	24
Total (0-100)	**n/a**	**49**

* 0=most free, 100=least free

POPULATION: 153 million
INTERNET PENETRATION 2012: 6 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Secularist blogger Ahmed Rajib Haider was murdered after calling for and promoting protests against a convicted Islamist war criminal online (see **VIOLATIONS OF USER RIGHTS**).
- Police charged four bloggers with harming religious sentiment under the ICT Act 2006 (see **VIOLATIONS OF USER RIGHTS**).
- Regulators blocked YouTube for nine months after the anti-Islamic "Innocence of Muslims" video sparked widespread criticism in September 2012; not all ISPs complied (see **LIMITS ON CONTENT**).

INTRODUCTION

As an emerging economy, Bangladesh has recognized information communication technologies (ICTs) as core tools for development. Even with new media still a comparatively recent phenomenon, however, officials have sought to control and censor online content—particularly as the internet took center stage in major social and political events in 2012 and 2013.

Since opening up the country's electronic media to the private sector in the early 1990s, the government has, at least officially, encouraged open internet access and communication. The ruling Bangladesh Awami League under Prime Minister Sheikh Hasina is working towards a "knowledge based networked society" under the "Digital Bangladesh by 2021" program launched in 2009.[1] The program seeks to integrate internet access with development efforts in national priority areas, such as education, healthcare, and agriculture. Private commercial stakeholders have also helped in the proliferation of net usage. Bangladesh further benefits from a vibrant—though often partisan—print and audio-visual media industry, but traditional journalists face physical threats and regulatory constraints that are increasingly being replicated online.

Religious sentiments and ICTs were both subject to manipulation, which led to major violations to internet freedom during the coverage period of this report. Authorities seemed ill-prepared at both policy and regulatory levels for the turbulent political developments and used a combination of punitive laws and ad hoc directives to curb expression on the internet, even while failing to offer adequate protection to individuals and websites under threat for their online activities. Police arrested four bloggers on the charge of harming religious sentiment, and regulators shut down their blogs without a court order. YouTube was inaccessible for nine months after the government blocked it in response to anti-Islamic content posted in 2012.

In October 2012, journalists traced attacks targeting Buddhist neighborhoods in the southeastern district of Ramu to a Buddhist's Facebook profile apparently altered to display anti-Islamic images and incite local Muslims to retaliate; it's not clear who was responsible for the alleged manipulation.[2] In February 2013, domestic tensions escalated when a war crimes tribunal sentenced Abdul Quader Mollah, leader of the country's largest political Islamic party Jamaat-e-Islami, to life imprisonment for crimes committed during the country's 1971 war of independence with Pakistan, including mass murder and rape.[3] Some thought the sentence was lenient, and tens of thousands of protesters gathered around the Shahbag intersection in the capital, Dhaka, for more than two months. Traditional social, cultural, and pro-independence political forces later joined and strengthened the non-violent demonstration, causing some observers to compare it to the 2011 protests in Egypt's Tahrir Square.[4] The Shahbag Movement, as it became known, was facilitated by

[1] "Digital Bangladesh Strategy Paper, 2010," Access to Information Program, Prime Minister's Office, The People's Republic of Bangladesh, http://www.a2i.pmo.gov.bd/tempdoc/spdbb.pdf.
[2] "A Devil's Design," *The Daily Star*, October 14, 2012, http://bit.ly/1eQ4GBn.
[3] Tamima Anam, "Shahbag Protesters Versus the Butcher of Mirpur," *The Guardian*, February 13, 2013, http://www.guardian.co.uk/world/2013/feb/13/shahbag-protest-bangladesh-quader-mollah.
[4] Saurabh Shukla, "Shahbag Square Cheers for Change: Dhaka's Young Protesters Demand Ban on Extremism and Death for War Criminals," *Daily Mail*, February 28, 2013, http://dailym.ai/18e9tHR.

blogs, Facebook, and Twitter, a convincing display of the power of ICTs to mobilize and disseminate information.[5] Its opponents certainly thought so: Mollah's supporters rallied in response against a conspiracy by "atheist bloggers."[6] On February 11, a pro-Jamaat-e-Islami blog identified blogger Ahmed Rajib Haider as a Shahbag ringleader; armed assailants attacked and killed Rajib outside his home four days later. These were troubling developments for a country still striving to become a part of the connected global community.

OBSTACLES TO ACCESS

The International Telecommunication Union reported internet penetration in Bangladesh at 6 percent in 2012.[7] Government estimates were closer to 20 percent.[8] Over 90 percent of users access the internet through GPRS/CDMA services, which local regulators classify as narrowband. The remainder subscribe to fixed lines, either through a traditional Internet Service Provider (ISPs) or via one of two WiMax operators.[9]

The government has established 4,501 Information Centers all over Bangladesh, with the goal of ensuring cost-effective internet access and related e-services for the base of the pyramid population.[10] No specific study has been done yet to analyze the user breakdown between urban and rural population.

Mobile penetration was at 64 percent in 2012, with connections provided by six operators.[11] Grameen Phone, owned by Telenor, is the market leader with 42 percent of the total customer base, followed by Orascom's Banglalink with 26 percent, and Robi, under the Axiata company, with 21 percent. The remaining three—Airtel, Citycell, and the state-owned Teletalk—have a total customer base of 10 percent.[12] Right now, Teletalk is the only entity offering mobile broadband to its comparatively small user base. Other operators offer 2G services, as the government is yet to provide licenses for 3G/4G operations.

While ICT usage is increasing fast, Bangladesh is lagging behind globally. The World Economic Forum's 2013 global IT report ranked Bangladesh 114 out of 144 countries worldwide, with infrastructure and the regulatory environment scoring poorly, though overall communication

[5] The movement's demands were diverse, including the death sentence for the war crimes conviction, and banning the Bangladesh Jamaat-e-Islami party from politics. See, "Shahbag Grand Rally Demands Hanging to War Criminals, Banning Jamaat (Updated)," *The Independent* (Dhaka), February 8, 2013, http://bit.ly/18zoSTZ.
[6] Al Jazeera, "Bangladesh Opposition Protests turn Deadly," February 22, 2013, http://aje.me/XF7s1z.
[7] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[8] Association of Mobile Telecom Operators of Bangladesh, "Telecom and ICT: Key Enablers for Economic Development," presentation, March 25, 2013, www.amtob.org.bd.
[9] Faheem Hussain, "License Renewal of Mobile Phone Services: What a Country Should Not Do (A Case Study of Bangladesh)," Telecommunication Policy Research Conference, George Mason University, VA, USA, September 21-23, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2032127.
[10] Faheem Hussain, "ICT Sector Performance Review for Bangladesh," *LIRNEasia*, 2011. Abstract available: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2013707.
[11] International Telecommunication Union, "Mobile-cellular Telephone Subscriptions, 2000-2012."
[12] Bangladesh Telecommunication Regulatory Commission, accessed March, 2013, http://www.btrc.gov.bd/.

service was comparatively affordable, a factor that is driving growth.[13] In addition, the ability to access localized information and create content in Bengali has contributed to the popularity of local blog hosting services.[14]

Bangladesh's physical internet infrastructure has been vulnerable to frequent disconnection, since the country historically relied on a single undersea cable (SEA-ME-WE-4) for its backbone.[15] In late 2012, however, Bangladesh became connected to an international terrestrial cable managed by private companies, reducing the country's the risk of being completely cut off from the "information superhighway."[16]

The Bangladesh Telecommunication Regulatory Commission (BTRC), established under the Bangladesh Telecommunications Act of 2001, is the official regulatory body overseeing telecommunication and related ICT issues. However, the current administration amended the act in 2010, passing control of regulating the telecommunication sector to the Ministry of Post and Telecommunications and making the BTRC an auxiliary organization.[17] This move created administrative delays in a number of basic processes like the announcement of new tariffs or license renewals.[18] In addition, the prime minister's office has an Access to Information (A2I) program, supported by the United Nations Development Program, which has considerable influence over top-level ICT-related decision making.[19]

LIMITS ON CONTENT

The BTRC blocked access to YouTube for nearly nine months in 2012. While it had blocked social media and communication apps in the past, some fear the anti-Islamic video that prompted the censorship was merely a pretext for officials to exert more control over online content. This fear grew in 2013. As the Shahbag movement showed online mobilization gaining force, BTRC officials—without a court order—directed local blog hosts to remove four blogs for alleged anti-religious content, apparently at the behest of religious groups. In another worrisome development, a Facebook page containing a religious insult launched violent attacks on Buddhist minorities and their establishments in Ramu. A newspaper subsequently reported that the page had been doctored to incite retaliation.

The BTRC censors content relating to religious issues or that offends state leaders primarily by issuing informal orders to domestic service providers, who are legally bound through their license

[13] Beñat Bilbao-Osorio, Soumitra Dutta, and Bruno Lanvin, "The Global Information Technology Report 2013," World Economic Forum, http://reports.weforum.org/global-information-technology-report-2013/.
[14] Interview with Syeda Gulshan Ferdous Jana, founder of *Somewhereinblog*, April 2013.
[15] Hussain, "ICT Sector Performance Review for Bangladesh."
[16] "Bangladesh Connected with Terrestrial Cable," *BDNews24*, December 8, 2012, http://bit.ly/1fyvt6J.
[17] S.M. Shahidul Islam and Abdullah-Al Monzur Hussain, "Bangladesh Telecommunication (Amended) Act, 2010," *Manual of Cyber Law in Bangladesh*, (Dhaka: Central Law Book House, 2011), 241-264.
[18] Faheem Hussain, "Telecom Regulatory Environment in Digital Bangladesh: Exploring the Disconnects Between Public Policies/Regulations and Real World Sector Performance," Sixth Communication Policy Research South Conference by LIRNEasia and Chulalongkorn University, Bangkok, 2011.
[19] "Access to Information Program," UNDP in Bangladesh, accessed in June, 2013, http://bit.ly/1biN3ty.

and operations agreements to cooperate. Service providers describe official censorship as ad hoc in nature, without proper follow up mechanisms in place to ensure whether the imposed restrictions have been carried out or not.[20] In addition, online news providers do not have the government recognition granted to traditional, licensed, press organizations, leaving them in regulatory limbo.
International social media and communication apps like Facebook and YouTube are regular victims of government censorship in Bangladesh. Facebook is one of the most visited websites in the country,[21] attracting more than 10 percent of the nation's total internet users.[22] The entire platform has been blocked several times, for periods ranging from a few hours to a few days at a time, though the process by which this decision is made and implemented is not known. Government officials justify such actions as necessary to "contain negative campaigns" on social networks.[23]

Google services, particularly its search engine and video-sharing website YouTube, also enjoy a high volume of user traffic. Despite its popularity, the BTRC blocked access to YouTube in Bangladesh from September 2012 to May 2013 in response to a 14-minute derogatory video about Islam titled, "The Innocence of Muslims."[24] The video, uploaded in the United States in summer 2012, incited violent anti-American protests in Bangladesh, among other predominantly Muslim nations.[25] Google temporarily blocked versions of the video in some countries, apparently on grounds that the content broke local laws, but declined to do so in Bangladesh.[26] Some critics said the length of the ban in Bangladesh indicates the disputed video was a pretext for officials to gain control over the video-sharing platform, which they have blocked in the past for politically sensitive content.[27] However, the impact of the censorship was less severe than the duration implies, since some ISPs informally unblocked the platform after just a few weeks. Other internet users continued to access it using proxy servers. So far, the BTRC has not sought to block software that allows users to circumvent content blocking.

Domestically-hosted websites, including the most popular news sites, *Prothom Alo*, *BDNews24*, and *Banglanews24,* have yet to face any targeted blocking. However, in March 2013, the government formed an official committee to identify bloggers who had allegedly demeaned the spirit of Islam.[28] The committee participated in discussions with clerics to produce a list of bloggers and Facebook users they alleged had published anti-Islamic blasphemy.[29] Though there were more than 80 names

[20] Author interviews with seven experts in Bangladesh who requested anonymity, early 2013.
[21] Alexa, "Top Sites in Bangladesh," accessed May, 2013, http://www.alexa.com/topsites/countries/BD.
[22] Social Bakers, "Bangladesh Facebook Statistics," accessed May 2013, http://bit.ly/lKcscJ.
[23] Ariful Faisal, "Facebook Opens After a Short Period Block," *Priyo*, February 28, 2012, http://bit.ly/16Jwtuo.
[24] Abdullah Mamun, "YouTube Blocked in Bangladesh," *The Daily Star*, September 18, 2012, http://bit.ly/1azjwHF.
[25] Mamun, "YouTube Blocked in Bangladesh."
[26] Arun Devnath & Haris Anwar, "Pakistan, Bangladesh Block YouTube; Saudis May Follow," Bloomberg News, September 20, 2013, http://www.bloomberg.com/news/2012-09-18/pakistan-bangladesh-block-youtube-to-restrict-anti-islam-film.html.
[27] Zafar Sobhan, "YouTube is Still Banned in Bangla," *The Sunday Guardian*, October 27, 2012, http://www.sunday-guardian.com/analysis/youtube-is-still-banned-in-bangla. Authorities have instigated politically-motivated, though temporary blocks on YouTube in the past. See: BBC News, "Bangladesh Imposes YouTube Block," March 9, 2009, http://news.bbc.co.uk/2/hi/7932659.stm.
[28] Global Voices Advocacy, "Bangladesh Authorities Go After 'Anti-Muslim' Bloggers," April 1, 2013, http://advocacy.globalvoicesonline.org/2013/04/01/bangladesh-authorities-go-after-anti-muslim-bloggers/.
[29] "*Churashi Bloggerer Talika Shorastro Montronaloye*," [Home Ministry has the List of Eighty-four Bloggers], *NatunBarta*, March 31, 2013, http://www.natunbarta.com/si-tech/2013/03/31/18939/.

on the list, the BTRC subsequently directed domestic blog hosting platforms to close the accounts of just four bloggers it identified as "anti-religious elements." All four were prominently involved in the Shahbag movement, which had come into conflict with ultra-religious groups as well as the administration, which they accused of poor governance. The owners of the host platforms reported that officials never used any court orders or legal explanations during their communications.[30] Officially, the legal system ensures the right to appeal against most government decisions, but the lack of a warrant, as well as the risk of losing a license or legal permission to operate, makes mounting such an appeal challenging, and so far none have been documented in response to censorship directives.

Such strict and opaque content regulation has resulted in self-censorship by social media users, bloggers, and online news media. In particular, the developments of the last year have made discussion of religious issues more sensitive. More positively, there has been no evidence of government officials proactively manipulating online content. Some unknown actors, however, apparently orchestrated an outbreak of religious violence in the Ramu area of southeastern Chittagong based on a Facebook profile. In September 2012, members of the local Muslim majority community accused a Buddhist of displaying an anti-Islamic image on his Facebook profile and launched retaliatory attacks that destroyed a dozen temples. *The Daily Star* newspaper reported in October that the image had been added to the Facebook profile, then shown to Muslims both online and off, falsely creating the impression that local Buddhists were sharing blasphemous material. No police investigation was launched into the alleged manipulation, and the page's owner was forced to flee the area.[31]

Despite recent restrictions and uncertainties, there are around 200,000 active bloggers in Bangladesh, and this number is growing. The BTRC has identified 48 active domestic blog hosting platforms. Leading examples, based on subscriber figures, include SomewhereinBlog, Amarblog, and Shocholayoton.[32]

The Shahbag Movement, which was initiated by the Bangladesh Online Activists' Network, is the country's most significant example of online activism to date. The protests coalesced around the International Crimes Tribunal verdict against the Jamaat-e-Islami leader (see Introduction) but quickly took on a political element.[33] In its early stages, however, the movement spread through blogging, Facebook, and mobile telephony.[34] Twitter, previously little-used in Bangladesh, gained popularity as a tool to broadcast information about Shahbag, both domestically and internationally.[35]

---

[30] Global Voices Advocacy, "Bangladesh Authorities Go After 'Anti-Muslim' Bloggers."
[31] "A Devil's Design," *The Daily Star*, October 14, 2012, http://bit.ly/1eQ4GBn.
[32] "Blog," *Daily Manab Zamin*, April 4, 2013, http://bit.ly/17cIexA.
[33] Mohammad Shahid Ullah, "Shahbagh People's Movement: New Generation Challenging the Unjust Structure," *Voice of the Oppressed*, February 18, 2013, http://www.voiceoftheoppressed.in/tag/bangladesh-online-activist-network/.
[34] Tamanna Khan, "Shahbag Beyond Boundaries," *The Daily Star*, March 29, 2013, http://bit.ly/18zMyW8.
[35] Faheem Hussain, Zyma Islam, and Mashiat Mostafa, "Proliferation of Twitter for Political Microblogging in a Developing Country: An Exploratory Study of #Shahbag," (unpublished research funded by the Asian University for Women Faculty Research Fund, 2013).

VIOLATIONS OF USER RIGHTS

The February 2013 murder of blogger Ahmed Rajib Haider by armed assailants after an ultra-religious blog identified him as a Shahbag organizer was one of the most shocking developments during the coverage period for this report. While the government offered to protect some secularist bloggers from the hate speech spiraling out of control online in the wake of the Shahbag movement, it clouded that message by arresting four of them, including one who had been stabbed just a few months before, in April. Domestic online news sites faced cyber-attacks during periods of heightened religious contention.

Article 39 (1, 2) of Chapter 2 in the Bangladeshi constitution recognizes freedom of thought, conscience, and speech as a fundamental right.[36] Online expression has been traditionally considered to fall within the scope of this provision. The Information and Communication Technology Act of 2006 is the primary legal reference for addressing issues related to internet usage, in addition to defining and protecting freedom of expression online; it also penalizes citizens who violate others' rights to communicate electronically.[37] In addition, the amended Bangladesh Telecommunication Act of 2010 allows officials to intercept electronic communications from any individual or institution to ensure the security of the state or public order.[38] The judicial system of Bangladesh is independent from the executive and the legislative branches of government, but critics say it can be partisan, and police and regulators generally bypass the courts to implement censorship and surveillance without oversight.[39]

Section 56 of the ICT Act defines hacking as a crime punishable by up to three years in prison, a fine of BDT 10,000,000 ($ 125,000), or both. Section 57 is vaguer, and characterizes different types of religious, social or political expression made electronically as potential violations. People found guilty under this section face a maximum of 10 years imprisonment and fines up to BDT 10,000,000 ($125,000).[40]

The first arrests made using these clauses took place in 2013. On April 1, as regulators were shutting down their websites, police detained bloggers Rasel Parvez, Mashiur Rahman Biplob, and Subrata Ashikari Shuvo. Two days later they also detained Asif Mohiuddin, author of a renowned blog on sensitive sociopolitical issues that won a user-nominated award from German broadcaster Deutsche Welle in 2012.[41] Just a few months before his arrest, in January 2013, Mohiuddin was

[36] S.M. Shahidul Islam and Abdullah-Al Monzur Hussain, "Right to Information Act, 2009", *Manual of Cyber Law in Bangladesh*, (Dhaka, Central Law Book House, 2011) 1-47.
[37] S.M. Shahidul Islam and Abdullah-Al Monzur Hussain, "Information and Communication Technology Act, 2006," *Manual of Cyber Law in Bangladesh*, (Dhaka, Central Law Book House, 2011) 90-91.
[38] Bangladesh Telecommunication (Amended) Act, 2010.
[39] "The Historic Masdar Hossain Case and the Independence of Judiciary of Bangladesh: A Compilation," *Wahab Ohid Legal Aid*, March 12, 2013, http://wahabohidlegalaid.blogspot.com/2013/03/the-historic-masdar-hossain-case-and.html; M. Moneruzzaman, "Judiciary Independence Still on Paper," *The Bangladesh Chronicle*, January 15, 2013, http://www.bangladeshchronicle.net/index.php/2013/01/judiciary-independence-still-on-paper/.
[40] Information and Communication Technology Act, 2006.
[41] Emran Hossain, "Bangladesh Arrests 'Atheist Bloggers,' Cracking Down on Critics," *Huffington Post*, April 3, 2013,

hospitalized with serious stab wounds, apparently inflicted by armed assailants in reprisal for his writing and activism.[42] All four bloggers were charged with harming religious sentiment under Section 57(2) of the ICT Act 2006, and conservative political forces branded them as anti-Islamic atheists, though activists defended them.[43] The bloggers were later released on bail, though Asif Mohiuddin's application was initially denied until he appealed on medical grounds in June.[44] A judge declined to extend bail beyond one month, and he was re-arrested in July.[45]

Also in April, police arrested Mahmudur Rahman, acting editor and majority owner of the pro-opposition newspaper *Amar Desh*, on charges that included defaming religion under ICT Act sections 56 and 57.[46] The case was the latest in dozens of investigations involving Rahman that his supporters characterize as politically motivated. In 2012, he was charged with sedition in relation to his paper's publication of private Skype communications involving an International Crimes Tribunal judge that cast doubt on the integrity of the tribunal's judgments;[47] the judge issued a court order against the U.K.-based *Economist* magazine in the same case, though much of the material was leaked online in Bangladesh.[48]

The threat of sedition charges—which carry a possible death penalty—has been used against others for online activity. In October 2012, Australian immigration authorities granted asylum to Muhammad Ruhul Khandaker after a court in Bangladesh recommended he be charged with sedition for a comment he posted to his personal Facebook account while living in Australia.[49] In January 2012, the court had sentenced Khandaker in absentia to six months in jail for contempt of court when he failed to attend a hearing in Dhaka in relation to the comment, which was considered insulting to Prime Minister Sheikh Hasina.[50]

At present, the government allows anonymous access and web posting, and does not require website owners, bloggers, or internet users to register. However, even though people can post comments online without revealing their true identities, they are susceptible to surveillance. Under the 2010 Telecommunication Act, regulators have the power to intercept any communication—

---

http://www.huffingtonpost.com/2013/04/03/bangladesh-bloggers_n_3009137.html; Arafatul Islam, "Bangladesh Gags Award-winning Blogger," Deutsche Welle, March 25, 2013, http://dw.de/p/183px.

[42] "Blogger Knifed in Dhaka," *BDNews24*, January 14, 2013, http://bit.ly/10vt99p.

[43] "'Bloggers' to be Charged under ICT Act," *BDNews24*, April 4, 2013, http://bdnews24.com/bangladesh/2013/04/02/bloggers-to-be-charged-under-ict-act. See also, Rezwan, "Bloggers in Bangladesh Face Threats Online and Off," *Slate, Future Tense* (blog), April 4, 2013, http://slate.me/Y0KiBE.

[44] "Bloggers Shuvo, Parvez Released," *The Daily Star*, May 12, 2013 http://www.thedailystar.net/beta2/news/bloggers-shuvo-parvez-get-bail/; Md Sanaul Islam Tipu, "Blogger Moshiur Granted Bail," *Dhaka Tribune*, June 2, 2013; http://bit.ly/13d88yi; "Blogger Asif Mohiuddin Gets Bail", *BDNews24*, June 27, 2013, http://bit.ly/18zMRQY.

[45] "Blogger Asif sent to jail again," *The Daily Star*, July 29, 2013, http://bit.ly/15qApCO.

[46] "Mahmudur Rahman Arrested Under ICT Act: MK Alamgir," *The Independent* (Dhaka), April 11, 2013, http://bit.ly/1fRgQZH.

[47] T.J., "Press Freedom in Bangladesh: "In the Best Interest of the Media,"" *Banyan* (blog), *The Economist,* May 25, 2013, http://www.economist.com/blogs/banyan/2013/05/press-freedom-bangladesh.

[48] *Economist,* "The Trial of the Birth of a Nation," December 15, 2012, http://econ.st/RpQnK7.

[49] Adam Gartrell, "Bangladeshi Gets Asylum over Facebook Case," Australian Associated Press, November 27, 2012, http://news.smh.com.au/breaking-news-national/bangladeshi-gets-asylum-over-facebook-case-20121127-2a5b9.html.

[50] Amanda Hodge, "Student, Muhammad Ruhul Khandaker, Fears Death Penalty for Facebook Comment," *The Australian*, January 10, 2012, http://bit.ly/woBd2q.

voice or data—over the telecom network without a court order.[51] Both data and voice service providers are required by law to aid the government in monitoring the user communications.[52] Meanwhile, citizens must provide their national identity card and related personal information to obtain a mobile connection.

The BTRC has also been using methods such as deep-packet inspection to identify "unlawful and sensitive information" sent over the internet, according to news reports.[53] The government has yet to define "unlawful" or "sensitive," but no abuse of deep-packet inspection has been documented. There is no independent oversight body in Bangladesh to guard against the abuse of surveillance options initiated by the government.

The physical safety of journalists and media personnel is at risk in Bangladesh, with three journalists killed in 2012.[54] Bloggers and online news providers have also suffered from physical attacks, and reported an increasing number of threats in the past year from different groups, perhaps in response to intensifying activism by the Shahbag Movement and others. The government's response was contradictory, supporting the pro-independence, secular bloggers against the threats of anti-Shahbag elements, while arresting some known, pro-Shahbag online activists for insulting Islam.

On February 15, 2013, during the peak of the Shahbag Movement, one of the group's leading activists, Ahmed Rajib Haider, was brutally murdered by suspected religious extremists.[55] Police found a series of posts targeting Rajib and other key figures in the movement on the blog, Sonar Bangladesh, which the BTRC subsequently blocked.[56] The first of such posts was against Rajib, whose critical stance against religious extremism apparently offended them. On March 1, five people police described as religious extremists were detained in connection with Rajib's murder.[57] On April 1, 2013, police arrested four suspects in relation to the attack on Asif Mohiuddin, also linking them with religious extremism.[58]

Cyberattacks on key government websites, online news sites, and blogs are also on the rise. News sites *The Daily Star*, *Prothom Alo*, *BDNews24*, and *Banglanews24* have regularly been victims of hacking and related cyberattacks by third parties; *Prothom Alo* and the London-hosted *UKBDNews* website

[51] Abu Saeed Khan, presentation in "Third South Asian Meeting on the Internet and Freedom of Expression," Dhaka, Bangladesh, 14-15 January 2013.
[52] Bangladesh Telecommunication (Amended) Act, 2010.
[53] Ashraf Khan, "*Cyber Crime Niyontrone Paanch Koti Takar Device*" [The Device Forth Five Crore to Control Cyber Crime], *Daily Manab Zamin*, April 20, 2013, http://bit.ly/1biMIHp.
[54] The motive for the murder was definitely related to journalism in one case; it remains unconfirmed in the other two. See, Committee to Protect Journalists, "14 Journalists Killed in Bangladesh since 1992," http://www.cpj.org/killed/asia/bangladesh/, accessed July 2013.
[55] "Blogger Brutally Killed," *The Daily Star*, February 16, 2013, http://archive.thedailystar.net/newDesign/news-details.php?nid=269336.
[56] "12 Blogs, Facebook Pages Blocked," *BDNews24*, February 20, 2013 http://dev-bd.bdnews24.com/details.php?id=240964&cid=2.
[57] "Blogger Rajib Killing - Mastermind Shibir man," *The Daily Star*, March 3, 2013 http://archive.thedailystar.net/newDesign/news-details.php?nid=271147.
[58] "4 Held For Attacking Blogger Asif," *BDNews24*, April 1, 2013, http://bdnews24.com/bangladesh/2013/04/01/4-held-for-attacking-blogger-asif.

reported being infected with malware in February 2013,[59] while *The Daily Star* site was attacked by Anonymous in March.[60] The youth population has turned out to be the most vulnerable group against any privacy violations, predominantly through mobile phones and the internet.[61] People are slowly realizing the importance of protecting their online presence against any outside, unlawful intrusion. ISPs informally organized a Bangladesh Cyber Emergency Response Team and are working towards dealing with cyberattacks, hacking, and other malicious threats.[62] In addition, the Bangladesh government has established its own response mechanism to deal with such issues.

[59] Eqramul Islam, "Prothom-alo Spreading Viruses, ukbdnews.com Under Attack," *UKBD News*, February 19, 2013 http://ukbdnews.com/english/1119-prothom-alo-spreading-viruses-ukbdnewscom-under-attack.html.
[60] "Daily Star Website Hacked," *Daily Sun*, March 5, 2013 http://www.daily-sun.com/details_yes_05-03-2013_Daily-Star-website-hacked_428_1_0_3_32.html.
[61] Faheem Hussain and Mohammad Sahid Ullah, "Mobile Communication and Internet in Bangladesh: Is Privacy at Risk for Youth Population?" *Media Watch*, Centre for Communication Studies, 2013
[62] Bangladesh Cyber Emergency Response Team, accessed April, 2013, http://www.bdcert.org/v2/.

BELARUS

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	16	16
Limits on Content (0-35)	23	22
Violations of User Rights (0-40)	30	29
Total (0-100)	**69**	**67**

* 0=most free, 100=least free

POPULATION: 9.5 million
INTERNET PENETRATION 2012: 47 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Change.org, an online petition platform, was blocked for two weeks in August 2012, possibly in connection with a petition that supported the release of two citizens who had been unjustly arrested (see **LIMITS ON CONTENT**).
- The overall number of online users arrested declined in comparison to the mass arrests that occurred during the spring 2011 protests; however, government persecution of online activists became more targeted as arrests and detentions were more directly linked to users' online activities (see **VIOLATIONS OF USER RIGHTS**).
- Each of the three major cases of criminal prosecution against media practitioners concerned internet publications (see **VIOLATIONS OF USER RIGHTS**).
- Instances of technical attacks against the websites of independent media and civil society groups continued to grow (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

The overall situation for internet freedom in Belarus remained relatively stagnant during 2012-2013. The government, run by the autocratic President Alexander Lukashenka, continues to exert control over the online sphere by blocking websites and intimidating online users. Repression of activists also became more targeted this year, compared to the large number of arrests made in connection with a series of protests in 2011.

During the past year, internet access in Belarus continued to grow. The country's external gateway capacity expanded to 350 Gbps, and significantly more users reported having access to broadband networks. All of Belarus' mobile operators offer internet access and the number of mobile internet users is growing. However, while access may be improving, the government continues to regulate, control, and restrict the scope of online content.

In 2010, the Ministry of Telecommunications issued a regulation for a catalogue of websites whose access should be blocked in state-run facilities and cybercafes. The procedure for consigning sites to this blacklist remains nontransparent and there is no functioning appeal process. As of February 2013, the list reportedly contained 119 websites, including a number of leading political, news, and human rights websites. The authorities continue the practice of occasionally blocking certain independent websites under specific circumstances. On September 23, 2012, the day of the parliamentary elections, the authorities blocked access to four websites that were reporting violations observed by independent organizations and citizens.

During the past year, the harassment and persecution of online journalists and activists deemed to be critical of the government continued and became more targeted. In 2012-2013, each of the three major cases of criminal prosecution against media practitioners concerned internet publications. Of the 11 political prisoners being held by the government, two regularly published online. There were about 60 cases of detentions of journalists, independent press distributors, and members of social networks. Instances of extralegal harassment of online activists, especially those involved in political communities on social networks, continued to take place. In August 2012, the authorities launched a campaign against social networks critical of President Lukashenka. Instances of technical attacks against independent websites grew. In April 2013, several leading political and civil society sites experienced a coordinated hacker attack, which included explicit threats against online publishers and journalists.

OBSTACLES TO ACCESS

From 2012-2013, the number of internet users in Belarus continued to grow rapidly and the quality of internet connections improved, despite a year of political and economic stagnation. The government's loss of popularity and credibility in the wake of the 2011 economic crisis continued

to spur demand for alternative sources of information.[1] With the authorities controlling the majority of print and broadcast outlets, the internet serves as the country's only island of free media. At the same time, the crisis did not dramatically affect government investment in the internet nor significantly increase internet costs, allowing many to begin using the internet as a source for news and a tool for social interaction.

The National Statistical Committee reported that Belarus has an internet penetration rate of 71.9 percent.[2] An independent study by Gemius in December 2012 found that there were 4.6 million internet users, or 13.8 percent more than the year before, producing a penetration rate of about 56 percent.[3] Statistics reported by the International Telecommunication Union (ITU) place the internet penetration rate lower at 47 percent for 2012.[4] In January 2013, the country's external internet gateway capacity was expanded to 350 Gbps. Following a growth of 20 percent in 2012, this upgrade will result in an increase in capacity of 44 percent in the first half of 2013.[5] In 2012, Belarus' wireless network was expanded to 1,300 hot spots, including 712 in the capital.[6]

The country's four mobile phone operators had a combined total of 10.7 million subscribers, for a total penetration rate of 113 percent as of January 2012.[7] All four mobile operators offer internet access, and 4,360 of the country's 15,000 base stations are 3G-capable. The share of smartphones in the mobile market is approximately 40 percent.[8] By October 2012, about 12 percent of internet users were accessing websites via mobile telephones, half of them with smartphones.[9] A report by Index on Censorship calculates that more than 2 million Belarusians have access to the internet via mobile devices and that more than 4 percent of online page views from Belarus now come from smartphones and tablets.[10] Mobile phone operators report considerable growth in the average

[1] Alyaksandr Klaskowski, "Private media gain credibility," Belapan, January 9, 2013, http://en.belapan.com/archive/2013/01/09/en_598444_598445. See also Александр Класковский, «Рупоры властей заржавели. Что взамен?» [Alyaksandr Klaskowski, The horns of the authorities rusted. What's instead?], Naviny.by, January 11, 2013, http://naviny.by/rubrics/society/2013/01/11/ic_articles_116_180482.
[2] National Statistical Committee (NSC), "Key indicators of public communication," accessed January 27, 2013, http://belstat.gov.by/homep/ru/indicators/transport.php. NSC data is based on the numbers reported by providers and does not distinguish between legal entities and private users.
[3] Mikhail Doroshevich, "Internet in Belarus, December 2012, E-Belarus, January 31, 2013. For the November 2012 statistics, see Alena Spasyuk, "Internet users in Belarus said to have increased in number by 13.3%," Belapan, November 23, 2012, http://en.belapan.com/archive/2012/11/23/en_19271123m.
[4] International Telecommunication Union (ITU), "Percentage of individuals using the Internet," 2012, accessed July 6, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
[5] Belarus plans to raise Internet gateway capacity nearly by half, http://news.belta.by/en/news/society/?id=697993.
[6] "Belarus external Internet gateway capacity up to 350Gbps, Belta, January 3, 2013, http://news.belta.by/en/news/society?id=703179.
[7] National Statistical Committee (NSC), "Key indicators of public communication," accessed January 27, 2013, http://belstat.gov.by/homep/ru/indicators/transport.php.
[8] "Цифры ИТ – статистика в Беларуси" [IT figures - statistics for Belarus], IT.tut.by, accessed January 27, 2013, http://it.tut.by/numbers/#cell. One of the four mobile phone operators, TeleGeography Mobile Digital Communications (Velcom), declared that as of December 31, 2012 its 3G/3G+ mobile networks were available to 100% of the urban population, while voice services coverage extended to 98.9% of the total population, http://www.e-belarus.org/news/201301101.html.
[9] Alena Spasyuk, "Internet users in Belarus said to have increased in number by 13.3%," Belapan, November 23, 2012, http://en.belapan.com/archive/2012/11/23/en_19271123m.
[10] Andrei Alexandrau, Belarus: Pulling the Plug, Index on Censorship, http://www.indexoncensorship.org/wp-content/uploads/2013/01/IDX_Belarus_ENG_WebRes.pdf.

revenue per user (ARPU), which is attributed to the rising number of the internet users and the development of data transmission services.[11]

According to Gemius, 80.7 percent of internet users in Belarus access the internet on a daily basis.[12] The key divide in levels of access is not between rural and urban populations—since almost 75 percent of Belarusians live in urban areas—but between the country's capital and other regions. However, the share of users in the capital city of Minsk has decreased from 40 percent to 28 percent over the last five years, and internet users in other cities with a population of more than 50,000 now account for more than 20 percent of the total.[13] Another significant determinant of internet use is age: 30 percent of all users are 25-34 years old, 21 percent are 19–24 years old, 19.5 percent are 35–44 years old, and only 6.5 percent are 55 years or older.[14] Most internet users—93.5 percent—regularly access the internet at home, and 29.8 percent do so at work. Internet cafes remain the least popular point of access, with just 4.2 percent of users utilizing them.[15]

While Belarus has two official languages—Belarusian and Russian—the majority of citizens use Russian in daily life. As a result, most online software is in Russian, although some popular software is also available in Belarusian, often translated by local enthusiasts.

In September 2012, almost 70 percent of Belarusian users reported having broadband access.[16] This figure has increased rapidly since 2010, when Belarus had Europe's lowest level of high speed access, at only 10 percent of the population. The largest choice and best quality of internet access is available in Minsk, where 38 companies offer internet access through ADSL, Ethernet, cable TV, and mobile networks. Smaller cities have a significantly narrower selection of options. Rural dwellers are largely dependent on the state-owned telecommunications monopoly Beltelecom, which provides IPTV[17] and internet access through ADSL (if phone lines are available), or via mobile internet, which is quite slow in remote locations. Internet connections are the slowest in the sparsely-populated areas of the southeastern and northern parts of the country.

The cost of broadband access via DSL and cable is generally tied to volume, reflecting the pricing structure that Beltelecom uses when selling bandwidth to downstream internet service providers (ISPs). This makes it somewhat expensive to download large items like music or movies, while for common activities such as e-mail and web browsing, the volume surcharges do not create a barrier for most users. An unlimited internet access service was launched by Beltelecom in 2007. Initially quite expensive, it has become more affordable, and prices range from approximately $5–$45 per

[11] "The average revenue per user (ARPU) of Belarusian mobile carriers rose considerably in Q3 2012," Belta, November 19, 2012, http://news.belta.by/en/news/econom?id=699383.
[12] Mikhail Doroshevich, "Internet in Belarus, December 2012, E-Belarus, January 31, 2013, http://www.e-belarus.org/news/201301311.html.
[13] Alena Spasyuk, "Internet users in Belarus said to have increased in number by 13.3%," Belapan, November 23, 2012, http://en.belapan.com/archive/2012/11/23/en_19271123m.
[14] "Internet audience in Belarus increased by 14%," IT.tut.by, October 24, 2012, http://it.tut.by/317249.
[15] Mikhail Doroshevich, "Internet in Belarus, December 2012," E-Belarus.org, http://www.e-belarus.org/news/201301311.html.
[16] "Internet audience in Belarus increased by 14%," IT.tut.by, October 24, 2012, http://it.tut.by/317249.
[17] IPTV refers to "internet protocol over television", a manner of providing television viewing through the internet rather than through traditional terrestrial, satellite, or other technologies.

month, depending on the speed. Beltelecom raised internet access prices by 10 percent in March 2012 and by another 10 percent in January 2013.[18] Mobile phone and internet access charges were increased by 20 percent in January 2013, as mobile operators were no longer exempted from paying a value added tax (VAT).[19]

The increase in internet penetration has resulted in the continued growth of citizens' activity on social networking sites. The Russian site VKontakte (vk.com) continues to be the most popular social network service, with 2.5 million accounts registered in Belarus, and is the most accessed website in the country.[20] About 1.6 million Belarusians use the Russian social network Odnoklassniki.ru.[21] As of February 2013, there were more than 112,000 blogs registered on LiveJournal from users in Belarus.[22] As of May 2012, there were 95,000 Belarusian users registered on Twitter, including 18,000 active users.[23] The total number of Facebook users in Belarus is close to 500,000 (about 5 percent of the total population and 16 percent of internet users), and has grown by more than 130,000 since May 2012.[24]

While foreign social networks remain very popular in Belarus and their number of users continues to grow, local networks appear to be gaining an audience within the country. In April 2012, the Minsk-based IT.TUT.by reported having over 1.2 million registered users on their social networking site, I.TUT.by.[25] As of January 2013, there were over 1 million users registered in another popular local social network, Vceti.by, compared to 315,000 users in October 2011.[26]

Beltelecom and the National Center for Traffic Exchange, established by the government in 2011, remain the only entities with the ability to handle connections with ISPs outside of Belarus. Beltelecom also holds a monopoly on fixed-line communications and internet services inside Belarus. In April 2012, the Center for Traffic Exchange replaced Beltelecom in providing access to the points of sharing national traffic (peering).[27] The Ministry of Communications and Information Technology has issued 180 licenses for secondary ISPs, though only 56 are currently active in Belarus. The Beltelecom subsidiary Belpak remains the largest ISP. While the government does not limit the amount of bandwidth that access providers can supply, all ISPs depend on the facilities of

[18] "Белтелеком не планирует повышать тарифы на Интернет до конца 2012 года" [Beltelecom is not planning to raise tariffs for Internet before the end of 2012], Ukaz60.net, accessed January 27, 2013, http://ukaz60.net/node/281; "С 18 января byfly и ZALA подорожают на 10%" [On January 18, byfly and Zala will increase prices by 10 %], Ukaz60.net, accessed January 27, 2013, http://ukaz60.net/node/298.
[19] Alyaksey Areshka, "Mobile phone, Internet access charges rise by 20 percent," Belapan, January 2, 2013, http://en.belapan.com/archive/2013/01/02/en_16550102.
[20] Alexa, "Top Sites in Belarus," accessed January 27, 2013, http://www.alexa.com/topsites/countries/BY.
[21] "Top 10 Websites," gemiusAudience, accessed on May 12, 2013, http://www.audience.by.
[22] "Цифры ИТ – статистика в Беларуси" [IT figures - statistics for Belarus], IT.tut.by, accessed March 8, 2013, http://it.tut.by/numbers/#cell.
[23] Ibid.
[24] "Belarus Facebook Statistics," SocialBakers, accessed January 27, 2013, http://www.socialbakers.com/facebook-statistics/belarus/last-3-months#chart-intervals.
[25] "Цифры ИТ – статистика в Беларуси" [IT figures - statistics for Belarus], IT.tut.by, accessed January 27, 2013, http://it.tut.by/numbers/#cell.
[26] Vseti.by, accessed on May 13, 2013, http://vseti.by.
[27] "Национальный центр обмена трафиком заменил Белтелеком в части услуг пиринга," [National Center for Traffic Exchange replaced Beltelecom in providing peering services], TechOnliner.by, April 3, 2012, http://tech.onliner.by/2012/04/03/nacionalnyj-centr-obmena-trafikom-zamenil-beltelekom-v-chasti-uslug-piringa.

the state-owned Beltelecom, which allows the authorities to control access speeds for the entire country, if needed.

There is no independent regulator overseeing ICTs in Belarus. The Ministry of Communications and Information Technology handles regulatory functions. In addition, the presidential administration's Operational and Analytical Center (OAC) has the authority to oversee ISPs, conduct overseas online surveillance, and manage Belarus' top-level domain (.by).[28] Other bodies with authority over this sector include the State Telecommunications Inspectorate, State Control Committee, and Prosecutor General's Office.

LIMITS ON CONTENT

With the 2000–2005 "color revolutions" and 2011 Arab Spring in mind, Belarus' authoritarian government has attempted to extend its control over online content. Local media rights groups have argued that the regulations adopted during the last three years—such as Decree No. 60, ("On measures for improving use of the national internet network")—reflect an alarming trend toward greater control of the internet, noting that many of the decree's provisions remain vague and unclear.[29] The procedure for putting sites on an official blacklist, for example, is completely nontransparent. Additionally, the government has continued to influence online content by increasing financial support to pro-government media outlets. There were a few instances of blocking in 2012-2013, such as the temporary blocking of Change.org in August 2012; however, other sites such as Facebook, Twitter, and YouTube remain accessible.

Decree No. 60, which was enacted on February 1, 2010 and came into effect on July 1, 2010, introduced provisions by which ISPs are required to block access to restricted information, such as pornography and material inciting violence. By law, the authorities can only institute this blocking in state institutions or when requested by individual users. In practice, however, the government has engaged in ad hoc efforts to limit access to internet content deemed contrary to its interests, though Belarusian telecoms typically cite technical problems rather than admitting to blocking. The authorities have regularly blocked certain websites on specific days when there are elections, holidays important to the democratic opposition, or scheduled protests.

On June 29, 2010, the Ministry of Telecommunications and the OAC issued a regulation calling for the creation of two lists to catalog the URLs of all websites whose access should be blocked in state-run facilities and internet cafes; one list is public, while the other is accessible only to ISPs.[30] As of May 2013, the publicly-accessible list did not contain any URLs, while the number of URLs on the

[28] See "Instructions on the procedure of domain names registration in the field of hierarchical names of the national segment of the Internet network" at http://cctld.by/eng/rules.html.
[29] Volha Prudnikava, "Authorities use both legal and illegal methods to control Internet, experts say," Belapan, January 11, 2012, http://en.belapan.com/archive/2012/01/11/en_522094_522095; "Belarus Again on the List of Internet Enemies (with Andrey Bastunets Comments)," Belarusian Association of Journalists, March 12, 2012, http://baj.by/en/node/11431.
[30] "БелГИЭ приступила к формированию "черного списка" [State Supervisory Body for Telecommunications Started Forming the "Black List"] Electroname, July 9, 2010, http://www.electroname.com/story/7329.

restricted list remains unknown.[31] On July 10, 2012, the state news agency Belta reported that the number of blacklisted websites had doubled since October 2011 and that the restricted list included 80 websites, most of which contain extremist or pornographic content.[32] According to Uladzimir Rabavolaw, the first deputy head of the presidential administration's Operational and Analytical Center (OAC), the list contained 119 websites as of February 2013.[33] Based on unofficial information, the blacklist also includes at least two of the country's most popular independent news and information websites, Charter97.org and Belaruspartisan.org, as well as the website of the Viasna Human Rights Center and the blog of the popular independent political commentator Yauhien Lipkovich.[34] The Prosecutor General's Office has confirmed that Charter97.org and Belaruspartisan.org are on the restricted list.[35] State officials claim that the sites remain privately accessible.[36] State bodies authorized to add sites to the blacklist include the Ministry of Internal Affairs, the Prosecutor General's Office, and the KGB.

Under amendments dating from November 2011, which stipulate the fines for violating Decree No. 60, ISPs that provide access to blacklisted websites are required to pay a small fine. In practice, ISPs seem to be inconsistent in blocking access to these sites; some have blocked access to blacklisted sites without any user requests, which is technically illegal under the decree, while others have ignored the blacklist.[37] ISPs block the blacklisted websites by web address or in combination with IP filtering. In December 2012, Index on Censorship conducted field research using a sample group of blacklisted sites to assess the scope of the filtering. The results indicated varying degrees of blocking. While the sites were available via internet cafes in Minsk and through Belarus' three major mobile operators, some or all were blocked in places where the state had greater control over the internet connection, such as government buildings and universities.[38]

The authorities continue to practice occasional blocking of certain independent websites under specific circumstances. In August 2012, Change.org, a site which offers individuals and organizations the opportunity to publicize petitions and gather more supporters, could not be accessed inside Belarus. The independent website Charter97.org alleged that the authorities had blocked Change.org in order to prevent citizens from signing an online petition for the release of Anton Surapin and Syarhey Basharymaw, who were unjustly arrested and charged with allegedly

[31] "Списки ограниченного доступа" [Lists of Restricted Access], Ministry of Telecommunications, accessed on May 12, 2013, http://belgie.by/node/216. For the online version, see also http://bit.ly/14TskaI.
[32] "В Беларуси удвоилось количество запрещенных сайтов," [Number of banned websites doubled in Belarus], Ej.by, July 10, 2013, http://www.ej.by/news/politics/2012/07/10/v_belarusi_udvoilos__kolichestvo_zapreschennyh_saytov.html.
[33] "ААЦ – заблякаваным сайтам: Пішыце апеляцыі"[OAC to blocked websites: Write appeals], Viasna, February 17, 2013, http://spring96.org/be/news/61348.
[34] Zmitsier Lukashuk, "Websites restricted for state institutions since November 28," Euroradio, November 30, 2011, http://baj.by/en/node/9118.
[35] Vyacheslaw Budkevich, "Government begins blocking access to opposition websites," Belapan, April 11, 2011, http://en.belapan.com/archive/2011/04/11/en_20240411.
[36] Tanya Korovenkova, "Belarus: Internet under surveillance, but still relatively free," Belapan, February 23, 2013, http://en.belapan.com/archive/2013/02/23/en_607543.
[37] Volha Prudnikova, "Authorities use both legal and illegal methods to control internet, expert says," Belapan, June 24, 2011, http://en.belapan.com/archive/2012/01/11/en_522094_522095.
[38] "Belarus: Pulling the Plug," Index on Censorship, pp. 12-13, http://www.indexoncensorship.org/wp-content/uploads/2013/01/IDX_Belarus_ENG_WebRes.pdf.

assisting in the illegal flight of a foreign airplane over Belarusian airspace on July 4, 2012.[39] While accessible from other countries, Change.org remained blocked in Belarus for two weeks.

On September 23, 2012, the day of the parliamentary elections, the authorities again used Beltelecom to block access to the websites of the civic and political For Freedom Movement (Pyx.by), Belarusian Christian Democracy party (Bchd.info), and the political news source Unity-Democracy-Freedom (UDF.by), as well as the crowdsourcing election monitoring platform Electby.org. The main criteria for the blocking were election-related activities; all of the sites on the list were publishing reports of violations from independent observation groups and ordinary citizens. IP filtering was used as the blocking mechanism. The blocking commenced at 7:30pm on September 23 and continued for about 24 hours. This type of blocking proved relatively easy to bypass by changing IP addresses and updating DNS records. Three of the four sites (Electby.org, Pyx.by, and UDF.by) utilized these tactics and were inaccessible for only short periods of time. The Bchd.info team was unable to restore access, most likely due to the limitations of its hosting, which did not permit changing the IP address. Unlike in past elections, most independent news sources, as well as the majority of the political opposition's websites, were not blocked. Social networks also remained accessible. This limited response by the authorities reflected the fact that citizens expressed little interest in these elections, and the opposition did not call for or plan public protests.

On February 25, 2013, the Belarusian authorities again blocked access to the website of the Belarusian Christian Democracy party (BChD), as reported by the press office of the unregistered opposition party. BChD Executive Secretary Dzyanis Sadowski linked the blocking to the party's campaign called "Wave of Solidarity," which is aimed at supporting political prisoners and other victims of the Lukashenka regime.[40]

To date, it appears that the Belarusian government does not possess the capacity to employ sophisticated internet blocking techniques, and therefore resorts to more basic approaches like IP filtering and disabling DNS records.[41] Also, it seems that the authorities do not perform regular or automated monitoring of the accessibility of banned sites, and it generally takes from 4 to 16 hours to block a new IP address. No documented instances of deep packet inspection (DPI) filtering have been recorded so far.

Since 2008, the government has employed stringent requirements for accreditation to restrict non-state journalists' access to information.[42] The Law on Mass Media requires journalists to obtain

[39] Syarhey Pulsha, "Web users in Belarus unable to access popular online petition site," Belapan, August 12, 2012, http://en.belapan.com/archive/2012/08/12/en_12081454b.
[40] Syarhey Karalevich, "Authorities block access to website of Belarusian Christian Democracy," Belapan, February 25, 2103, http://en.belapan.com/archive/2013/02/25/en_17350225m.
[41] "В Беларуси заблокирован доступ к сайту Change.org" [In Belarus access to Change.org website is blocked], Providers.by, August 13, 2012, http://providers.by/2012/08/news/v-belarusi-zablokirovan-dostup-k-change-org.
[42] The Law on Mass Media envisages an authorization-based procedure of accreditation. Moreover, it does not allow the possibility to appeal against a refusal of accreditation as a journalist. A journalist is forbidden to carry out professional activities, if he or she is not accredited. "Comments on Suggestions to Media Law," Belarusian Association of Journalists, January 24, 2013, http://baj.by/en/node/19255.

authorization before they can become accredited and it does not allow individuals to appeal the decision in cases where their accreditation is refused. Journalists, including those publishing online, are not allowed to work professionally if they are not accredited.[43]

In January 2013, the Ministry of Foreign Affairs denied the accreditation application of Pavel Sviardlou, a Belarusian journalist known for his online reports for the Warsaw-based European Radio for Belarus.[44] The ministry cited Sviardlou's previous arrest in June 2012—when police officers grabbed him off the street and forced him into a minibus, after which he served a 15-day detention on the charge of using obscene language—as the reason for denying his application. On March 26, 2013, the ministry denied accreditation, for the third time, to Belsat, the Warsaw-based independent Belarusian-language satellite television channel and online news source, on the grounds that Belarusian journalists reporting for the channel had violated Belarusian media laws.[45] Additionally, journalists for Belsat have been continually harassed by the Belarusian authorities through warnings and administrative arrests.

Another result of state pressure is self-censorship, which has become a pervasive phenomenon for web-based media, especially state and commercial outlets. Online commentators and administrators of web portals avoid posting content that might put them at odds with the authorities. Many Belarusian websites and forums still practice pre-moderation of comments, which discourages regular users and restricts communication. Under the Administrative Offences Code, criminal code, and Decree No. 60, websites are not liable for users' comments, but in practice sites often face consequences for certain kinds of comments. Typically, users are warned in the forum rules that they are responsible for their comments. Nevertheless, many site owners have stated that they have been contacted by officials and businesspeople unhappy with comments. Moreover, readers who are offended by comments often attribute blame to the website itself, indicating that readers do not always make the distinction between the journalism content posted by the website owners and commentary posted by unaffiliated users.[46]

During the parliamentary election campaign in the fall of 2012, a pro-governmental candidate threatened the editor of *Uzhorak*, a local independent print and online newspaper in the Mogilev region, for publishing an article on the newspaper's website informing citizens that he had refused to take part in a public debate with a local democratic candidate.[47] He was especially unhappy with users' comments and demanded that the article be withdrawn from the website. The editor refused to remove the online article. Moreover, it was later published in the newspaper's print issue.

On November 10, 2012, an anonymous blogger posted a critical article about the director of the local post office in Hlybokaye on Westki.info, a popular independent information resource for

[43] "Comments on Suggestions to Media Law," Belarusian Association of Journalists, January 24, 2013, http://baj.by/en/node/19255.
[44] "Belarus Media Law Offers No Defense," Belarusian Association of Journalists, February 20, 2013, http://baj.by/en/node/19694.
[45] "Belsat TV Denied Accreditation Again," Belarusian Association of Journalists, March 23, 2013, http://baj.by/en/node/20242.
[46] Volha Prudnikava, "Bynet: rudeness is an issue," Belapan, August 8, 2012, http://en.belapan.com/archive/2012/08/08/en_566422_566423.
[47] Andrei Borovko, "Волков отказался от дебатов" [Volkov refused to take part in the debates], Horki.info, August 28, 2012, http://horki.info/news/88/2549.html.

northwestern Belarus. Westki.info is a regional media site and blogging platform, where anyone can create a personal blog. Blogs and comments are not moderated. Even though the director's name was not mentioned in the anonymous article or the comments, she contacted the website's administrator and demanded the personal information and contact information of the blog's author, as well as those of all critical commentators, as she was planning to sue them for slander. After consultations with a lawyer, the Westki.info administrator removed the controversial post from the site, but refused to turn over any personal information about the blogger and commentators.

The government is attempting to counter the gains in quality, popularity, and trust made by independent civil society by increasing its own presence and influence online. Despite national, regional, and local state agencies having an online presence, most government websites are outdated, lack interactivity, and are not user-friendly.[48] Local state websites usually have poor designs, are not relevant, and draw few readers.[49] A special governmental program was launched in 2010 to assist regional and local state newspapers in creating and promoting their websites. To aggregate the content produced by local and regional state publications, a portal for their websites was created at Belsmi.by.

While the total amount of funding provided to pro-government online media is unknown, the authorities continue to increase support to the state-owned media as a whole, despite economic stagnation. The 2013 state budget allocated €60 million ($77 million) in subsidies for state media, €19 million ($24 million) more than in 2012, including €46 million ($59 million) to TV and radio, €6 million ($8 million) to print outlets and publishing houses, and €7.5 million ($9.6 million) to "other mass media issues," though it is not clear which line items include online media.[50]

Media experts and website moderators see trolling—the use of inflammatory, extraneous and provocative messages—as a major issue. Since the 2010-11 protests, the number of trolls and paid commentators, and their disruptive activities, has significantly increased on independent websites, the blogs of civic activists and commentators, and popular opposition communities on social networks. Obscenities and rudeness continue to be a challenge for the Belarusian internet, often making discussions on forums difficult.[51]

While massive, orchestrated commentary by provocateurs usually takes place around important political and civic events, such as the "silent protests" in the summer of 2011, there are also "agent commentators" whose job is to regularly post comments on major independent websites and popular political social network communities. On May 2, 2012, an ad was published on Freelance.ru, a job search website, seeking to hire people to write negative comments about the opposition on the forum of Belaruspartisan.org, one of the most popular independent websites.

[48] "Дзяржаўныя сайты адстаюць на дзесяцігоддзе," [State websites are a decade behind], *Tut i Ciaper*, January 21, 2013, http://svabodaby.net/by/196/society/1693/Дзяржаўныя-сайты-адстаюць-на-дзесяцігоддзе--Люстра-дзён.htm.
[49] "Authorities can liberalize media market "only at gun point," expert says," Belapan, January 17, 2013, http://en.belapan.com/archive/2013/01/17/en_599921_599922.
[50] "60 million goes to state-run mass media," Belarusian Association of Journalists, December 19, 2012, http://baj.by/en/node/18895.
[51] Volha Prudnikava, "Bynet: rudeness is an issue," Belapan, August 8, 2012, http://en.belapan.com/archive/2012/08/08/en_566422_566423.

The ad was posted from an anonymous account with only an ICQ name as a contact.[52] Several similar ads were posted on the same site under the names of real people, who later claimed that their accounts on social networks had been hacked and that they had nothing to do with the dubious posts, sparking anger and threats from other users.[53] After the independent media exposed this trolling scandal, the ads were removed.

The government's growing attempts to control the internet can be explained by the internet's growing popularity as a source of information, even while traditional print and broadcast media remained the main sources of news for most Belarusians in 2012-2013. According to an independent nationwide survey conducted in May 2012, 34.3 percent of respondents said that they use the internet as their primary source of information. In 2012, independent web-based media continued to serve larger audiences than state-supported online outlets. According to the Belarusian ranking service Akavita.by, most of the top 10 and a majority of the top 50 news and information websites are run by independent or opposition groups.[54] The daily audience of Charter97.org, the most popular opposition website, has quadrupled since November 2010 to more than 100,000 unique visitors a day.

Not only are greater numbers of Belarusians reading independent news, they also find it more credible. An independent survey conducted in December 2012 found that more Belarusians trust independent media than the state media (48.1 percent versus 38.1 percent). Trust in the state media has dropped by 14.8 percent since December 2010.[55] The government has been forced to recognize the growing importance of independent online media. On January 15, 2013, President Lukashenka surprised the public when he opened his annual press conference by addressing a question raised on the popular independent website Gazetaby.com, even though its journalists were not invited to the conference itself.[56]

The government also employs direct and indirect economic pressure to limit financial support for independent media. A series of restrictive amendments to the Law on Public Associations and the criminal code were passed secretly in October 2011 and came into force a month later. Of note were provisions that made it a criminal offense for nongovernmental organizations (NGOs) to receive foreign funding. Since most independent online media outlets are run as NGOs, the amendments constitute a grave threat to Belarusian civil society, including free media.[57]

---

[52] "Стань лукашистом да деньги, или Тролль детектед," [Become a lukashist for money, or Troll is detected], UDF.by, May 11, 2012, http://udf.by/news/main_news/59506-stan-lukashistom-za-dengi-ili-troll-detekted.html.
[53] Yahor Marcinovich, "Застабілы, як твой муж, павінны здохнуць," [Lukashists, like your husband, must die], NN.by, May 11, 2012, http://nn.by/?c=ar&i=73256.
[54] "Top ranker," Akavita.by, accessed on January 28, 2013, http://www.akavita.by/ru/top/All/Mass_Media_and_News/today/visitors/All/All.
[55] "Belarusians' trust to non-state media rises, unlike to state-run media," Belarusian Association of Journalists, January 8, 2013, http://baj.by/en/node/19052; Alyaksandr Klaskowski, "Private media gain credibility," Belapan, January 1, 2013, http://en.belapan.com/archive/2013/01/09/en_598444_598445.
[56] Kirill Bukin, "Лукашенко первым делом ответил на вопрос 'Салідарнасці'," [Lukashenko first of all answered the question of Solidarity], Gazetaby.com, January 15, 2013, http://gazetaby.com/cont/art.php?&sn_nid=52702.
[57] See: "Belarus: Open Joint NGO Letter to the Parliament of Belarus," Human Rights Watch, October 20, 2011, http://www.hrw.org/news/2011/10/20/belarus-open-joint-ngo-letter-parliament-belarus.

Forced to operate in semi-underground conditions and experiencing constant pressure from the authorities, independent online media and opposition websites are unable to monetize their increasing audiences and growing popularity. During the first half of 2012, Belarus' internet advertising market rose by 20 percent and totaled over $2.7 million, up from $2.3 million in the same period of 2011.[58] But most independent news and information websites remain at an economic disadvantage because state and private companies are afraid to advertise on them. Moreover, there is an unwritten rule advising companies connected with the state that they should not advertise in the independent media, including internet outlets. As a result, even the most popular independent or opposition websites, such as Charter97.org and NN.by, generate little or no advertising revenue. Since this ban exists only in the form of an oral recommendation, media and human rights groups have been unable to oppose it.

Since the 2006 presidential election, independent websites, blogs, internet forums, and online communities have played a significant role in educating citizens, turning out voters, monitoring the polls, and mobilizing those protesting electoral irregularities. Beginning in 2010, social networks have become an important tool for carrying out solidarity actions and organizing peaceful protests. With the rapid rise of new media, independent online sources were able to compete with state-controlled newspapers, radio, and television during the 2010 presidential and 2012 parliamentary elections.

In 2012, pro-democratic forces significantly increased and diversified their presence and activities in social networks. According to the digital marketing agency Ashwood Creative, as of December 2012, 28 of the top 30 Belarusian media communities on Facebook are run by independent media and civil society groups.[59] Despite crackdowns, hacking attacks, and the persecution of online activists, numerous political communities are openly critical of the regime on VKontakte and Facebook. Independent media, civil society organizations, the political opposition, and individual citizens use the internet and other ICTs as tools for disseminating information, raising awareness and mobilizing supporters. Online actions are often combined with offline activities, such as demonstrations, meetings, flash mobs, political performances, underground exhibits, and alternative concerts. The ongoing solidarity campaign with the country's political prisoners includes raising awareness on social networks, posting articles and banners on popular news websites, and creating online petitions and appeals to national and international institutions, as well as demonstrations and multimedia exhibitions.

Online petitioning became a popular form of civic activism in 2012. More than a dozen petitions were created and carried out by Belarusian rights groups and individuals on Change.org alone, addressing a gamut of issues, from the return of the body of Vladislav Kovalev (who was executed in 2011) to his mother,[60] to the protection of Belarusian wetlands from destruction.[61] Petitions on

[58] Alyaksey Areshka, "Internet advertising market up by 20 percent in first six months of this year," Belapan, August 11, 2012, http://en.belapan.com/archive/2012/08/11/en_11081522b.
[59] "Рейтинг белорусских страниц Facebook за декабрь," [Rating of Belarusian pages on Facebook in December], Ashwood Creative, accessed on January 29, 2013, https://www.facebook.com/ashwoodcreative/app_152031511604374.
[60] "Petition: Give Vlad's Body Back," Change.org, accessed on January 29, 2013, http://chn.ge/14cFyim.
[61] Anastasiya Yanushewskaya, "Over 10,000 sign online petition against peat mining in wetlands," Belapan, February 1, 2013, http://en.belapan.com/archive/2013/02/01/en_01021551b.

simplifying visas, boosting local border traffic, preserving green spaces, reforming the election law, and preserving historic sites were also launched by civil society.

The effective use of online media and ICT tools also helped citizens draw attention to and even solve some pressing social issues, especially at the local level. In October 2012, several leading independent news sites wrote about the construction of an entertainment complex on the territory of Kurapaty, a forest on the outskirts of Minsk containing the graves of victims of Stalinist repression.[62] These articles generated a great deal of public discussion and outrage. An online petition to stop the construction of the brothel 'Bulbash Hall' in Kurapaty was posted on Change.org and signed by almost 4,500 people.[63] A campaign against the project was also launched via social networks. As a result, the General Prosecutor's Office conducted an inspection, which revealed serious planning violations, and decided to halt the construction.[64] According to recent statements by state officials, a memorial will be built there instead of the entertainment center.

In September 2012, the crowdsourcing platform Electby.org was used to monitor parliamentary election violations (it was launched prior to the 2010 presidential elections). In the course of one week, voters and observers sent in 528 testimonies on a variety of violations. This past year, the monitoring was conducted in close cooperation with independent observation groups, making the mapping more accurate. Electby.org moderators were able to verify 44 percent of all messages received via different sources.[65]

Since Belarusian users have regular access to most online resources under normal circumstances—blacklisted sites are blocked only in public facilities, not private offices or households—they generally have not employed proxy servers or other circumvention tools, leaving them vulnerable during politically sensitive periods when targeted disruptions occur. Circumvention tools have not been blocked by the authorities. Most often, people are reminded about blocking, hacking, trolling, and phishing only when it takes place.[66]

VIOLATIONS OF USER RIGHTS

While the overall level of repression decreased over the past year due to the lack of mass social protests such as those in 2011, the repression of online users became more targeted in 2012-2013. All three criminal cases involving the media during this period were for instances of online activism. Extralegal harassment and intimidation of online users has also increased.

[62] "Памерлыя глядзяць на 'свята жыцця'," [The dead look at 'celebration of life'], Novychas.info, October 24, 2012, http://novychas.info/hramadstva/pamierlyja_hliadziacj_na_sviat.
[63] http://chn.ge/1bhDs2F, accessed on January 29, 2013.
[64] "Как сеть Интернет победила 'Бульбашъ-Холл'," [How Internet defeated 'Bulbash Hall'], NN.by, December 4, 2012, http://nn.by/?c=ar&i=101189&lang=ru.
[65] "Electby," http://electby.org/, accessed on May 13, 2013.
[66] Yahor Kanapkin, "Праз дзірку ў абароне Skype масава выкрадалі акаўнты" [Through the bug in Skype protection accounts have been massively stolen], Generation.by, November 14, 2012, http://generation.by/news5764.html.

While the right to information and freedom of expression are guaranteed by the Belarusian constitution, they remain severely restricted and violated in practice. Formally, there are no laws ascribing criminal penalties or civil liability specifically for online activities, but since 2007 the government has employed a series of repressive laws—mainly defamation laws—that target traditional media to stifle critical voices online. The 2008 Law on Media identified online news outlets as "mass media." According to this law, the Council of Ministers was supposed to further specify criteria for defining which websites belong to the category of "mass media," as well as the procedures for their registration.[67] To date this clarification has not taken place. Therefore, at the moment, online news outlets are not obliged to obtain state registration as mass media.

In October 2011, the government introduced, and the parliament approved, an "anti-revolutionary" package of amendments to laws regulating civic organizations and political parties, as well as to the criminal code. These amendments—which apply to internet-based media outlets—further criminalize protest actions, make receiving foreign funding a criminal offense, and extend the authority of the KGB. Under the amendments, the KGB is now freed from the oversight of other state bodies and has powers previously granted only during a state of emergency, including the right to enter the homes and offices of any citizen at any time without a court order.[68]

While the repression of media practitioners and civic activists decreased in 2012, the persecution became more targeted. According to the Viasna Human Rights Center, there were 233 cases of politically-motivated administrative persecution (arrests, detentions, and fines) documented in 2012, including 104 arrests for terms ranging from 1 to 15 days.[69] In 2012, the Belarusian Association of Journalists registered approximately 60 cases of detentions of journalists, independent press distributors, and members of social networks by representatives of different law-enforcement bodies. Detained media practitioners were usually released within 2-3 hours. There were, however, cases in which media workers were taken to court and sentenced to fines and terms of imprisonment (up to 15 days) under administrative law. In 2012, at least 13 journalists were officially warned by public prosecution offices for cooperating with foreign media without valid press credentials.[70]

In the past year, each of the major cases of criminal prosecution against media practitioners concerned internet publications. The most prominent case concerned the outspoken journalist Andrzej Poczobut, who in the last three years has been repeatedly detained, fined, and placed under administrative arrest. In 2011, he was convicted and received a three-year suspended sentence for insulting the president of Belarus in a series of articles posted online, including on the websites of the Polish daily *Gazeta Wyborcza* and Belaruspartisan.org, as well as on his LiveJournal blog. In June 2012, Poczobut was detained again for slandering the president in articles written on

[67] Law of the Republic of Belarus No. 427 of July 17, 2008, "On Mass Media," available in Russian at http://www.mininform.gov.by/documentation.
[68] "Belarus has adopted 'anti-revolutionary' amendments to the legislation," Human Rights House, October 20, 2011, http://humanrightshouse.org/Articles/17082.html.
[69] "Адміністратыўны перасьлед" [Administrative persecution], Viasna Human Rights Center, accessed on May 12, 2013, http://spring96.org/persecution/?DateFrom=2012-01-01&DateTo=2012-12-31&ArrestFrom=1&ArrestTo=15&Page=0.
[70] Mass Media in Belarus – 2012: A Brief Review and Analysis, Belarusian Association of Journalists, February 11, 2013, http://baj.by/en/monitoring/85.

the opposition websites Charter97.org and Belaruspartisan.org.[71] During the politically-motivated investigation into his writings, Poczobut could not leave his city of residence. If convicted, he would have faced up to seven years in prison.[72] On March 15, 2013, the Investigative Committee closed the case against Mr. Poczobut, having found no legitimate evidence of the alleged crime.[73]

On July 4, 2012, as part of a publicity stunt carried out by the foreign advertising agency Studio Total, two Swedish pilots flew across the Belarusian border in a small plane and dropped hundreds of teddy bears with messages in support of solidarity and freedom of speech. On July 13, Anton Surapin, a 20-year-old journalism student who posted the first photos of the teddy bears on his website Belarusian News Photos, was arrested and spent over a month in a KGB prison for allegedly "assisting foreign citizens in illegally crossing the Belarusian border." On August 17, Surapin was released, but the charges against him have not been lifted.[74] Amnesty International included Surapin's case in its top 10 most absurd and unjust arrests of 2012.[75] Additionally, when Surapin's independent media colleagues launched a solidarity campaign on his behalf that involved posting photographs of individuals holding messages of support, two individuals were arrested and fined for "unsanctioned picketing in the form of photography."[76]

On August 17, the journalist and civic activist Mikalay Petrushenka was criminally charged with defaming an Orsha public official in an article published on the Vitebsk-based Nash-dom.info website. The criminal proceedings were dropped on October 17, 2012.

In December, the prosecutor's office issued a warning to a democratic activist from Rahachou concerning his articles published on a local independent website. The prosecutor claimed that the activist's posts contained inaccurate information about the political and economic situation in Belarus, thus violating several articles of the criminal code regarding "insulting and discrediting the Republic of Belarus."[77]

In January 2013, three human rights defenders from Hrodna were convicted and fined for an unauthorized demonstration. The case was based on a photo posted on the website of the Viasna

[71] "Official information: Poczobut accused of libel against the president," Belarusian Association of Journalists, June 22, 2012, http://baj.by/en/node/12746.
[72] "Poczobut's case extended till December 2012," Belarusian Association of Journalists, November 21, 2012, http://baj.by/en/node/18464; "Additional linguistic expertise in Poczobut's case," Belarusian Association of Journalists, November 29, 2012, http://baj.by/en/node/18590.
[73] "Poczobut's case closed," Belarusian Association of Journalists, March 15, 2013, http://baj.by/en/node/20026.
[74] "Freelancer Anton Surapin taken to questioning," Belarusian Association of Journalists, July 13, 2012, http://baj.by/en/node/1299; "KGB brings charges over teddy bear drop," Belarusian Association of Journalists, August 7, 2012, http://baj.by/en/node/13098; "Anton Surapin is free," Belarusian Association of Journalists, August 17, 2012, http://baj.by/en/node/13607.
[75] "10 absurd and unjust arrests of 2012," Amnesty International, December 26, 2012, http://blog.amnestyusa.org/music-and-the-arts/10-absurd-and-unjust-arrests-of-2012.
[76] "Darashkevich and Kozik fined 3 million Br each for unlawful picket," Belarusian Association of Journalists, August 9, 2012, http://baj.by/en/node/13383.
[77] "Rachahou activist receives a warning over contributing to independent website," Belarusian Association of Journalists, December 29, 2012, http://baj.by/en/node/18996.

Human Rights Center, which showed them holding the portrait of political prisoner Ales Bialiatski and a copy of the Universal Declaration of Human Rights.[78]

In September 2012, the Belarusian government lifted a travel ban that had been placed on journalists, civic activists, and opposition politicians. Beginning in March 2012, a significant but unknown number of individuals, including practitioners working within online media, were banned from traveling abroad.[79] This violation of freedom of movement was allegedly a reaction to the extension of the European Union's visa ban list of Belarusian officials involved in the 2010-2011 repression. After removing the ban in September, the Citizenship and Migration Department explained it away as a software glitch.[80]

While the authorities have long used petty charges to prosecute civic activists and independent reporters, this technique was increasingly applied against online activists in 2012-2013. Charges of "petty hooliganism" (Article 17.1 of the administrative code) were used to detain and arrest a number of online activists.[81] For example, on May 7, 2013, in two separate court hearings, the blogger Dzmitry Halko and journalist Aliaksandr Yarashevich were found guilty of alleged petty hooliganism and disobeying the police (Article 23.4) and were sentenced to 10 and 12 days of arrest, respectively. Both were detained the night before near the Akrestina detention center in Minsk, where civil activists, politicians, and other journalists had gathered to meet those arrested during the April 26 Chernobyl March.[82] For Yarashevich, this was the second arrest in a fortnight. On April 26, he and journalist Henadz Barbarych were detained for allegedly disobeying the police. On April 29, the Soviet district court of Minsk sentenced the journalists to three days of administrative detention (which they had almost served by the end of the trial) in spite of obvious contradictions and blatant discrepancies in the testimonies of policemen.[83]

Individuals are required to present their passports and register when they buy a SIM card and obtain a mobile phone number. All telecommunication operators are obliged to install real-time surveillance hardware, which makes it possible to monitor all types of transmitted information (voice, mobile text message and internet traffic) as well as obtain other types of related data (such as user history, account balance, and other details) without judicial or other independent oversight. Mobile phone companies are required to turn over personal data of their customers at the government's request.

[78] "Hrodna: Human rights defenders get fined 4.5 million rubles for a photo on the web," Spring96.org, January 8, 2013, http://spring96.org/en/news/60388.
[79] For Belarusian Association of Journalists' reaction to the restriction on journalists' travel, see http://baj.by/en/node/11459.
[80] Mass Media in Belarus – 2012: A Brief Review and Analysis, Belarusian Association of Journalists, February 11, 2013, http://baj.by/en/monitoring/85.
[81] "Belarus: Pulling the Plug," Index on Censorship, p. 10-11, http://www.indexoncensorship.org/wp-content/uploads/2013/01/IDX_Belarus_ENG_WebRes.pdf.
[82] "Journalists Sentenced to 10 and 12 Day Arrest," Belarusian Association of Journalists, May 7, 2013, http://baj.by/en/node/20780.
[83] "A protest of BAJ against arbitrary detentions of journalists," Belarusian Association of Journalists, May 8, 2013, http://baj.by/en/node/20790.

Since 2010, the Belarusian government has allocated resources for online surveillance technologies.[84] In 2012, there were reports of Western firms supplying telecommunications hardware and software that would allow the state to expand its surveillance of citizens. A report by Index on Censorship states that the Swedish telecom companies TeliaSonera and Ericsson are possible purveyors of this type of equipment, working through Turkish and Austrian firms that are part-owners of Belarusian mobile telephone companies. The report also noted that the German police had trained their Belarusian colleagues to use software that could track communications in social networks.[85]

Russian surveillance technologies are also employed in Belarus. In March 2010, Belarus acquired the SORM ("system for operational-investigative activities") surveillance system, and has reportedly also purchased other Russian surveillance software that is designed to allow for monitoring of social networks.[86]

Decree No. 60 requires ISPs to maintain records of the traffic of all internet protocol (IP) addresses, including those at home and at work, for one year. As a result, the state can request information about any citizen's use of the internet. As of 2007, internet cafes are obliged to keep a year-long history of the domain names accessed by users and inform law enforcement bodies of suspected legal violations.[87] In December 2012, the Council of Ministers abolished the requirement that the customers of internet cafes must present their passports. Instead, cybercafe employees are required to take pictures of or film visitors.[88] This regulation, "On personal identification of internet cafe users," came into legal force on January 28, 2013.[89] Restaurants, cafes, hotels, and other entities are obliged to register users before providing them with wireless access, whether free of charge or paid.[90]

On July 17, police searched the apartment of the editor of the local independent website Orsha.eu. The editor's computer and memory cards were confiscated on suspicion that the website contained a link to another website with pornographic content. The equipment was returned five months later without any explanation.[91] In August, a correspondent of another independent regional

[84] Мероприятия по реализации Национальной программы ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011–2015 годы [Measures on implementation of the National program of accelerated development of information and communication technologies for 2011-2015], http://www.mpt.gov.by/File/Natpr/pril1.pdf.
[85] "Belarus: Pulling the Plug," Index on Censorship, p. 16-17, http://www.indexoncensorship.org/wp-content/uploads/2013/01/IDX_Belarus_ENG_WebRes.pdf.
[86] Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," World Policy Institute, Fall 2013, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.
[87] "Совет Министров Республики Беларусь Положения о порядке работы компьютерных клубов и Интернет-кафе" [Council of Ministers of the Republic of Belarus. Regulations on computer clubs and internet cafe functioning], Pravo.by, April 29, 2010, http://pravo.by/webnpa/text.asp?start=1&RN=C20700175.
[88] Alyaksey Areshka, "Authorities scrap passport requirement for Internet cafes' visitors," Belapan, December 27, 2012, http://en.belapan.com/archive/2012/12/27/en_27122104b.
[89] "Passport identification in cyber cafes to become obsolete?", Belarusian Association of Journalists, January 29, 2013, http://baj.by/en/node/19310.
[90] Including the user's name, surname, type of ID, ID number, and name of the state body which issued the ID, as per Article 6 of the Regulation on computer clubs and internet café functioning, http://pravo.by/main.aspx?guid=3871&p0=C20700175&p2={NRPA}.
[91] "Equipment given back after 5 months' check-up," Belarusian Association of Journalists, November 29, 2012, http://baj.by/en/node/18627.

website was summoned to the prosecutor's office and questioned about an article by a local opposition leader, which called for a boycott of the 2012 parliamentary elections and was published on Westki.info. The prosecutor threatened the journalist with administrative responsibility for the article, despite the fact that it was authored by another person.[92]

Instances of extralegal intimidation and harassment for online activities continued to take place in 2012-2013. In April 2012, a girlfriend of one of the leaders of the "Revolution Through Social Networks" internet group, which organized the 2011 "silent protests," was taken from her apartment by plainclothes police officers, interrogated for eight hours, threatened with death, forced to record a video slandering her boyfriend Viachaslaw Dziyanau and herself, and was tried and fined for "hooliganism." While leaving the country after the process, she was body-searched and her laptop and other electronic devices were confiscated at the border.[93] On May 8, 2012, a customer was kicked out of an internet cafe in Minsk, insulted, and beaten up by the police for reading the Charter 97 website.[94]

In 2012, the authorities continued to harass active users of opposition communities on social networks. On August 30, the KGB raided the apartments and detained the administrators of the "We Are Sick of Lukashenka" online community, one of the largest on VKontakte. Created on the eve of the 2010 presidential election, the group numbered 37,000 users, mainly 15 to 25 years old, by August 2012. On the same day, the apartments of the administrators of a second community were also raided. Known as "Only ShOS," which stands for "Wish He would Die," this community had 15,000 members. The young activists were interrogated for four hours, threatened, and beaten. Two were incarcerated for five to seven days for "hooliganism," while the rest were released. Simultaneously, hackers gained access to both online communities and removed their content.[95] Nevertheless, the moderators created a backup VKontakte group, which already numbers more than 4,000 users.

On February 17, 2013, two Belarusian students on their way back from Warsaw, where they participated in a meeting dedicated to the "Day of Belarusian Wikipedia," were detained in Brest. The students were questioned and their personal belongings were inspected. The students were released several hours later.[96]

---

[92] "Кастуся Шыталя распытвалі ў пракуратуры пра публікацыю, у якой згадваўся байкот," [Kastus Shytal interrogated by the prosecutor office about the publication mentioning boycott], Wetski.info, August 13, 2012, http://westki.info/artykuly/13588/kastusya-shytalya-raspytvali-u-prakuratury-pra-publikacyyu-u-yakoy-zgadvausya-baykot.

[93] "Лавышак: Мяне пагражалі вывезці ў лес і растраляць," [Lavyshak: "I was threatened to be taken to the forest and shot there"], Svaboda.org, May 4, 2013, http://www.svaboda.org/content/article/24569492.html; "The police threatened to take me to the woods and shoot", http://udf.by/english/main-story/59240-the-police-threatened-to-take-me-to-the-woods-and-shoot-photo.html.

[94] "Милиция избила витебчанина за просмотр сайта Хартии 97," [Police beat a Vitebsk customer k for reading the Charter 97 website], Charter97.org, accessed on February 2, 2013, http://charter97.org/ru/news/2012/5/8/51879/pf.

[95] Iryna Lewshyna, "Two young men linked to opposition online communities get jail terms," Belapan, August 31, 2013, http://en.belapan.com/archive/2012/08/31/571400_571404.

[96] "Затрыманых студэнтаў-вікіпедыстаў адпусьцілі" [Detained students - "wikipedists" were released], Svaboda.org, February 17, 2013, http://www.svaboda.org/content/article/24904651.html.

One observer suggests that the August crackdowns were related to appeals for a public boycott of the September 2012 parliamentary elections, which the government considered to be both illegal and a threat to its legitimacy. First embraced by some opposition political parties, the calls for a boycott were taken up and advocated for by some internet communities.[97] Dunja Mijatovic, the OSCE Representative on Freedom of the Media, condemned the persecution and noted that they "show continued efforts to muzzle dissenting voices and clamp down on freedom of expression online."[98]

Instances of technical attacks against the websites of independent media and civil society groups have continued to grow. Trojans are often used to spy on opposition activists and the independent media. In April, Iryna Khalip, a prominent Belarusian journalist and correspondent for the Russian newspaper *Novaya Gazeta*, received an infected file from an unknown user via Skype. The file posed as a photo of a document with a list of questions to be discussed during an urgent government meeting concerning the fate of her then imprisoned husband, former presidential candidate Andrei Sannikov. This Trojan, sent by an unknown user, was investigated by independent experts and found to have successfully infected 14 other computers, most of which belonged to Belarusian opposition politicians and civic activists.[99]

A similar tactic was used against the independent trade union of the Belarusian Radio and Electronics Workers (REP). After the Skype and e-mail accounts of its leaders were hijacked with Trojan software, the hackers pretended to be REP representatives and contacted the union's Danish partners in an attempt to obtain financial information regarding joint projects. This attack coincided with the confiscation of a laptop of a REP activist, Andrej Strizhak, by border control officers, and with verbal attacks against REP by state officials.[100]

From July through August 2012, the website of "Platform," an organization defending the rights of prisoners, experienced repeated distributed denial-of-service (DDoS) attacks. On August 7, 2012, the site was inaccessible for six hours. On the same day, the deputy director of the organization was detained near her house for allegedly "using bad language" in public.[101] On August 31, 2012, unknown persons hacked the blog of the prominent opposition politician Viktar Ivashkevich on the popular news website Belaruspartisan.org. A text insulting Iryna Khalip was posted on the blog on behalf of Ivashkevich.[102]

---

[97] Vadzim Smok,"Internet Activism Under Siege in Belarus," Belarus Digest, September 11, 2012, http://belarusdigest.com/story/internet-activism-under-siege-belarus-11112.
[98] Tanya Korovenkova, "OSCE media freedom representative concerned about crackdown on online dissent in Belarus," September 4, 2012, http://en.belapan.com/archive/2012/09/04/en_15260904H.
[99] "Хартыя выкрыла чарговы траян спецслужбаў," [Charter unveiled another Trojan spread by intelligence], NN.by, April 25, 2012, http://nn.by/?c=ar&i=72400.
[100] "Скайп и почтовый ящик профсоюза РЭП взломали," [Skype and email account of REP trade union hacked], Praca-by.info, August 7, 2013, http://www.praca-by.info/cont/art.php?&sn_nid=4805&sn_cat=1.
[101] "Сайт ""Плятформы" зноў спрабавалі ўзламаць," ["Platforma" website was attacked again], Svaboda.org, August 7, 2012, http://www.svaboda.org/content/article/24669047.html.
[102] Iryna Lewshyna, "Two young men linked to opposition online communities get jail terms," Belapan, August 31, 2013, http://en.belapan.com/archive/2012/08/31/571400_571404.

On April 2, 2013, the website of the Mogilev branch of the Viasna Human Rights Center was hacked and a fake article, containing threats by a human rights defender against an independent journalist, was posted.[103] On April 23–26, 2013, four independent websites were hacked. On April 23, the Charter 97 website experienced a DDoS attack and ceased to function for an hour. The attacker was not identified, but Charter 97 attributed the attack to the Belarusian special services.[104] On the morning of April 25, Belaruspartisan.org was attacked and a threatening letter from anonymous hackers was posted on the site.[105] In the evening of that same day, the Viasna Human Rights Center website was hacked. Several publications posted on the site were distorted after attackers gained unauthorized access. The attack affected all three language versions of the site.[106] On April 26, the website of the Belarusian Association of Journalists also experienced a DDoS attack, which started half an hour after an article was published titled, "Why independent websites are being hacked."[107]

Belarusian criminal law prohibits these types of "technical violence." Specifically, Article 351 of the Criminal Code, covering "computer sabotage," stipulates that the premeditated destruction, blocking, or disabling of computer information, programs, or equipment is punishable by fines, professional sanctions, and up to five years in prison.[108] A special department at the Ministry of Internal Affairs is tasked with investigating such crimes. In reality, a number of the attacks on the independent websites and personal accounts of democratic activists have been linked to the authorities. The government has stated its intention to accede to the Council of Europe's Convention on Cybercrime, but it has made no move to sign on to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[109]

[103] "Праваабаронцы выступілі з заявай наконт узлому сайта магілёўскай 'Вясны'"[Human rights defenders made a statement in connection with the hacker's attack on Mogilev "Viasna" website], Belarusian Association of Journalists, April 4, 2013, http://baj.by/be/node/20342.
[104] "Charter 97 under attack," Charter 97, April 23, 2013, http://charter97.org/en/news/2013/4/23/68349.
[105] "Belaruspartizan website cracked," Belarusian Association of Journalists, April 25, 2013, http://baj.by/en/node/20617.
[106] "Viasna's website resumes work after hacker attack," Viasna, April 26, 2013, http://spring96.org/en/news/62869.
[107] "Сайт БАЖ подвергся хакерской атаке" [BAJ's website experienced hacker's attack], Gazetby.com, April 26, 2013, http://gazetaby.com/cont/art.php?sn_nid=56172.
[108] "«Белтелеком»: Возможно, независимые сайты блокировали другие организации" [Beltelecom: Independent websites could be blocked by other organizations], Charter 97, January 10, 2008, http://www.charter97.org/ru/news/2008/1/10/2905.
[109] Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," 1 January 1981, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CL=ENG.

BRAZIL

	2012	2013
INTERNET FREEDOM STATUS	FREE	PARTLY FREE
Obstacles to Access (0-25)	7	7
Limits on Content (0-35)	6	8
Violations of User Rights (0-40)	14	17
Total (0-100)	**27**	**32**

* 0=most free, 100=least free

POPULATION: 194.3 million
INTERNET PENETRATION 2012: 50 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Brazil's Electoral Law, which prohibits online media and traditional broadcasters from focusing on candidates for three months prior to an election, took center stage ahead of the October 2012 municipal elections, resulting in increased takedown notices and prosecutions of users found in violation of the law (see **LIMITS ON CONTENT**).
- High-profile cases of intermediary liability—including criminal charges against Google executives—attracted international attention in 2012 and 2013 (see **LIMITS ON CONTENT**).
- Retaliatory violence and intimidation of online journalists and bloggers increased in late 2012 and early 2013. Eduardo Carvalho, owner and editor of the *Ultima Hora News* website, was murdered in November 2012 in connection with his online work (see **VIOLATIONS OF USER RIGHTS**).
- Brazil's cybercrime law went into effect and its reconfigured Azeredo Bill, which establishes a framework for judicial takedown notices, was approved in April 2013 (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Brazil, which was first connected to the internet in 1990, has made significant gains in expanding internet access and mobile phone usage in recent years, offering tax incentives to the purveyors of information and communication technologies (ICTs) for continued investment in Brazilian infrastructure, and providing public access points (LAN houses) to citizens in order to facilitate internet connectivity.[1] Despite such notable progress in increasing ICT availability, particularly via mobile technologies—4G services were introduced to Brazil in late April 2013—Brazil still faces challenges in its quest to reach internet penetration rates commensurate with the country's economic wealth.

According to the International Telecommunication Union (ITU), Brazil's internet penetration rate falls below the average enjoyed by North American and European countries, as does the number of Brazilian households with computers. Among the primary reasons for these deficiencies are faulty infrastructure, social inequality, and poor education. In order to combat such issues, the federal government has executed several national policies over recent years, resulting in an increase in social network activity and internet-mediated civic participation.[2]

There is no evidence of the Brazilian government employing technical methods to filter or otherwise limit access to online content; however, it does frequently issue content removal requests to Google, Twitter, and other social media companies. Such requests increased in 2012 ahead of Brazil's municipal elections, with approximately 235 court orders and 3 executive requests imploring Google to remove content that violated the electoral law.[3] The law's prohibition of any content that ridicules or could offend a candidate directly impacted freedom of online expression and played a pivotal role in two highly publicized cases of intermediary liability extending to Google executives. Law 9.054 prohibits online and traditional media from publishing stories about candidates for three months prior to elections. It also bans candidates from advertising on the internet for the same period of time unless they are contenders for the office of president.[4]

Additional challenges to online expression in 2012 and 2013 came from civil defamation suits, increasing violence against bloggers and online journalists, and legal action by the judiciary and government officials. The penalties for such charges extend to content removal and fines. Brazil has

---

[1] Robert Hobbes Zakon, "Hobbes' Internet Timeline v8.2," Zakon Group LLC, accessed August 11, 2010, http://www.zakon.org/robert/internet/timeline/; Tadao Takahashi, ed., *Sociedade da Informação no Brasil: Livro Verde* [Information Society in Brazil: Green Book] (Brasilia: Ministry of Science and Technology, September 2000), http://www.mct.gov.br/index.php/content/view/18878.html; National Education and Research Network (RNP), "Mapa do Backbone" [Map of Backbone], accessed August 11, 2010, http://www.rnp.br/backbone/index.php.

[2] Cetic.br, Communication Technologies, pg. 236, February 15, 2013, http://www.nic.br/english/activities/ceticbr.htm.

[3] Sarah Laskow, "Google vs. Brazil: Why Brazil Heads Google's List of Takedown Requests," April 29, 2013, Columbia Journalism Review, http://www.cjr.org/cloud_control/brazilian_takedown_requests.php?page=all&print=true.

[4] http://www.article19.org/data/files/pdfs/press/brazil-proposed-electoral-law-restricts-internet-freedom.pdf; See also: Article 19, Press Release: Brazil: Proposed Electoral Law Restricts Internet Freedom, September 14, 2009, http://www.article19.org/data/files/pdfs/press/brazil-proposed-electoral-law-restricts-internet-freedom.pdf, and Gabriel Elizondo, "Brazilian Elections No Joke – Literally," August 25 2010, AlJazeera, http://blogs.aljazeera.com/blog/americas/brazilian-elections-no-joke-literally.

also witnessed an ongoing trend in which private litigants and official bodies sue internet service providers (ISPs) and ask for takedown notices to be sent to blogging and social-networking platforms. As Brazil rises to the level of other leading global economies and comes closer to a networked society, issues such as cybercrime and distributed denial-of-service (DDoS) attacks, access to public information, election campaigning on the internet, and intellectual property protection are increasingly in the spotlight.

Although 2012 was witness to positive legislation regarding cybercrimes, the right to information, and open governmental action plans, frustration has surrounded Brazil's Marco Civil Bill, also known as the "Civil Rights Framework for the Internet," introduced to Congress in August 2011. Congressional vote on this policy—which aims to guarantee access to the internet, safeguard freedom of speech and communication, protect privacy and personal data, and preserve net neutrality, among other provisions—was postponed five times during 2012. As of May 2013, a vote had not yet occurred.[5] The main barrier to passage of the Marco Civil Bill has been Brazil's telecom lobby, which objects to some of the provisions regarding net neutrality.

OBSTACLES TO ACCESS

Although development of information and communication technologies (ICTs) has increased in recent years, Brazil still lags behind many developing countries in terms of relative proportion of citizens with internet access.[6] Widespread adoption of household internet services has been hindered by high costs, low quality, and regional infrastructural disparity. Despite these challenges, a number of government initiatives predicated on increasing national internet penetration have begun to bear fruit. The country's mobile sector is thriving, and Brazilians are increasingly turning to smartphones to connect to the internet. As of mid-2013, Brazil was home to the largest mobile phone market in Latin America.[7]

Internet penetration varies greatly among different geographical regions in Brazil due to inconsistent infrastructure; access also varies from urban to rural areas. In 2012, Brazil's aggregate penetration rate was 50 percent.[8] The latest figures from the Brazilian Internet Steering Committee portray disparate figures in urban versus rural areas: household penetration was measured at 43 percent in urban zones, compared to 10 percent in rural areas. Internet access is also less widespread in urban areas in the Northeast (22 percent penetration) than in the Southeast (49

[5] Murilo Roncolato, "Marco Civil é Adiado Pela Quinta Vez" [Marco Civil is Postponed for the Fifth Time] *Link* (blog), February 15, 2013, http://blogs.estadao.com.br/link/marco-civil-e-adiado-pela-quinta-vez/.
[6] International Telecommunication Union (ITU), "Percentage of Individuals Using the Internet," 2011, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#; and "Fixed (wired) Broadband Subscriptions," http://www.itu.int/ITUD/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2011&RP_intLanguageID=1&RP_bitLiveData=False.
[7] Sergio Spagnuolo, "Brazil Launches 4G Wireless Service with Few Smartphone Options," *Reuters*, April 17, 2013, http://www.reuters.com/article/2013/04/17/brazil-telecom-smartphones-idUSL2N0D32ON20130417.
[8] International Telecommunication Union (ITU), *Statistics: Percentage of Individuals Using the Internet, 2000-2012*, ITU, June 17, 2013, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls.

percent penetration).[9] Although the number of broadband connections is increasing as prices begin to fall, widespread adoption of high-speed household connections has been delayed by a lack of infrastructure and a market dominated by major telecommunications and cable companies.

There are no specific legal or economic restrictions related to operating ISPs, mobile, or other digital technology providers, yet the Brazilian market remains highly concentrated. As of the fourth quarter of 2012, four companies—Oi, NET, Telefonica, and GVT—accounted for roughly 90 percent of the country's broadband market.[10] Fixed broadband technology, such as DSL and cable, accounts for 68 percent of household internet connections in Brazil. While mobile broadband, measured at 18 percent, is still in the minority, such technology now accounts for most new household broadband connections. In 2011, mobile broadband subscriptions exceeded dial-up connections for the first time, indicating that Brazil is following global broadband growth trends.[11]

Public paid access centers—also known as local area network, or LAN, houses—are the primary means of internet access for low income Brazilians in many regions, providing access to nearly 68 percent of those from the lowest income brackets.[12] A report from the Brazilian Internet Steering Committee noted a 10 percent decrease in use of LAN houses for internet access between 2011 and 2012. Nonetheless, such access points remain relevant to digital inclusion in Brazil, particularly in the northernmost regions of the country, where they are the second most commonly used means of connection after households.

Six private companies dominate Brazil's mobile sector, the largest four of which—Oi, TIM, Claro, and Vivo—control over 99.8 percent of market share.[13] Mobile penetration has grown significantly over the past five years, increasing by an average of 19 percent annually, and reaching 145 percent by the end of 2012.[14] Smartphone sales also increased by 77 percent in the first half of 2012 as compared to the same period in 2011.[15] Given such growth, Reuters forecasts that Brazil will become the fifth largest smartphone market in the world by the end of 2013.[16]

Investment in mobile technology is further increasing due to the perceived demands of the World Cup, which will be hosted by Brazil in 2014. The country's four largest mobile providers each

[9] Brazilian Internet Steering Committee (CGI.br), "Survey on the Use of Information and Communication Technologies in Brazil 2011," pg. 436, on February, 15, 2013, http://op.ceptro.br/cgi-bin/cetic/tic-domicilios-e-empresas-2011.pdf.
[10] Teleco, "Seção: Banda Larga—Market Share de Banda Larga no Brasil" [Section: Broadband—Market Share of Broadband in Brazil], January 20, 2013, http://www.teleco.com.br/blarga.asp.
[11] Brazilian Internet Steering Committee (CGI.br), "ICT Households and enterprises 2011 - Survey on the use of Information and Communication Technologies in Brazil" pg. 358, Accessed February 20, 2013, http://bit.ly/Poj2ue.
[12] Brazilian Internet Steering Committee (CGI.br), "Survey on the Use of Information and Communication Technologies in Brazil 2011," pg. 436, on February, 15, 2013, http://op.ceptro.br/cgi-bin/cetic/tic-domicilios-e-empresas-2011.pdf.
[13] Teleco, "Seção: Telefonia Celular—Operadoras de Celular, Jun/10" [Section: Cellular Telephony—Cellular Operators, June 2010], Accessed February, 2013, http://www.teleco.com.br/mshare.asp.
[14] Budde.com, "Brazil - Telecoms, Mobile, Broadband and Forecasts 2012," Budde.com, Accessed February 2013, http://www.budde.com.au/Research/Brazil-Telecoms-Mobile-Broadband-and-Forecasts.html?r=51.
[15] Teleco, "Seção: Telefonia Celular—Estatísticas de Celulares no Brasil" [Section: Cellular Telephony—Statistics of Cellular Telephones in Brazil], February 6, 2012, http://www.teleco.com.br/ncel.asp; See also: Roberta Prescott, "Brazilian smartphone sales increase 77% to 6.8 million in 1H 12," September 14, 2012, http://bit.ly/PBrRTj.
[16] Sergio Spagnuolo, "Brazil Launches 4G Wireless Service with Few Smartphone Options," *Reuters*, April 17, 2013, http://www.reuters.com/article/2013/04/17/brazil-telecom-smartphones-idUSL2N0D32ON20130417.

began offering 4G services in April 2013 ahead of the Confederations Cup[17] and each company has signed an agreement with National Telecommunications Agency ANATEL to provide 50 percent coverage in major cities by June 2013.[18] It is likely that the timing of this agreement (which required that the companies be 4G ready ahead of the Confederations Cup) was conceived in order to provide the technology ample time for adoption—as well as a trial run—before the World Cup. Despite high hopes that 4G will elevate Brazil's technological capacity, consumer advisory board *Reclame* has advised consumers that the expensive new service is unlikely to live up to its potential until infrastructure is improved. Such a prediction is unsurprising given that 40 percent of mobile phone users are reportedly unhappy with the quality of their current 3G coverage.[19]

In recent years, the Brazilian Government has initiated multiple programs to connect the population to the internet. The National Broadband Plan, for example, launched in 2010, aims to triple broadband access by 2014.[20] An increase in ICTs over the past few years, along with an attendant increase in the number of internet users, has also encouraged governmental agencies to improve the accessibility and quality of information available on institutional websites.[21] In February 2012, the government announced a series of planned investments and tax incentives intended to expand various ICT and technological capabilities throughout the country. The development portion of the plan includes the expansion of the national fiber-optic cable from 11,000 to 30,000 km, the renewal of the One Laptop per Child program, and the extension of broadband technology to an additional 13 million households.[22] It was also reported that tax incentives would apply to various technologies, including tablets, which would be distributed to public school teachers, presumably to increase digital literacy in classrooms. Following reports that tablets would benefit from tax incentives, sales increased by 127 percent.[23] Incentives were also extended to telecom companies in exchange for an agreement to invest $8 billion in Brazilian ICT infrastructure by 2016.[24]

Brazil's digital information landscape is largely unrestricted. Brazilians freely gather information from the internet, as well as through mobile phone technology and other ICTs. They also have access to a wide array of national and international news sources, blogs, social-networking

[17] Telecompaper, "Oi Launches 4G Services in Rio de Janeiro," April 26, 2013, Telecompaper.com, http://www.telecompaper.com/news/oi-launches-4g-service-in-rio-de-janeiro--939998.
[18] Ben Tavener, "4G Data Services Launched in Rio," *The Rio Times*, April 26, 2013, http://riotimesonline.com/brazil-news/rio-business/4g-services-mobile-launched-in-rio/.
[19] Angelica Mari, "We've Got 4G in Brazil! Oh, Wait…," *Brazil Tech*/ZDNet, May 8, 2013, http://zd.net/10dWeQb.
[20] Ministry of Communications, "Um Plano Nacional para Banda Larga" [A national plan for high bandwidth], accessed August 30, 2012, http://www4.planalto.gov.br/brasilconectado/pnbl.
[21] Marcelo Sarkis, "Access to Public Information in Brazil: What Will Change with Law No. 12.527/2011?" Freedominfo.org, May, 14, 2012, http://bit.ly/LK0P89.
[22] Roberta Prescott, "Brazil Announces Tax Breaks to Boost Economy; Positive Impacts for ICT Sector," RCR Wireless, April 4, 2012, http://bit.ly/HfWVBq.
[23] Joe Aimonetti, "Apple gets tax incentives in Brazil to begin iPad production," CNET, January 25, 2012, http://reviews.cnet.com/8301-19512_7-57366337-233/apple-gets-tax-incentives-in-brazil-to-begin-ipad-production/; See also: (1) "Primeiros a receber tablets serão professores, anuncia MEC," Estadao.com.br, February 3, 2012, http://www.estadao.com.br/noticias/vidae,primeiros-a-receber-tablets-serao-professores-anuncia-mec,830914,0.htm [in Portuguese] and (2) Roberta Prescott, "Hot market for tablets in Brazil," RCR Wireless, January 2, 2013, http://www.rcrwireless.com/americas/20130102/devices/hot-market-tablets-brazil/.
[24] Ben Tavener, "4G Data Services Launched in Rio," *The Rio Times*, April 26, 2013, http://riotimesonline.com/brazil-news/rio-business/4g-services-mobile-launched-in-rio/.

platforms, and citizen journalism, the latter of which has proliferated over the past year. In keeping with Brazil's ardent and growing internet user database, economists predict that eCommerce in Latin America's largest economy will total $18.7 billion in 2012, representing a 21.9 percent increase from 2011.[25]

Social media and communication apps such as Orkut, Facebook, and YouTube are freely accessible and widely used in Brazil. In December 2011, Facebook surpassed Orkut, its rival within the country, in terms of subscribers. As of June 2012, 42 million Brazilians had Facebook accounts, a number which had ballooned to nearly 67 million by February 2013, ranking Brazil as the second largest user of Facebook after the United States. As a nation, Brazil is also home to the fifth-largest contingent of Twitter users in the world; among non-English speaking countries, it has the highest percentage of users globally.[26]

Two regulatory bodies oversee Brazilian ICTs: ANATEL, viewed by some Brazilians as inefficient, and the Administrative Council for Economic Defense (CADE), an antitrust body that is perceived to be more effective in addressing complaints. While both regulators are tasked with ensuring free, fair, and independent operation of ICTs, the General Telecommunications Law also authorizes CADE to make decisions concerning market concentration and price setting.[27] Despite the presence of these regulatory bodies, competition between ICTs remains uneven. The Brazilian Internet Steering Committee (CGI.br), a multi-stakeholder organization created in 1995, has played a substantive role in Brazilian internet governance and regulation debate.[28] The Committee's contributions include reliable and comprehensive yearly reports on the state of internet adoption in Brazil as well as funding for internet governance-related research and academic publications. Committee members are drawn from the government, the private sector, academia, and nongovernmental organizations. The latest group of representatives was chosen in 2010 in relatively democratic and open elections.[29]

LIMITS ON CONTENT

The Brazilian government does not employ technical methods to filter or otherwise limit access to online content. Nonetheless, legal action pertaining to content removal by the judiciary and government officials, as well as highly publicized cases of intermediary liability, have emerged as possible barriers to free speech. Ahead of the October 2012 Municipal Elections, stringent enforcement of the Brazilian electoral law, which prohibits coverage of candidates in online and

[25] Brazilian Internet Steering Committee (CGI.br), "Survey On The Use Of Information And Communication Technologies In Brazil 2011," p. 297; See also: "More Buyers Join Brazil's Robust Ecommerce Market" http://bit.ly/13V1sYm.
[26] New Media Trend Watch, "Brazil: European Travel Commission (ETC)," New Media Trend Watch, Accessed February 2013, http://www.newmediatrendwatch.com/markets-by-country/11-long-haul/42-brazil.
[27] Maria Cecília Andrade, Ubiratan Mattos, and Pedro C. E. Vicentini, "Reforms in Brazilian Telecommunications Regulations and their Impact on Sector Competition," in *The Antitrust Review of the Americas 2009* (London: Global Competition Review, 2009), http://bit.ly/1fRMA0S; See also: Teleco, "Regulation: Legislation Guide," July, 28, 2010, http://bit.ly/19NMMIw.
[28] CGI.br, *Principles for the Governance and Use of the Internet*, accessed February16, 2013, http://www.cgi.br/english/regulations/resolution2009-003.htm.
[29] CGI.Br, "CGI.br Anuncia Nomes dos Representantes Eleitos da Sociedade Civil" [CGI.br announces names of elected representatives], Accessed February 16, 2013, http://www.nic.br/imprensa/releases/2011/rl-2011-05.htm.

traditional media for three months prior to elections and also bans any online content which might "offend the dignity or decorum" of a candidate, added to the challenges associated with freedom of online expression.[30] While fears have also surfaced regarding Brazil's international image and censorship of national issues such as poverty ahead of the 2014 World Cup and 2016 Olympic Games, social media have been used for positive citizen action in recent years, extending to advocacy for the rights of indigenous communities.

Neither federal nor state governments have sponsored systematic content filtering or online censorship, however efforts to place limits on content have occurred periodically. A Google Transparency Report shows that in 2012, Brazil issued the highest number of government requests for content removal of any country.[31] Brazil also ranks in the top three countries in all categories related to requests for content removal on Twitter's Transparency Report,[32] with 16 court orders issued between July and December 2012.[33] Recent cases related to content removal concern defamation, nudity, and concern over Brazil's international image. In May 2012, Facebook made the decision to remove photos of "SlutWalk," demonstrations in which topless women advocated for women's rights in various Brazilian cities. Facebook affirms that the censored photos constitute "nudity and pornography,"[34] and removal is therefore in line with company policy. Members of SlutWalk allege that Facebook's decision constitutes censorship of civil society action and urge the company to "distinguish between pornography and protest material" when removing content.[35] In a separate instance, Google reportedly received requests from the Brazilian government to remove the world "favela" (slum) from its maps of the country, in order to detract attention from Brazil's poor neighborhoods in advance of the 2014 World Cup and 2016 Olympic Games. Bloggers have been vocal in their condemnation of such censorship.[36]

In July 2012, digital newspaper Século Diário received a court order to remove three articles and two editorials from its site, all of which concerned the performance of Prosecutor Marcelo Barbosa de Castro Zenkner. The judge further ruled that Século Diário must follow editorial recommendations stipulated by the court in future posts. This was the third time that Século Diário was issued a court order for the removal of content.[37] In November 2012, a judge prohibited media

[30] Sarah Laskow, "Google vs. Brazil: Why Brazil Heads Google's List of Takedown Requests," April 29, 2013, Columbia Journalism Review, http://www.cjr.org/cloud_control/brazilian_takedown_requests.php?page=all&print=true.
[31] Google, "Transparency Report," Google, Accessed February 15, 2013, http://www.google.com/transparencyreport/removals/government/BR/.
[32] Nick Kolakowski, "Twitter's New Transparency Report: Governments Still Want Your Data," Slashdot, January 28, 2013, http://slashdot.org/topic/bi/twitters-new-transparency-report-governments-still-want-your-data/; See also: (1) Twitter, Transparency Report, "Government Requests Received for User Information", Accessed February 15, 2013, https://transparency.twitter.com/information-requests-ttr2; and (2) Twitter, Transparency Report, "Government Requests Received to Withhold Content", accessed on February 15, 2013, https://transparency.twitter.com/removal-requests-ttr2.
[33] Twitter, Transparency Report, "Government Requests Received to Withhold Content", accessed on February 15, 2013, https://transparency.twitter.com/removal-requests-ttr2.
[34] Raphael Tsavkko Garcia, "Brazil: Facebook Censors Photos of the 'SlutWalk'," Global Voices Online, June 2, 2012, http://globalvoicesonline.org/2012/06/02/brazil-facebook-censor-photos-slutwalk/.
[35] Raphael Tsavkko Garcia, "Brazil: SlutWalks Spread across the Country," Global Voices Online, May 29, 2012, http://globalvoicesonline.org/2012/05/29/brazil-slutwalks-photos-videos/.
[36] Citizen Lab, "Latin America and the Caribbean CyberWatch," Citizen Lab, May 3, 2013, https://citizenlab.org/2013/05/latin-america-and-the-caribbean-cyberwatch-april-2013/.
[37] Natalia Mazotte, "Knight Center Launches Timeline of Judicial Censorship in Brazil," Knight Center for Journalism in the Americas, February 21, 2013, https://knightcenter.utexas.edu/blog/00-12987-knight-center-launches-timeline-judicial-

from mentioning the name of the current vice mayor and mayor-elect of the city of Campo Mourão in articles concerning an alleged vote-buying scandal that occurred during the election. Notifications of the order were sent to a number of print and digital news sites investigating the alleged scheme, including the websites of *Tásabendo* and *Coluna do Ely*. Should any of the outlets ignore the judicial order, they will face fines of up to $14,000.[38]

State-initiated censorship in Brazil has primarily appeared in the context of elections, with defamation charges and the removal of content related to elected officials becoming increasingly common. This phenomenon is due in large part to an electoral law, extended to the internet in 2009, which tightly restricts the airing by opponents of content related to political candidates.[39] In March 2012, a ruling by the Electoral Superior Court resulted in the application of "time and place" restrictions to political speech on Twitter and other social media platforms, as well as the internet at large.[40] Although the law does not benefit any particular party, but instead seeks to maintain a civil and dignified electoral process, it has come under fire by freedom of expression advocates for its restriction of content both online and offline. Journalists and bloggers cannot presently make accusations against candidates for three months prior to elections; if they post any inflammatory content online related to a political candidate, they risk having their writing or videos removed, as well as being fined or arrested for defamation and violation of the country's electoral law. A 2011 proposal to reform the current law would loosen pre-campaign restrictions, allowing for expanded discussion and campaigning by candidates online, so long as such political promotion is performed without intent of commercial gain.[41] Thus far, two committees have approved the bill; it is currently among those items prioritized for review.[42]

In late 2012 and early 2013, a spate of legal cases concerning intermediary liability drew worldwide attention to Brazil's internet policies. In September 2012, a Brazilian electoral court issued arrest warrants for two senior Google Brazil executives, Edmundo Luiz Pinto Balthazar and Fabio Jose Silva Coelho, for failure to remove content prohibited under electoral law. The executives were accused of violating a vague provision that bans campaign material which "offend[s] the dignity or decorum" of a candidate.[43] Although the arrest of Balthazar was quickly overturned by a higher court on grounds that "Google [was] not the intellectual author of the video…and [could not] be

---

censorship-brazil; See also: SIPIAPA, "Assembly 2012 – General Assembly, Sao Paulo, Brazil Reports," Published January 1, 2013, http://www.sipiapa.org/en/asamblea/brazil-35.

[38] Natalia Mazotte, "Judge in Brazil Blocks Media from Mentioning Mayor-Elect in Alleged Vote-Buying Scandal," Knight Center for Journalism in the Americas, November 29, 2012, https://knightcenter.utexas.edu/blog/00-12222-judge-brazil-blocks-media-mentioning-mayor-elect-alleged-vote-buying-scandal.

[39] Agência de Notícias da Justiça Eleitoral, "TSE Mantém Multa por Propaganda Eleitoral Antecipada em Blog a Favor de Dilma" [TSE Keeps Fine for Electioneering in Anticipation of Favor from Dilma], March 17, 2011, http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1363510; See also: Agência de Notícias da Justiça E`leitoral, "TSE Aplica Multa a PSDB-MG por Propaganda Antecipada em Favor de José Serra," [TSE Applies Fine to PSDB-MG for early Advertising in Favor of Jose Serra], November16, 2010, http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1345485.

[40] Tribunal Superior Eleitoral [Electoral Superior Court], "Candidatos só Podem Utilizar Twitter em Campanha Eleitoral a Partir de 6 de Julho" [Candidates can only Use Twitter for Electoral Campaign Starting July 6th], March 2012, http://bit.ly/zG9zEp.

[41] Rachel Librelon, "Proposta regula pré-campanha e propaganda eleitoral na internet," Agência Câmara de Notícias, May 13, 2011, http://bit.ly/jsm8mq [in Portuguese].

[42] http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=491421

[43] The Guardian staff and agencies, "Google Executive in Brazil Detained after Failure to Remove YouTube Video," The *Guardian*, September 26, 2012, http://www.guardian.co.uk/technology/2012/sep/27/google-brazil-remove-youtube-video.

punished for its propagation,"[44] the case was later reinstated, bringing Balthazar back into the realm of the judiciary. Google finally blocked access to the controversial video in late September 2012 under pressure from Brazilian courts.[45] In March 2013, Balthazar was denied habeas corpus relief (a writ or legal action requiring that a prisoner be taken before a judge in order to determine whether his detention is lawful[46]) and the Brazilian Superior Electoral Court upheld the criminal charges filed against him for failing to comply with an electoral court order.[47] Google maintains that as a platform it is not responsible for content published by users. Accordingly, the company announced that it would comply with only 35 of the 316 Brazilian court orders it received from July to December 2012 requesting the removal of content in violation of the country's electoral law. In the remaining 281 cases, Google said that it would "exercise its right of appeal…on the basis that content is protected by freedom of expression under the Brazilian Constitution."[48] As of May 2013, criminal cases against both Coelho and Balthazar were still pending in Brazil.

Social media platforms such as Facebook and Orkut have also been subject to intermediary liability issues and are the main target of civil liability claims regarding content removal and defamation. In response to an electoral court order in December 2011, Google removed four Orkut profiles with content that violated Brazil's electoral law.[49] State courts in Brazil are still largely divided on the issue of intermediary liability, however. Some attribute the legal burden to crowdsourcing websites and social networks; others have adopted a notice-and-takedown approach that imposes liability only if the intermediary fails to remove content after judicial notice. A Brazilian judge issued a court order to YouTube for the removal of an anti-Islam video which sparked worldwide controversy and was blamed for instigating outbursts of violence in multiple countries.[50] Citing fear of incitement to violence, Judge Gilson Delgado Miranda gave Google YouTube ten days to remove the trailer for the movie from its website.[51] Nationwide legislation pertaining to takedown processes has been under debate in Brazil since the Marco Civil Bill, which includes a provision for the establishment of a judicial notice-and-takedown framework, began gaining media attention in 2009.

The Marco Civil Bill is intended to serve as a "Constitution for the Internet," guaranteeing freedom of expression, net neutrality, and the right to privacy.[52] Although previously lauded by Brazilian

---

[44] The Guardian staff and agencies, "Google Executive in Brazil Detained after Failure to Remove YouTube Video," Th*e Guardian*, September 26, 2012, http://www.guardian.co.uk/technology/2012/sep/27/google-brazil-remove-youtube-video.
[45] Reporters Without Borders, "Content Removal: Call for Quick Adoption of Internet Law Amid Continuing Harassment of Technical Intermediaries," October 2, 2012, Reporters Without Borders online, http://bit.ly/SAkmbI.
[46] Cornell University Law School, *Legal Information Institute*, Cornell University, Accessed September 20, 2013, http://www.law.cornell.edu/wex/habeas_corpus.
[47] Paulo Sa Elias, "Contempt of Court," Paulo Sa Elias, March 21, 2013, http://www.direitodainformatica.com.br/?p=1420.
[48] Google Transparency Report, Brazil, Google, Accessed September 27, 2013, http://bit.ly/QIAicO.
[49] Brad Haynes, "Google Executive in Brazil Faces Arrest over Elections Law," Reuters, Sep 25, 2012, http://www.reuters.com/article/2012/09/26/net-us-google-brazil-election-idUSBRE88O18B20120926.
[50] Reuters, "Brazil Court Ordered YouTube to Remove Anti-Islam Film," Reuters Brazil, September 26, 2012, http://www.reuters.com/article/2012/09/26/us-protests-brazil-idUSBRE88P05A20120926.
[51] Sorcha Pollack, "Google Executive Arrested as Brazil Bans Anti-Muslim Film," *Time*, *Newsfeed* (blog), September 27, 2012, http://newsfeed.time.com/2012/09/27/google-executive-arrested-as-brazil-bans-anti-muslim-film/; See also:Jenny Barchfield and Juliana Barbassa, "Fabio Jose Silva Coehlo, Google Exec, Detained by Brazil Police over Refusal to Pull YouTube Clips Criticizing Politicians," *Huffington Post*, September 26, 2012, http://huff.to/OrE52s.
[52] Carolina Rossini, "The Brazilian Congress Needs to Pass Marco Civil for Brazilians – and the World," Infojustice online, May 22, 2013, http://infojustice.org/archives/29726.

civil society, last-minute changes—including a provision that excludes copyright claims—threaten the bill's original promise, leaving users and ISPs in a climate of legal uncertainty.[53] Activists warn that recent changes could pave the way for the removal of allegedly copyrighted content without a judicial order. Copyright owners could then sue intermediaries for alleged content infringement by users, a precedent that could force ISPs to police users themselves. The final language used in the new exclusionary paragraph of the Marco Civil Bill may also threaten legal certainty surrounding safe harbors for ISPs. [54] Despite deep concern about these changes, House Representative Alessandro Molon is optimistic that the Marco Civil Bill will come to vote in the Chamber of Deputies and be signed into law by the end of 2013.[55]

Over the past few years, Brazil has made several important developments regarding access to public information. The Access to Information initiative, signed into law in November 2011, went into effect in early 2012 and promises to increase transparency and enhance opportunities for civic participation, social action, and the exposure of corruption.[56] The enactment of the Access to Information Act affords citizens the ability to request governmental information via the internet, while also requiring that state bodies utilize the internet for the disclosure of information about public administration, projects, and finances, all of which must be presented in an easily accessible and understandable manner and kept up to date.[57] Brazil is also a founding member of the Open Government Partnership—a global effort to increase government transparency, efficacy, and accountability.[58] Brazil's Action Plan for Open Government includes the adoption of measures that will allow the country to (1) continue making headway in public transparency, (2) strengthen access to information, (3) manage public funds, (4) promote integrity in the public and private sectors, (5) foster citizen participation, and (6) deliver public services.[59] According to a recent OGP report, to date, Brazil has secured 32 commitments by 5 governmental bodies, 18 of which have already been completed. [60]

Social media is increasingly being used for civic activism in Brazil, with campaigns regarding indigenous rights,[61] sanitation and water,[62] and the need for reducing electoral campaign waste,[63]

---

[53] Carolina Rossini, "New Version of Marco Civil Threatens Freedom of Expression in Brazil," Electronic Frontier Foundation, November 9, 2012, https://www.eff.org/deeplinks/2012/11/brazilian-internet-bill-threatens-freedom-expression; See also: Rodrigo Borges Carneiro, "Internet Bill should Not Fail to Include the Respect for Intellectual Property as a Principle," *Entertainment Law Brazil* (blog) April 11th, 2013, http://entertainmentlawbrazil.com.br/2013/04/11/internet-bill-should-not-fail-to-include-the-respect-for-intellectual-property-as-a-principle/#more-1049.

[54] Carolina Rossini, "New Version of Marco Civil Threatens Freedom of Expression in Brazil," Electronic Frontier Foundation, November 9, 2012, https://www.eff.org/deeplinks/2012/11/brazilian-internet-bill-threatens-freedom-expression.

[55] Index on Censorship, "Threats to Online Free Speech are a Civil Society Defeat," March 27, 2013, http://bit.ly/16XBC5A.

[56] Article 19, "Brazil Adopts Access to Information Law," Article 19, November 22, 2011, http://bit.ly/sCLNZH.

[57] United Nations Online Training Centre, "Learner's Submission: Access to Information in Brazil" UNPAN, February 11, 2013, http://unpanelearning.wordpress.com/tag/freedom-of-information-act/.

[58] http://bit.ly/16laayQ.

[59] Open Government Partnership, "Brazil's Country Commitment to the Open Government Partnership," Open Partnership.org September 20, 2011, http://www.opengovpartnership.org/countries/brazil.

[60] Open Government Partnership, "Brazil's Country Commitment to the Open Government Partnership," Open Partnership.org September 20, 2011, http://www.opengovpartnership.org/countries/brazil.

[61] Sara Moreira, "From Indigenous Protest to Online Preaching, Portuguese Language Countries in 2012," Global Voices online, December 31, 2012, http://bit.ly/VTLUKH.

[62] Sara Moreira,"Brazil: Rio de Janeiro Demands Better Sanitation," Global Voices online, November 12, 2012, http://globalvoicesonline.org/2012/11/12/brazil-sanitation-rio-de-janeiro/.

popping up on Twitter and Facebook as people in all regions of the country call the government to action. In late 2012, the Guarani-Kaiowá, an indigenous community in Mato Grosso do Sul threatened with eviction from ancestral lands, found support on Facebook and other social media platforms. In late October and early November, a wave of protests occurred in six Brazilian cities, as well as in overseas locales as far flung as Germany, Portugal, and the United States. Although it is difficult to ascertain the impact of the protests, given that the Guarani-Kaiowá also sent a letter to legislators announcing an intention to fight to the death for their land, a federal judge decided to suspend their eviction.[64] Various campaigns for environmental rights have also been started on Twitter, Facebook, and other online forums, with online petitions being used to pressure the Secretary of State for the Environment to clean up pollution and prevent future sewage spills on local beaches.[65]

VIOLATIONS OF USER RIGHTS

The Brazilian constitution forbids anonymity but protects freedom of speech, including cultural and religious expression. Specific laws also establish freedom of the press.[66] Various cybercrime initiatives and court rulings made headlines in 2013 for their impact on regulation of computer intrusion, brand infringement, and discriminatory content. Although the internet is generally viewed as a freer atmosphere than traditional media, in 2012, 40 percent of the threats received by journalists and bloggers were related to content posted on personal blogs, websites, and social networks. This phenomenon emphasizes the multivariate challenges to freedom of expression on the internet, which concern not only legislation but also physical safety.[67]

An increase in retaliatory violence against journalists and bloggers in late 2012, which appears to bear a clear link to content they posted online, negatively impacts freedom of expression and has the potential to encourage self-censorship. According to Reporters Without Borders, Brazil is now one of the world's five deadliest countries for media personnel.[68] In 2012 and 2013, Brazil was also witness to instances of local officials bringing defamation suits against bloggers and online journalists. One blogger faced a prison sentence for a fictional story he posted online.

In recent years, various legislative initiatives have directly affected freedom of expression rights. The Azeredo Bill (Lei Azeredo, Law #12.735/2012), which pertains to regulation of content online, was approved in April 2013 after major changes to its original, highly controversial

[63] The "Quem Suja Agora" Facebook page was created to monitor and denounce the refusal to collect electoral campaign waste: https://www.facebook.com/quemsujaagora.
[64] Sara Moreira, "From Indigenous Protests to Online Preaching, Portuguese Language Countries in 2012," Global Voices Online, November 28, 2012, http://globalvoicesonline.org/2012/11/28/worldwide-protests-for-brazils-indigenous-guarani-kaiowa/; See also: *Huffington Post*, "Guarani-Kaiowa Land Dispute: Brazil Judge Suspends Eviction of Indians," *Huffington Post*, October 31, 2012, http://www.huffingtonpost.com/2012/10/31/guarani-kaiowa-eviction_n_2051454.html.
[65] Sara Moreira, "Brazil: Rio de Janeiro Demands Better Sanitation," Global Voices Online, November 12, 2012, http://globalvoicesonline.org/2012/11/12/brazil-sanitation-rio-de-janeiro/.
[66] An English translation of the Constitution is available here: http://www.v-brazil.com/government/laws/constitution.html.
[67] UN Refugee Agency, "Brazil: Serious crimes against free expression in 2012", Article 19, UNHCR, March 14, 2013 http://www.unhcr.org/refworld/docid/51499abf2.html.
[68] Reporters Without Borders, "Brazil," Reporters Without Borders, July 3, 2013, http://en.rsf.org/report-brazil,169.html.

proposal. By the time it was approved, only 6 of the law's initial 22 articles remained. These items establish the creation of specialized teams and sectors structured by the judicial police to combat cybercrimes and to take down racist content (other defamatory content is not directly covered by the bill). Takedowns require judicial notice, but can be issued before police investigations have begun.[69] Another initiative currently under consideration in the Senate, Bill 494/08, aims to impose a series of obligations on ISPs, websites, and blogs to ensure cooperation with the police in pedophilia investigations.[70]

Two recent court decisions have made headlines in regard to their potential to influence the scope of freedom of expression on the internet. In September 2010, popular newspaper Folha de São Paulo won an injunction against satirical blog Falha de São Paulo on grounds that the name and layout of the blog were too similar to that of the newspaper and constituted brand infringement. The domain Falhadespaulo.com.br was subsequently frozen. In a countersuit in early 2013 in which the blog owners fought back against the newspaper, a Brazilian court upheld the ruling, permanently disabling the satirical site.[71] Critics allege that such rulings set a dangerous precedent for censorship and interfere with diversity of online content while proponents applaud the court for upholding brand integrity and intellectual property standards.[72]

In two separate cases in 2012, legal proceedings were brought against bloggers for alleged defamation. In the first case, blogger Afrânio Soares was sued by Ipu city council president Carmen Pinto. If he is found guilty, Soares may be charged with fines of more than $ 12,000.[73] In the second case, defamation charges were filed against journalist and blogger José Cristian Góes in December 2012 for a fictional story he posted on his blog *Infonet*. The charges, which were both civil and criminal, were initiated by high court judge Edson Ulisses, who claimed that both he and his brother were defamed in the story, which mocks political corruption in Brazil but does not name or describe any particular person.[74] In early July 2013, Góes was sentenced to 7 months and 16 days in prison. The sentence has since been commuted to community service. Góes plans to appeal the ruling .[75]

---

[69] Rafaella Torres, "Aprovação de Leis sobre Crimes Cibernéticos" [Approval of Cybercrime Laws], *A2K Brazil* (blog) January 17, 2013, http://www.a2kbrasil.org.br/wordpress/2013/01/aprovacao-de-leis-sobre-crimes-ciberneticos/.

[70] Website of the Brazilian Senate, *PLS Senate Bill #494/2008*, submitted for review March 24, 2013, http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=88862.

[71] Raphael Tsavkko Garcia, "Cries of Censorship as Brazilian Satire Blog Ordered Shut Down," Global Voices Online, March 22, 2013, http://globalvoicesonline.org/2013/03/22/cries-of-censorship-as-brazilian-satire-blog-ordered-shut-down/.

[72] Katrina Kaiser, "Sorry We're Not Sorry: An Interview with Lino Bocchini of Falha de Sao Paulo," Electronic Frontiers Foundation, May 25, 2012, https://www.eff.org/deeplinks/2012/05/sorry-were-not-sorry-interview-lino-bocchini-falha-de-s-paulo; See also: Raphael Tsavkko Garcia, "Blog Countersues over Web Domain," Global Voices Online, May 7, 2012, http://globalvoicesonline.org/2012/05/07/brazil-blog-falha-countersues-folha-sao-paulo-web-domain/.

[73] Blog do Kleber Teixeira, "Vereadora entra com Processo contra Bloguiero" [Counselor Enters Blogger Trial], Blog do Kleber Teixeira (blog), July 15, 2012, http://www.blogdokleberteixeira.com/2012/07/vereadora-entra-com-processo-contra.html.

[74] Isabela Fraga, "Brazilian Prosecutor Files Criminal Charges Against Journalist for Writing Fictional Blog Post," Knight Center for Journalism in the Americas, February 15, 2013, https://knightcenter.utexas.edu/blog/00-12953-brazilian-prosecutor-files-criminal-charges-against-journalist-writing-fictional-blog-; See also: Reporters Without Borders, "Journalist gets 'Judicially Insane' Jail Term for Fictional Short Story," July 8, 2013, http://bit.ly/12SU1Pr.

[75] Rafael Spuldar, "Brazilian Writer Convicted for Fictional Story," Index on Censorship, July 15, 2013, http://www.indexoncensorship.org/2013/07/brazilian-writer-convicted-for-fictional-story/.

As mentioned above, several legal provisions, including Article 57-D of the recently revised electoral law, place restrictions on anonymity. Users are generally required to register with their real names before purchasing mobile phones or opening a private internet connection, though the use of pseudonyms in discussion forums is common. Despite the potential for registries to be employed to punish users for critical online speech, as of May 2013, there were no reports of such actions, nor were there reports of government efforts to track netizens participating in discussions critical of the government or particular social or political groups.

Extralegal surveillance of internet activities by the government is not believed to be widespread, although efforts to collect user data have increased in recent years. In 2012, the Brazilian government submitted more user data requests to Google than all other Latin American nations combined. Although there is no public count, most of these requests are believed to be warrants or court orders likely related to ongoing investigations or lawsuits. In the case of Twitter, most user information requests were tied to criminal investigations. With the exceptions of an emergency situation or a legal prohibition related to a specific case, Twitter notifies users of requests for account information. With a total of 2,777 information requests sent to Google in 2012, and 34 sent to Twitter, Brazil is ranked by both companies as third worldwide in number of requests, following the United States and Japan.[76]

Some lawmakers have pushed for legal provisions requiring the recording of internet communications from public access points such as LAN houses in order to prevent crime. Such surveillance, lawmakers say, would also allow LAN houses to avoid liability for acts committed by users. Legislation of this kind already exists in São Paulo and Rio de Janeiro. A federal measure pertaining to compulsory registration of LAN users was approved by the House of Representatives in 2011 and is currently in the Senate, where it has been approved by three commissions and now awaits a final report.[77] If finalized, the legislation would regulate LAN houses as "multi-purpose entities of special interest for digital inclusion," requiring them to register all users.[78]

In a disturbing trend, threats, intimidation, and violence against online journalists and bloggers have been increasing in recent years. In February 2012, Mario Randolfo Marques Lopes, editor-in-chief of news website *Vassouras na Net*, was kidnapped and murdered. Marques, who often reported on police corruption and violence, had previously survived a 2011 assassination attempt that left him in a coma for three days.[79] In late April 2012, Décio Sá, a longtime political journalist and blogger who wrote for the newspaper *O Estado do Maranhão* and ran a blog by the name of *Blog do Décio*, was

[76] Zach Miners, "Twitter Transparency Report Shows Government Data Requests on the Rise," Good Gear Guide, PC World Australia, January 28, 2013, http://bit.ly/TNX6Pc; See also: Google, "Transparency Report - Brazil : Summary of Requests," Accessed February, 2013, https://www.google.com/transparencyreport/userdatarequests/BR/.
[77] Federal Senate of Brazil, Portal Atividade Legislativa, *Projeto de Lei da Camara, No 28 de 2011* [Camara Bill, No. 28/2011], http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=100025.
[78] Draft Legislation no. 4361/2004, proposed by representative Vieira Reis, accessed February 7, 2012, http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=268907.
[79] Committee to Protect Journalists, "Mario Randolfo Marques Lopes," February 9, 2012, CPJ online, http://cpj.org/killed/2012/mario-randolfo-marques-lopes.php.

shot to death while sitting in a bar. Police suspect that Sá, who is survived by a pregnant wife and eight year old daughter, was targeted for his reporting.[80]

In July 2012, journalist Andre Caramante began receiving threats from Adriano Lopes Lucinda Telhada, a former military police commander and a candidate in the October 2012 municipal elections. The threats began after Caramante wrote a column that was critical of Telhada for newspaper *Folha de Sao Paulo*. Telhada quickly turned to Facebook to vent his anger, where he posted inflammatory messages that surpassed defamation and amounted to incitement of hatred, according to a press release from Reporters Without Borders. Telhada, who later won the municipal election and is now a councilman in Sao Paulo, denies having posted such material online.[81]

In November 2012, Eduardo Carvalho, owner and editor of the *Ultima Hora News* website, was murdered as he returned to his home in Campo Grande. Carvhalo, a former military police officer who often wrote about local corruption, had already survived one earlier attack on his life. Prior to his murder, Carvhalo had received so many death threats that he always carried a gun and often wore a bullet proof vest.[82] In December 2012, the home of Antonio Fabiano Portilho Coene, owner of the *Portal i9* website, was attacked by unidentified gunmen who threw a Molotov cocktail into the courtyard and fired shots on the house. Before leaving, the assailants placed a hammer outside the house with a message warning that Portilho would be beaten to death and referencing the murder of fellow corruption reporter Eduardo Carvalho. No injuries were sustained by Portilho or his family.[83]

Cyberattacks are a significant problem in Brazil, with targets ranging from online banking sites to energy plants.[84] In early 2012, the hacker group Anonymous made a significant impact by launching distributed denial-of-service (DDos) attacks against the websites of three of Brazil's largest banks,[85] including Banco de Brasil, the largest in the country. An increasing amount instructional material for hackers is also produced in Brazil, including information on how to conduct illegal mobile phone wiretaps or hack passwords.[86]

In April 2013, a Brazilian cybercrime law commonly referred to as "Lei Dieckman" came into force. The law's adopted moniker comes from actress Carolina Dieckman due to the fact that the

---

[80] Committee to Protect Journalists," Décio Sá," April 23, 2012, CPJ online, http://cpj.org/killed/2012/decio-sa.php.
[81] Danilo Thomaz, "'Nunca o Ameacei,' Diz Telhada Sobre Journalista"[I Never Threatened Him, Says Telhada of Journalist], Epoca online, October 8, 2012, http://glo.bo/PQykWO; "Online Hate Messages: Newspaper Reporter Targeted on Former Police Chief's Facebook Page," Reporters Without Borders, July 20, 2012, http://bit.ly/PiB7r6.
[82] Committee to Protect Journalists, "Brazilian Journalist Killed in Campo Grande," CPJ online, November 26, 2012, http://cpj.org/2012/11/brazilian-journalist-killed-in-campo-grande.php#more.
[83] Reporters Without Borders, "News Website Owner's Home Attacked in Brazil," IFEX, December 4, 2012, http://www.ifex.org/brazil/2012/12/04/brasil_actu_update_port/.
[84] Dmitry Bestuzhev, "Brazil: A Country Rich in Banking Trojans," Securelist, October 16, 2009, http://www.securelist.com/en/analysis/204792084/Brazil_a_country_rich_in_banking_Trojans.
[85] Kenneth Rapoza, "Hacker Group 'Anonymous' Gun For Brazil Banks; Itau Internet Banking Briefly Shut Down," Forbes, February 8, 2012, http://onforb.es/xtjC5w.
[86] For examples of tools for "do-it-yourself wiretapping," see: (1) ItecDiffusion.com: http://www.itecdiffusion.com/PT/escuta_telemovel.html; (2) Apostila Hacker [Hacker Toolkit]: http://www.apostilahacker.com.br/.

legislation took center stage after nude photos of her were distributed online in early 2012.[87] The law criminalizes breaches of digital privacy such as computer intrusion, the "installation of vulnerabilities," and editing, obtaining or deleting information—including credit card numbers—without authorization. The distribution, sale, production, or offer of programs or devices meant to facilitate the aforementioned actions or to interrupt ICT services are also categorized as crimes. Associated punishments vary from fines to up to five years imprisonment.

[87] The News Desk, "After 13 Years, Brazil Approves Two Cybercrime Laws at Once," *Linha Defensiva*, http://www.linhadefensiva.com/2012/11/after-13-years-brazil-approves-two-cybercrime-laws-at-once/.

BURMA

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	22	20
Limits on Content (0-35)	23	16
Violations of User Rights (0-40)	30	26
Total (0-100)	**75**	**62**

* 0=most free, 100=least free

POPULATION: 55 million
INTERNET PENETRATION 2012: 1 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Burma lifted online censorship in 2012—in practice, if not in law (see **LIMITS ON CONTENT**).
- In January 2013, Information Minister Thein Tun was dismissed on corruption charges after he blocked attempts to reduce the high cost of mobile SIM cards (see **OBSTACLES TO ACCESS**).
- A 2013 government distribution of cheaper SIM cards spawned a black market without improving service (see **OBSTACLES TO ACCESS**).
- Vicious online postings, some by officials, promoted violence that internally displaced over 120,000 Rohingya Muslims (see **LIMITS ON CONTENT**).
- A draft telecommunications law, though badly needed to attract foreign investment, retained repressive measures that were still being debated in mid-2013 (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Burma's nominally civilian government took significant steps in the past year to reform what was, until very recently, among the world's most repressive and underdeveloped telecommunication sectors, notably lifting a policy of media censorship that had been in place for the past 48 years in August 2012. Few limits on content remain online, and several experts privately told Freedom House that the government has no plans to expand monitoring and filtering technology nationwide.[1] If true, this liberalized attitude has yet to be supported by legal reform. Repressive media laws enacted by the military regime are still in place, and could be used at any time to punish online expression, while drafts prepared to replace them retained content restrictions and harsh penalties for violating them electronically. In summer 2013, lawmakers still appeared open to consultation to improve these drafts. Doing so would keep them on the startling upward trajectory the country registered for its internet freedom record in 2012.

The changes stem from Burma's gradual transition from military rule to democracy following what were widely viewed as sham 2010 elections that secured the junta's supporters an 80 percent majority in the legislature.[2] When parliament appointed Thein Sein—a military leader who had served as prime minister since 2007—as its first civilian president in March 2011, a political transformation seemed unlikely.[3] But Thein Sein proved a comparative moderate. While he maintained discriminatory policies against ethnic minorities like the Muslim Rohingya,[4] he also engineered a détente with opposition leader Aung San Suu Kyi and her National League for Democracy (NLD) party, which won 43 of the 44 parliamentary seats they contested in April 2012 by-elections.[5] Though the win was too small a gain to affect the balance of power in government, the NLD's participation alone was significant. Since the junta discounted a landslide NLD electoral victory in 1990, the opposition has either boycotted or been excluded from politics. Suu Kyi, a Nobel Peace laureate kept under house arrest for much of the past two decades,[6] was sworn into public office as a representative of the township of Kawhmu in the lower house of parliament on May 2, 2012.[7]

Burma's young information and communications technology (ICT) sector developed in a climate of fear and self-censorship under the junta. The government's first attempt to restrict internet freedom was through the 1996 Myanmar Computer Science Development Law, which made the

[1] Unless otherwise noted, all interviews for this report were conducted in Burma on the basis of anonymity.
[2] The military-led government renamed the country Myanmar without a referendum in 1989, a decision the opposition rejected as politicized. Many international governments and organizations, including Freedom House, retain the use of Burma on those grounds, though Myanmar is becoming more common since the regime has adopted a more civilian form of government.
[3] The Associated Press, "Burma Names Thein Sein as President," via *Guardian*, February 4, 2011, http://www.guardian.co.uk/world/2011/feb/04/burma-names-thein-sein-president.
[4] Human Rights Watch, "Burma: Rohingya Muslims Face Humanitarian Crisis," March 26, 2013, http://www.hrw.org/news/2013/03/26/burma-rohingya-muslims-face-humanitarian-crisis.
[5] "Myanmar Confirms Sweeping Election Victory for Suu Kyi's Party," CNN, April 4, 2012, http://www.cnn.com/2012/04/04/world/asia/myanmar-elections.
[6] "NLD Sweeps Parliamentary By-Elections," Radio Free Asia, April 2, 2012, http://www.rfa.org/english/news/burma/elections-04022012160808.html.
[7] "Burma's Aung San Suu Kyi Sworn in to Parliament," BBC, May 2, 2012, http://www.bbc.co.uk/news/world-asia-17918414.

possession of an unregistered computer modem and connection to unauthorized networks punishable by up to 15 years in prison.

How the industry will adapt once the model of state control is transformed has yet to be seen. In 2012 the government announced plans to systematically privatize its telecommunications sector. Yet the persisting state monopoly keeps costs high and quality low, while competing services, like voice over internet protocol applications, are banned. Although mobile phone use expanded in 2012, phone and internet connectivity remains extremely poor, and only a tiny percentage of the population has regular access to ICTs. In January 2013, just after Transparency International ranked Burma fifth worst worldwide out of 176 countries in a global survey of corruption in the public sector,[8] Information Minister Thein Tun became the first member of the cabinet to be dismissed amid an anti-graft probe, leading many to hope that these systemic inequalities are on the point of change.

Besides corruption, lack of coordination between government agencies and rivalries among ruling elites are also responsible for confusing and contradictory initiatives. SIM cards with quality service cost citizens over $200, while a 2013 government initiative to distribute them for $2 each was mired in corruption allegations by mid-year. The government is also planning to offer overseas visitors affordable mobile service during the December 2013 Southeast Asian Games as part of a bid to raise Burma's profile on the international stage; Burma is also chairing the ASEAN regional meeting in 2014.[9] Though the government awarded two foreign telecom companies licenses to provide service, observers say a draft telecommunication bill could oblige them to cooperate with state interception and monitoring of their users. Meanwhile, Chinese companies play a central role in sustaining the industry, but two of them, Huawei and ZTE, were implicated in the corruption investigation into Thein Tun, according to Radio Free Asia. Even while reforms are underway, the average Burmese user may be the last to benefit.

Burma's engaged online communities, however, are resilient, and their influence has often been felt beyond their comparatively small subset of the population. Many pushed the boundaries of permissible speech during the era of censorship, ensuring the offline spread of reports by exile-run news websites, among other banned content. Ethnic minority groups—of which official statistics count more than 130, not including an estimated 800,000 population of Rohingya who are denied citizenship under Burmese law—have also used the internet to promote a multi-ethnic Burma in the past.

Troublingly, the newly liberalized online space shows signs of disconnecting from this pluralistic vision, in part because poor infrastructure and connections discourage consumers from seeking out diverse sources of information, but also because the lifted restrictions allowed for an outpouring of hate speech directed at the Muslim minority. In the past year, social media played an undisputed role in amplifying racial and religious tensions—further stoked by some state institutions and

[8] Transparency International, "Corruption by Country/Territory: Myanmar," December 2012, http://www.transparency.org/country#MMR.
[9] "ASEAN Gambles on Myanmar's Regional Leadership," Reuters, November 17, 2011, http://www.reuters.com/article/2011/11/17/us-myanmar-idUSTRE7AG0QQ20111117.

mainstream news websites—between them and the majority Buddhist groups in western Arakan state.[10] Over 100 people were killed and 120,000 people, mostly Rohingya, internally displaced in the violence that resulted;[11] more than 40 were reported dead after similar riots broke out in the heartland township of Meiktila in March 2013.[12] Deadly riots were subsequently documented in the central town of Okkan and Lashio in northern Shan state in April and May.[13]

Other post-censorship phenomena included a parliamentary hunt for an anonymous blogger who criticized a new law that defies the constitution. Cyberattacks on Burmese news websites also appear to be on the rise. Several media practitioners reported hackers attempting to compromise their personal email accounts in late 2012 and early 2013, prompting open debate about the alleged involvement of the military, which a government spokesperson denied.[14] It is too soon to cast this as a negative trend. However, those in Burma who have undergone decades of information control and strict punishment for forbidden expression, and minority communities who fear further marginalization from the dominant national discourse, remain cautious. Some distance still needs to be covered before they enjoy full freedoms online.

OBSTACLES TO ACCESS

Besides a state monopoly of telecommunications companies, the lack of a legal framework, poor infrastructure and widespread poverty limit Burmese citizens' internet access and usage. Over the past three years, the number of internet users has notably increased, though it remains only a fraction of the population. The International Telecommunication Union (ITU) estimated internet penetration at 1 percent in 2012.[15] This seems surprisingly low, although the precise scale of usage is notoriously difficult to ascertain in Burma, where independent surveys are not available and government statistics historically lack credibility. Nevertheless, government sources and a Burmese telecommunications expert interviewed for this report estimated one million internet users in the country in 2012,[16] putting penetration closer to 2 percent. One 2012 news report put the number of broadband Internet users at 150,000;[17] the ITU estimated just 5,400 in its 2012 survey.[18]

---

[10] Arakan was renamed Rakhine when Burma became Myanmar. "UN Says Over 26,000 Displaced by Myanmar Unrest," Agence France-Presse via *ReliefWeb*, October 28, 2012, http://bit.ly/1hfKXrJ.
[11] "Myanmar Riots Stoke Fears of Widening Sectarian Violence," Reuters, March 22, 2013, http://www.reuters.com/article/2013/03/22/us-myanmar-unrest-meikhtila-idUSBRE92L04G20130322.
[12] "Burma: State of Emergency Imposed in Meiktila," BBC, March 22, 2013, http://www.bbc.co.uk/news/world-asia-21894339; "Seven Muslims jailed over violence in Burma's Meiktila, "BBC, May 21, 2013, http://bbc.in/12IQ7rD.
[13] Yadana Htun, "Myanmar Anti-Muslim Violence Injures At Least 10 In Okkan As Mosques, Homes Attacked," The Associated Press, via *Huffington Post,* April 30, 2013, http://www.huffingtonpost.com/2013/04/30/myanmar-anti-muslim-violence_n_3185932.html; Zunetta, "Violence in Lashio," Partners Asia (blog), May 31, 2013, http://bit.ly/16awgos
[14] "State-Sponsored Attack Warning of the Google does not Need to Cause Excessive Concern, Says Government Spokesman" (in Burmese), *Popular News*, February 11, 2013.
[15] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[16] "Sky Net Internet Installation Cost Reduced" (in Burmese), *Popular News*, January 26, 2013.
[17] "Mobile Internet Users Experience Slow Connection," *Eleven Media News*, November 23, 2012, http://elevenmyanmar.com/national/science-tech/1426-mobile-internet-users-experience-slow-connection.
[18] International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2012."

The Ministry of Communications and Information Technology (MCIT) retains control over the country's international connection to the internet through two main internet service providers,[19] the state-owned Myanmar Post Telecommunication (MPT) and the military-linked Yatanarpon Teleport (YTP). Private internet connections are prohibitively expensive, though there is significant regional variation. The one-time installation cost of broadband access ranged from $530 to $588 in early 2012, down from $625 the previous year, depending on speed and connection method.[20] Monthly fees vary from $30 for 512Kbps to $155 for 3Mpbs.[21] MPT and YTP also offer ADSL service via landline, and dramatically lowered installation costs in late 2012.[22] YTP reduced them from $588 to $117, while MPT's went down from $588 to $58. For comparison, the private company Redlink charges about $500 for installation and monthly fees from$30 to US$130 for its popular Wi-Fi service, according to its data plan. However, since Burma's gross domestic product was just $848 per capita in 2012, these costs keep personal internet access far out of reach for the majority.[23]

More people can access the internet via mobile phone. Government sources reported 5.4 million mobile phone subscribers in Burma at the end of December 2012, a significant jump from the 2.8 million mobile subscribers Freedom House documented in February 2012;[24] the ITU agreed and estimated penetration at 11 percent. One November 2012 news report estimated the number of mobile internet users at over 200,000.[25] Meanwhile, once-essential cybercafés are receiving fewer visitors as personal connections proliferate.[26]

MPT controls the mobile phone market, but grants distribution rights to a select set of trusted companies, either military-linked—like YTP—or privately owned but closely linked to the government—like Elite, a subsidiary of Htoo Trading Company owned by tycoon Tay Za, who the U.S. government has long sanctioned from trading with American companies for his association with the junta.[27] Smaller firms seeking retail vending rights must purchase equipment from these

[19] Many still refer to the Ministry, formerly responsible for Communications, Posts and Telegraphs, by its old abbreviation MCPT.
[20] Interview with telecommunication company employees, January 2013.
[21] "WiMax Reduced Internet Installation Price from 630,00 Kyats to 450,000 Kyats Since December 6" (in Burmese), *Eleven Media News,* , December 5, 2012, http://news-eleven.com/local/16670-wimax.
[22] MCIT, Republic of the Union of Myanmar, "Telecommunication Operator Tender Evaluation and Selection Committee Nay Pyi Taw," accessed May 2013, http://www.mcit.gov.mm/sites/default/files/Expression_of_Interest.pdf.
[23] International Monetary Fund, "World Economic Outlook Database," October 2012, http://www.imf.org/external/pubs/ft/weo/2012/02/weodata/weorept.aspx?pr.x=84&pr.y=11&sy=2010&ey=2017&scsm=1&ssd=1&sort=country&ds=.&br=1&c=518&s=NGDPDPC%2CPPPPC&grp=0&a=.
[24] "Digicel Goes after Myanmar," *Guardian Media* (Port-of-Spain), February 3, 2013, http://guardian.co.tt/business/2013-02-02/digicel-goes-after-myanmar; "Myanmar Sets 2015 Goal for Teledensity," *Myanmar Times*, January 16, 2013, http://www.mmtimes.com/index.php/business/technology/3790-myanmar-sets-2015-goal-for-teledensity.html. An independent observer estimates that there are just over three million mobile phone users. See "Footsteps of 2012" (in Burmese), *Internet Journal*, January 1, 2013, http://myanmarinternetjournal.com/ij/article/6275-2013-01-02-09-02-46.
[25] "Mobile Internet Users Experience Slow Connection," *Eleven Media News*, November 23, 2012, http://elevenmyanmar.com/national/science-tech/1426-mobile-internet-users-experience-slow-connection.
[26] Interviews with three cybercafé proprietors in Rangoon and two in Naypyidaw, and nine mobile phone users in Rangoon and Mandalay, January 2013. See also, "Cyber Cafes do not Receive Internet Users as Before, and Asked for Price Reduction" (in Burmese), *Popular News*, August 11, 2012.
[27] Erika Kinetz and Matthew Pennington, "AP Impact: Myanmar Sanctions List Languishes," Associated Press, May 18, 2013, http://bigstory.ap.org/article/ap-impact-myanmar-sanctions-list-languishes-0.

larger distributors and are generally unable to offer consumers lower prices than the ones mandated by those at the top of the chain.

The retail mobile market has become more dynamic to meet rising demand,[28] but poor service has limited the expansion of mobile internet, even after some ambitious public initiatives. In 2011, the government announced a project to expand the number of mobile phone lines almost six-fold—to 30 million—over the next five years. In January 2012, private company Shwe Pyi Ta Khun announced it was seeking permission from the President's Office to sell a SIM card for 5,000 kyat ($6) as part of the president's poverty reduction initiative, to widespread acclaim. Within a week, however, officials rejected the proposal. Authorities subsequently pressured companies to chop the price of a SIM card from 500,000 kyats ($625) to 200,000-250,000 kyats ($250-312). But the supply of new cards could not meet consumer demand, while the continuing poor quality of service disappointed users, according to news reports and Freedom House interviews. In many cases mobile internet barely functions, even in major cities.

In March 2013, facing mounting public pressure, President Thein Sein pledged that the government would price SIM cards at 1,500 kyat ($2) starting in April. Though a welcome development, the distribution of the new cards was a gift to corrupt officials and black market racketeers. Rather than make them available through service providers, users were directed to local government offices, where they were asked to submit household registration, ID, and two photos. The application was not for a SIM card, but for the opportunity to enter a draw for the chance to buy one of the 350,000 circulated nationwide.

Events in the Rangoon Division are probably representative of what happened next around the country. Having received a quota of 119,000 cards, local officials promptly reserved a quarter for themselves and their staff before allocating the rest to different townships. In one neighborhood, over 2,500 applicants competed for 114 cards that were soon being resold for 60,000 kyats ($666) to 90,000 kyats ($1000), despite numerous reports of unreliable, substandard service. The government issued a second round of 1,500 kyat cards using the same system in May.

Another major drawback of the SIM cards is that they used an outdated CDMA 800 MHz network launched in 1999, rather than the GSM system that is more common worldwide, even though GSM has been available in Burma since 2002 and is considerably more popular.[29] Sources interviewed for this report told Freedom House that the CDMA network is owned by the military conglomerate Myanmar Economic Cooperation (MEC), which sold the SIM cards cheaply for public use because the CDMA network is no longer useful for the military. The deal benefits Chinese companies selling CDMA-capable handsets. The best-selling mobile handset in 2012 was one developed by

[28] "Mobile Phone Accessory Shops Increase" (in Burmese), *7Days News*, January 25, 2013, http://www.7daynewsjournal.com/article/9515.

[29] December 2012 figures showed 4 million subscribers on the GSM network, and 1 million on two CDMA networks, 800MHz and 450 MHz. An additional 0.7 million subscribed to 3G services on the WCDMA network launched in 2008. In December 2012, the Ministry launched a joint "One Million Phone Lines" project with Chinese telecommunication companies to introduce 3G network-capable GSM and WCDMA phones in five cities. See, MCIT, "Telecommunication Operator Tender Evaluation."

Chinese technology giant Huawei, which at 100,000 kyats ($117), was still beyond the reach of most Burmese, according to local market researchers.

In July 2012, the government announced plans to liberalize its telecom sector and invite foreign investment.[30] A senior official said that a total of four operating licenses would be granted—two for Burmese companies and two for foreign firms, incorporating 4G services as early as 2013. The plan proposed privatizing MPT to form the Myanmar Telecoms Company, which would be awarded one of the cellphone licenses. Another would go to YTP, though other companies were reportedly applying,[31] possibly for joint ventures. Critics raised concerns about possible conflicts of interest in the tender process for domestic licenses.

In June 2013, the government awarded the international licenses Norway's Telenor and Qatar Telecom, allowing them to offer services and infrastructure alongside local firms.[32] However, as the coverage period of this report ended, the legislature has not enacted a telecommunications law governing their operation.[33] Critics of a draft from early 2013 noted repressive prohibitions of anti-state content and social media use, and that it may require intermediary service and content providers to cooperate with state surveillance to detect violators.[34] Human Rights Watch warned international telecommunications companies that there is a risk of complicity in human rights abuses if they enter the Burmese market before adequate protections are in place.

In the meantime, foreign investment in telecommunications was less than $6 million per year in early 2012.[35] According to official data, there are currently 14,000 kilometers of fiber in Burma and around 1,800 towers, leaving an estimated 15,000 towers and hundreds of thousands of kilometers of fiber to make up the difference required to meet the government's expansion objectives. Experts estimate the total cost involved would be closer to $4 billion.

The government—though unable to meet demand for existing services—announced two additional projects during the coverage period for this report. The first was an installment plan to offset the cost of mobile telephones in rural areas begun in October 2012, which requires a 40,000 kyats ($47) down payment followed by 10,000 kyats ($11) per month.[36] Critics said the plan disguises the high cost of the phones—which comes to a total of 150,000 kyats ($176)—rather than bringing

[30] Martin Petty, "Insight: Disconnected for Decades, Myanmar Poised for Telecoms Boom," Reuters, September 13, 2012, http://in.reuters.com/article/2012/09/13/us-myanmar-telecoms-idINBRE88C03K20120913.
[31] "Elite Tech Plans to Apply for Private Telecommunications Operator" (in Burmese), *7Days News*, September 29, 2012, http://www.7daynewsjournal.com/article/7792.
[32] Shibani Mahtani and Chun Han Wong, "Norway's Telenor, Qatar Telecom Get Myanmar Telecom Licenses," *Wall Street Journal,* June 27, 2013, http://online.wsj.com/article/BT-CO-20130627-703302.html.
[33] "Japan and Singapore Technology Firms Invest in Burma" (in Burmese), *7Days News*, December 27, 2012, http://www.7daynewsjournal.com/article/9090; "Those Firms which Want to Invest in Burma Waiting for Telecommunications Law" (in Burmese), *7Days News*, December 8, 2012, http://www.7daynewsjournal.com/article/8763.
[34] Human Rights Watch, "Reforming Telecommunications in Burma," May 19, 2013, http://www.hrw.org/reports/2013/05/19/reforming-telecommunications-burma.
[35] "Myanmar (Burma) - Telecoms, Mobile and Internet," BuddeComm, accessed January 2, 2012, http://www.budde.com.au/Research/Myanmar-Burma-Telecoms-Mobile-and-Internet.html.
[36] "Huawei Ranks Bestselling Hand-set in 2012" (in Burmese), *7Days News*, December 26, 2012 http://www.7daynewsjournal.com/article/9089.

it down.[37] The second project involved SIM cards for foreign visitors during the Southeast Asia Games, which Burma is scheduled to host in December 2013. According to a senior government official, the temporary SIM card will be sold to non-Burmese citizens for $15, some 12 times cheaper than the price paid by most locals. The information ministry also announced that it will increase internet connection speeds in time for the Games. Chinese firms will reportedly provide technical support for this upgrade and broader ICT security efforts.[38] Huawei, for example, donated three million dollars' worth of video conferencing equipment to organizers of the Games in late 2012.[39]

Though limits on content have declined dramatically in the past two years, the state's links with telecommunications companies mean it is still inclined to restrict ICT access when profits are at risk. In October 2012, the government announced that it would sever internet connections detected making international calls via Voice over Internet Protocol (VoIP).[40] International VoIP calls made via applications such as Skype, Gtalk, Pfingo, VBuzzer, and VZO were banned under a government directive in March 2011, which prescribed penalties ranging from fines or confiscation of property to five years' imprisonment. The measure was apparently aimed at protecting revenue earned from international phone calls made over the network of the state-owned telecom,[41] or via a new government-sponsored VoIP program called Ytalk launched in late 2011.[42] The directive, however, is not effectively enforced.

The Posts and Telecommunications Department regulates Burma's telecommunications industry under the MCIT. While there are several other state institutions tasked with ICT development and management, they are either not very active or exist only on paper.[43] Under the junta, the MCIT and intelligence agencies implemented arbitrary and ad hoc censorship decisions. Under the more civilian government, however, the MCIT has demonstrated more authority on telecommunications issues.

In early January 2013, Minister of Information and Telecommunications Thein Tun was fired for alleged corruption, in the first anti-graft probe under the new government to target a cabinet minister.[44] The minister, who had blocked efforts to reduce the price of SIM cards in favor of his own initiative to sell four million cards at $220 a pop, is now under house arrest; the investigation,

---

[37] Author's interview with three local journalists who cover IT news, January 2013.
[38] "China Supports Burmese Internet Security" (in Burmese), *Popular Journal*, accessed January 8, 2012, http://popularmyanmar.com/mpaper/archives/33163.
[39] "Huawei Helps US$3 Million for Video Conference System in 2013 SEA Games" (in Burmese), *7Days News*, September 26, 2012, http://www.7daynewsjournal.com/article/7790.
[40] "Phone Lines that Make Illegal Calls to Foreign Countries Will be Cut" (in Burmese), *Internet Journal*, October 20, 2012 http://myanmarinternetjournal.com/mobile/mobile-news/5337-2012-10-15-09-52-34.
[41] Aung Myat Soe, "Government Bans Internet Overseas Calls," *Mizzima*, March 16, 2011, http://mizzimaenglish.blogspot.com/2011/03/government-bans-internet-overseas-calls.html.
[42] Author's interviews with two Burmese IT experts and four local journalists, June 2012.
[43] These include the Myanmar Computer Science Development Council, the e-National Task Force, the Myanmar Computer Federation, the Myanmar Computer Professionals' Association, the Myanmar Computer Industry Association, and the Myanmar Computer Enthusiasts' Association.
[44] "Myanmar Ex-Telecoms Minister Faces Graft Probe," The Associated Press, January 24, 2013, http://bigstory.ap.org/article/myanmar-ex-telecoms-minister-faces-graft-probe.

which is also looking into handsets produced by Huawei and ZTE, is ongoing.[45] The investigation overshadowed the reforms in the telecommunications sector, but also signaled a possible turning point. Many observers expressed hopes of fairer pricing and a lifting of the VoIP ban in the aftermath of the minister's removal.[46] In a reminder that the military still has an overwhelming influence in government, however, Thein Sein tapped Myat Hein, commander-in-chief of the air force, to replace him in February 2013.[47]

LIMITS ON CONTENT

On August 20, 2012, the government lifted the systematic state censorship of traditional and electronic media prior to publication that had been in place for nearly five decades. Political content appeared to be almost universally available, and even social content, such as pornography, was not blocked in mid-2013. Troublingly, however, draft legislation maintains that may even intensify limits on content outlined in existing laws. What's more, the transformation had some unforeseen effects, as simmering distrust between Burma's ethnic groups found expression on social media, and particularly targeted the Rohingya, whom commentators of all stripes characterized as "dogs, thieves, terrorists and various expletives."[48] Though other online activism was more positive, the role of ICTs in fermenting violence that affected over a hundred thousand people—and sent ripples through sympathetic Muslim communities across Asia—cast a shadow over the newly open internet landscape.

For years, the Burmese government had systematically restricted access to political content online, but in September 2011 they lifted blocks on foreign news sources and major exile media sites; the latter had long been on the regime's blacklist for their critical reporting.[49] The websites of international human rights groups were also unblocked. In tests conducted by OpenNet Initiative on YTP in August 2012, only 5 out of 541 URLs categorized as political content were blocked. When Freedom House conducted its own tests in December, almost all previously banned websites, including those five, were accessible.[50] By mid-2013, even sites hosting previously-filtered social content about pornography or drugs, were no longer blocked.

[45] "Ex-Minister Under House Arrest," Radio Free Asia, January 23, 2013, http://www.rfa.org/english/news/burma/phone-01232013152301.html.
[46] Telephone interviews with a senior Ministry of Information and Telecommunications official and a key telecommunications investor, January 2013. See also, "Expectation on Better Telecoms Service Grows as Minister Resigns" (in Burmese), *7Days News*, January 17, 2013, http://www.7daynewsjournal.com/article/9403.
[47] Nyein Nyein, "Former Generals to Run Burma's Telecoms, Border Affairs Ministries," *Irrawaddy*, February 14, 2013, http://www.irrawaddy.org/archives/26820.
[48] "Internet Unshackled, Burmese Aim Venom at Ethnic Minority," *New York Times*, June 16, 2012, http://www.nytimes.com/2012/06/16/world/asia/new-freedom-in-myanmar-lets-burmese-air-venom-toward-rohingya-muslim-group.html?_r=0.
[49] The Associated Press, "Myanmar Authorities Unblock Some Banned Websites," *Yahoo News*, September 16, 2011, http://news.yahoo.com/myanmar-authorities-unblock-banned-websites-050311492.html; Qichen Zhang, "Burma's Government Unblocks Foreign Websites Including YouTube," OpenNet Initiative, September 20, 2011, http://opennet.net/blog/2011/09/burmas-government-unblocks-foreign-websites-including-youtube.
[50] One of the URLs listed as blocked by ONI, http://www.niknayman-niknayman.co.cc, was not found in or outside Burma.

Despite these notable positive developments, the impact of the new opening has been tempered by an atmosphere of uncertainty. In particular, harsh laws governing content remain in effect pending the passage of replacements to repeal them, which some observers say could be even stricter. The draft telecommunications bill that will regulate service providers also contains content restrictions, at least in early drafts, according to news reports. A report published in November 2012 noted that one of the law's new articles appeared to ban social media use entirely, though whether that was the intent or how it might be implemented is not known.[51] Human Rights Watch reported that a draft it reviewed includes ill-defined bans on "indecent" and "undesirable" content that are open to abuse.[52] Journalists also objected to another draft law governing the print media for introducing the kind of censorship familiar from its repressive predecessor, including bans on criticism of the constitution; the implications for online news outlets remain unclear.[53] Civil society groups objected to both drafts, and their passage was consequently delayed beyond the coverage period of this report. Observers noted that although government consultations with different stakeholders regarding the law were far from perfect, they were better than in the past.

Threats remain effective tools to force intermediaries to delete content; however, the extent of this practice and its impact on the information environment as a whole is hard to measure. Self-censorship remains common online, though topics considered off-limits have changed. In particular, internet users have been reluctant to raise human rights abuses committed in the past under the junta, for fear of jeopardizing the political opening. Objective coverage of the Rohingya, let alone defense of the persecuted minority, has become taboo, and news outlets that continue to provide it are accused of anti-Burmese bias.[54]

As limits on content are lifting, ministries and political groups have used ICTs to challenge the opposition, rather than blocking them. Several ministries, including the Ministry of Information, have their own websites and blogs. Other blogs, such as *Myanmar Express* and *OppositEye*, were more manipulative, launching smear campaigns against the opposition and Aung San Suu Kyi.

As in 2011, social media tools gained prominence in 2012 and 2013, including Facebook, Twitter, Friendfinder, Netlog, and Google+. Facebook is the most popular, since many users developed the habit of using the platform to share information, initiate collective action on social and political issues, or follow exile media outlets when website blocking was still pervasive. Although no precise statistics are available on the number of Facebook users in Burma, one expert estimated that 80 percent of the country's internet users had a Facebook account in 2011.[55] For some users frustrated at the challenge of navigating between sites on poor connections, Facebook is the sole source of online news.

---

[51] "Myanmar Bans Social Media Use Under Telecoms Bill," *Eleven Media News,* November 12, 2012, http://elevenmyanmar.com/politics/1280-myanmar-bans-social-media-use-under-telecoms-bill.
[52] Human Rights Watch, "Reforming Telecommunications in Burma,"
[53] Committee to Protect Journalists, "Draft Media Law a Step Backward for Burma," news alert, March 1, 2013, http://www.cpj.org/2013/03/draft-media-law-a-step-backward-for-burma.php.
[54] Asia Sentinel, "Burma's Irresponsible New Media," *Irrawaddy,* July 11, 2013, http://www.irrawaddy.org/archives/8862.
[55] Based on an estimated 500,000 internet users in Burma. Tun Tun, "Facebook's Mini-Revolution in Burma," *Mizzima*, August 17, 2011, http://www.mizzima.com/edop/features/5786-facebooks-mini-revolution-in-burma.html.

Unfortunately, hate groups and manipulative photos and messages are also common on Facebook, and Burmese internet users spread racially-charged comments across social media platforms throughout the coverage period.[56] Several promoted violence, including a self-designated "beheading gang" that targeted Muslims on Facebook, which the platform later removed from the site.[57] The hatred expressed online and in government statements in the media proved mutually reinforcing.[58] In 2012, religious riots broke out in western Arakan state sparked by state and private media reports that treated the rape and murder of a local woman as a racially-motivated crime,[59] and contrasted the Arakan Buddhist victim with her allegedly Muslim attackers.[60] Propaganda photos and posts from both sides of the conflict circulated on the internet.[61] A senior official from the president's office framed the issue as a matter of national security on his personal Facebook page and urged people to rally behind the armed forces.[62] Since the riots took place in a remote area challenging for journalists to reach, these Facebook updates were disproportionately influential in media reports.[63] The anti-Rohingya rhetoric sparked counter-protests overseas, including one coordinated by hacktivist group Anonymous, which sent 24,000 messages per hour with the hashtag #RohingyaNOW one day in March 2013.[64]

Other online activism was more positive. In 2012, villagers, Buddhist monks, and citizen journalists united on Facebook to mobilize against a copper mine in the central Letpaudaung hills, run by the military-owned conglomerate Union of Myanmar Economic Holdings Limited and China's Wanbao Mining Limited, a subsidiary of the arms manufacturer NORINCO. Initially, politicians and traditional media largely ignored the protesters, who called for a halt to the project citing environmental, social and health concerns. However, on November 29, 2012, riot police raided six protest camps at the mine, detained several dozen protesters, and injured at least 100 Buddhist monks and villagers, many of whom incurred severe burns. Activists used Facebook extensively to post photos and information about the crackdown, triggering an outcry from the media and the political opposition. Recognition, however, was the only substantive outcome of the action. President Thein Sein appointed Aung San Suu Kyi to chair an Investigation Commission. However, the Commission recommended that the mining project go ahead in March 2013.[65]

---

[56] Sait Latt, "Intolerance, Islam and the Internet in Burma today," *New Mandala*, June 10, 2012, http://asiapacific.anu.edu.au/newmandala/2012/06/10/intolerance-islam-and-the-internet-in-burma-today/.

[57] Min Zin, "Why Sectarian Conflict in Burma is Bad for Democracy," *Transitions* (blog)*, Foreign Policy,* June 13, 2012, http://transitions.foreignpolicy.com/posts/2012/06/13/winners_and_losers_from_the_conflict_in_arakan.

[58] *New Light of Myanmar,* a state newspaper, printed a government statement that included the racial epithet *kalar*, a derogatory term for foreigners of Indian appearance, when referring to the Muslim victims of mob violence. It corrected the reference to "Islamic residents" the following day, but did not apologize. See, Hanna Hindstrom, "State Media Issues Correction After Publishing Racial Slur," *Democratic Voice of Burma*, June 6, 2012, http://www.dvb.no/news/state-media-issues-correction-after-publishing-racial-slur/22328.

[59] "Burma's Irresponsible Media," *Irrawaddy*, July 11, 2012, http://www.irrawaddy.org/archives/8862.

[60] On June 3, 10 Muslims were killed in the same region in apparent retaliation for the murder of the Buddhist girl.

[61] "Media Freedom Still Murky in Myanmar Despite Progress," *Global Voices*, February 21, 2013, http://globalvoicesonline.org/2013/02/21/myanmar-media-freedom-still-under-threat/.

[62] Min Zin, "Why Sectarian Conflict in Burma is Bad for Democracy."

[63] Hmuu Zaw's Facebook page, accessed on August 2013, https://www.facebook.com/hmuu.zaw.

[64] "Anonymous Taught Twitter About the Rohingya Genocide," *Vice*, March 26, 2013, http://www.vice.com/read/anonymous-taught-twitter-about-the-rohingya-genocide.

[65] Kyaw Phyo Tha, "Wanbao Welcomes Inquiry Commission's Verdict," *Irrawaddy*, March 13, 2013, http://www.irrawaddy.org/archives/29255.

Besides employing online tools for social and political mobilization, users have organized gatherings, with government permission, to share general ICT-related knowledge. In January 2013, Burma's fourth BarCamp—a user-generated conference about technology and the internet—was held in Rangoon with over 6,000 participants.[66] BarCamp meetings were also held in cities like Mandalay and Bassein.

VIOLATIONS OF USER RIGHTS

Given Burma's appalling history of violating user rights, late 2012 and early 2013 were comparatively neutral periods as citizens awaited the results of sluggish legislative reforms. Users remain at risk of prosecution and imprisonment under the repressive laws enacted by the junta, and in a troubling May 2013 analysis, Human Rights Watch noted that an early draft of the telecommunications law retained the Electronic Transactions Law's repressive section 33 without change. Bloggers are not immune from legal threats, and a parliamentary committee wasted valuable time and resources trying to identify an anonymous blogger who had criticized their conflict with a constitutional court. Yet no new arrests were reported, and the only ICT-related imprisonments on record involve former officials accused of leaking secrets.

The current constitution, drafted by the military-led government and approved in a flawed 2008 referendum, does not guarantee internet freedom. It simply states that every citizen may exercise the right to "express and publish their convictions and opinions," but only if these are "not contrary to the laws enacted for Union [of Myanmar] security, prevalence of law and order, community peace and tranquility or public order and morality."[67] Three other laws govern ICTs: the 1996 Computer Science Development Law, the 2002 Wide Area Network Order, and the 2004 Electronic Transactions Law (ETL).[68] Of the three, the ETL is the most notorious and frequently used. Under section 33, internet users face prison terms of 7 to 15 years and possible fines for "any act detrimental to" state security, law and order, community peace and tranquility, national solidarity, the national economy, or national culture—including "receiving or sending" related information.[69] In 2011, state-run media warned that the ETL could apply to defamatory statements made on Facebook.[70]

Draft laws to reform this legislative framework were expected to pass in 2013,[71] but their status at the end of the coverage period remained unclear. Traditional media censorship was still authorized in theory by the Printers and Publishers Registration Act of 1962, even though the board that

[66] "BurmaCamp Rangoon: Over 6,000 Participants" (in Burmese), *Myanmar Times*, January 23, 2013, http://myanmar.mmtimes.com/index.php/technology/3334-2013-01-23-10-37-23.html.
[67] "Constitution of the Republic of the Union of Myanmar (2008) – English," available *Online Burma/Myanmar Library,* http://www.burmalibrary.org/show.php?cat=1140.
[68] "List of Burma/Myanmar laws 1988-2004 (by date)," available *Online Burma/Myanmar Library,* http://www.burmalibrary.org/show.php?cat=1729.
[69] "Electronic Transactions Law, State Peace and Development Council Law No. 5/2004," available *United Nations Public Administration Network,* http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan041197.pdf.
[70] Francis Wade, "Prison Threat for Facebook 'Defamers'," *Democratic Voice of Burma*, August 3, 2011, http://www.dvb.no/news/prison-threat-for-facebook-'defamers'/16865.
[71] Interview with a senior government advisor, January 2013.

enforced it was dismantled. Though new legislation that would repeal this law was passed in the lower house of parliament in July 2013, it stalled in the upper house. Critics point out it retains vaguely worded content controls and potentially punitive licensing for news outlets,[72] even though many lawmakers believed these had been removed following consultations with journalists.[73] Similarly, the draft telecommunications law, which corresponds most closely to the ETL, reproduced that law's repressive section 33 verbatim, according to a review of one draft by Human Rights Watch.[74] Officials told Human Rights Watch that many repressive measures were missing from a subsequent draft, but this has not been made public.[75]

While potential penalties for ICT use still exist, no arrests were reported during the coverage period. At least three former military or government officials remain imprisoned after they were sentenced in early 2010 for leaking sensitive information about junta activities to overseas groups via the internet.[76] Dozens of political prisoners formerly jailed for electronic activities remain free since they were released en masse in 2011. In general, however, these releases came with a condition that reoffenders will receive a new sentence in addition to previously unfinished sentences.

Although limits on content have loosened, content producers continue to face legal investigations for publishing online. Two print newspapers with websites, the *Voice Weekly* and *Modern Journey*, were sued for libel in 2012 for reports they said were in the public interest.[77] In another notorious example, a member of the military-backed ruling party urged parliament to uncover the identity of pseudonymous blogger, "Dr. Seik Phwar," following a January 14, 2013 post titled, "Is Parliament Above The Law?"[78] The article questioned parliament's decision to amend a law governing a nine-member, presidentially-appointed constitutional tribunal with power to overrule the government. The amendment, which Thein Sein adopted on January 22 under pressure from parliamentarians, gives them the right to challenge the tribunal's rulings, even though its authority is outlined in article 324 of the 2008 constitution.[79] On February 8, a 17-member parliamentary committee was established to uncover the blogger's identity, though when it announced its findings in July it did

[72] Simon Roughneen, "Burma's Press Council Threatens Resignation Over Media Rules," July 18, 2013, http://www.irrawaddy.org/archives/39522.
[73] "Bad News: New Freedoms Under Threat," *Economist,* August 17, 2013, http://www.economist.com/news/asia/21583700-new-freedoms-under-threat-bad-news.
[74] Human Rights Watch, "Reforming Telecommunications in Burma,"
[75] In August 2013, outside the coverage period of this report, a state news report said a bill amending the ETL submitted to parliament proposed more lenient sentences.
[76] In January 2010, a former military officer and a foreign affairs official were sentenced to death, and another foreign affairs official was sentenced to 15 years in prison, for leaking information and photographs about military tunnels and a general's trip to North Korea. Interview with Bo Kyi, cofounder of the Association for Assisting Political Prisoners (Burma), July 2012. The executions have not been carried out.
[77] "Burmese Editor and Publisher Charged with Libel," BBC, September 20, 2012, http://www.bbc.co.uk/news/world-asia-19659294; Phanida, "Gov't Construction Engineer Sues Modern Journal," *Mizzima,* March 7, 2012, http://www.mizzima.com/news/inside-burma/6721-govt-construction-engineer-sues-modern-journal.html.
[78] Oliver Spencer, "Myanmar: Dr Seik's Famous Blog Post being Investigated by Parliament (in English)," Article 19, February 13, 2013, http://www.article19.org/join-the-debate.php/91/view/; Saw Zin Nyi, "Naypyitaw Investigates the Mysterious Case of 'Dr. Seik Phwar,'" *Mizzima*, March 5, 2013, http://www.mizzima.com/news/inside-burma/9003-naypyitaw-investigates-the-mysterious-case-of-dr-seik-phwar.html.
[79] "Burmese MPs Force Out Constitutional Court Judges," BBC, September 6, 2012, http://www.bbc.co.uk/news/world-asia-19498968.

not appear to have succeeded.[80] The case was further complicated by the blogger's unclear political affiliation, since Seik Phwar had criticized both Aung San Suu Kyi and Thein Sein alike since 2011, and many observers believe he is influenced by anti-reformist military hardliners. Some of his articles were reproduced in the journal *Smart News*, which is published by the information ministry.

How the new environment might transform state surveillance, which has historically been pervasive and politicized, is not known. Experts interviewed for this report said there are no funds or interest in developing nationwide technical surveillance at present, though activists are still monitored.

The junta is believed to have carried out cyberattacks against opposition websites in the past. These attacks increased in February 2013 when many journalists and academics, including the author of this report, received Google's notification of state-sponsored attempts to infiltrate personal accounts on its e-mail service, Gmail;[81] officials denied responsibility.[82] Some recipients speculated the attackers had military support.[83]

[80] "Parliamentary Commission Fails to Expose Defamatory Blogger," *Eleven Media News,* July 2, 2013, http://elevenmyanmar.com/national/2656-parliamentary-commission-fails-to-expose-defamatory-blogger.
[81] Thomas Fuller, "E-Mails of Reporters in Myanmar Are Hacked," *New York Times*, January 10, 2013, http://www.nytimes.com/2013/02/11/world/asia/journalists-e-mail-accounts-targeted-in-myanmar.html?_r=3&; Shawn Crispin, "As Censorship Wanes, Cyberattacks Rise in Burma," *CPJ Internet Channel*, February 11, 2013, http://www.cpj.org/internet/2013/02/as-censorship-wanes-cyberattacks-rise-in-burma.php.
[82] The Associated Press, "Myanmar Denies Hacking Journalist Email Accounts," February 11, 2013, http://bigstory.ap.org/article/myanmar-denies-hacking-journalist-email-accounts.
[83] IT experts and journalists interviewed in 2012 and 2013 noted that those who previously received ICT trainings in Russia and other countries could still be playing a role in launching cyberattacks against opposition websites and journalists.

CAMBODIA

	2012	2013
INTERNET FREEDOM STATUS	N/A	PARTLY FREE
Obstacles to Access (0-25)	n/a	14
Limits on Content (0-35)	n/a	15
Violations of User Rights (0-40)	n/a	18
Total (0-100)	**n/a**	**47**

* 0=most free, 100=least free

POPULATION: 15 million
INTERNET PENETRATION 2012: 5 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- In May 2012, the government announced it was in the process of drafting Cambodia's first ever cybercrime law, which netizens fear could extend traditional media restrictions online (see **VIOLATIONS OF USER RIGHTS**).
- At least three antigovernment blogs remain inaccessible on most ISPs, after an apparent government ban in 2011, implemented without transparency, (see **LIMITS ON CONTENT**).
- In November 2012, the government told internet cafés near Phnom Penh schools to relocate or close, threatening access throughout the capital (see **OBSTACLES TO ACCESS**).

INTRODUCTION

New media and increased internet access are transforming the information environment in Cambodia, where press freedom is traditionally curtailed. Through the use of new media and digital tools, young activists of both genders are able to disseminate views on important social and political issues, including the country's besieged environmental resources. Social media websites are quickly becoming an integral tool for sharing information and opinion.

The Royal Government of Cambodia,[1] led by Prime Minister Hun Sen since 1998, restricts access to sexually explicit content but has yet to systematically censor online political discourse, leading some observers to hope Cambodia is entering an era of "digital democracy."[2]

Yet the tide may be turning. Authorities have begun to interfere with information and communications technology (ICT) access, blocking at least three blogs hosted overseas on multiple ISPs for content that criticized the government since 2011. In 2012, government ministries threatened to shutter internet cafes too near schools—citing moral concerns—and instituted surveillance of cafe premises and cell phone subscribers as a security measure that could foretell the emphasis of the country's first cybercrime law, which the government began drafting in May 2012. Online activists continued to raise public awareness around a number of causes such as the imprisonment of veteran journalist Mam Sonando, who was sentenced to 20 years imprisonment after documenting land seizures in 2012, then released on probation in 2013. Yet the very success of such campaigns may be spurring the leadership's efforts to curb internet freedom in the same way they do traditional media.

OBSTACLES TO ACCESS

The International Telecommunication Union reported internet penetration in Cambodia at just 5 percent in 2012.[3] Other estimates are higher: Cambodia's Ministry of Posts and Telecommunications (MPTC) reported 2.7 million Internet users in March 2013, around 18 percent of the population of around 15 million.[4]

The absence of an extensive landline network has historically restricted internet penetration, since the fixed landlines that broadband internet services depend on are often unavailable in rural areas. Wireless broadband, which emerged in 2006, has helped bridge the digital divide between rural and urban internet users.

---

[1] Cambodia is a constitutional monarchy. King Norodom Sihamoni succeeded his father as head of state in 2004.
[2] Sopheap Chak, "Digital Democracy Emerging in Cambodia," *UPI Asia Online*, November 11, 2009, http://bit.ly/1fyzWq3.
[3] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://bit.ly/14IlykM.
[4] Suy Heimkhemra, "Cheap Data, Better Tech Putting More Cambodians Online," Voice of America, March 25, 2013, http://www.voanews.com/content/cheap-data-better-tech-putting-more-cambodians-online/1628531.html. The consulting firm "We Are Social" put penetration at 16 percent in a late 2012 report. See, Simon Kemp, "Social Digital and Mobile in Cambodia," *We Are Social* (blog), November 7, 2012, http://wearesocial.net/blog/2012/11/social-digital-mobile-cambodia/.

There are at least 24 internet service providers (ISPs) operating in the Cambodian market—government accounts cite as many as 27[5]—and they offer competitive rates for high-speed internet, at around $12 a month.[6] Affordable smart phones, tablets and other devices have also contributed to the rise in the number of Cambodian internet and mobile users. About 98 percent of internet users today have mobile access, either via satellite networks or Wi-Fi connections, according to the MPTC. However, insufficient electricity supplies often result in nationwide blackouts—which impose constraints on computer and internet use.

Mobile phone users surpassed the number using fixed landlines surprisingly early in Cambodia, and have gained in popularity since 2000, even at the bottom of the economic pyramid, due to their affordability.[7] As of September 2012, mobile penetration was at 131 percent, because some people own more than one device.[8] The figures are the outcome of intense competition among 10 mobile service providers, who offer free SIM cards, affordable handsets and bonuses in their efforts to secure more market share. In April 2013, the MPTC attempted to pass a resolution banning all providers from offering these bonuses, apparently to protect companies with links to officials from losing out to their competitors, but backed down after a public outcry.[9]

Thanks to these low prices, mobile phones have become indispensable in Cambodia, preferred over traditional communications including landlines and the postal service. With poor transportation infrastructure and electricity coverage, mobile phones offer the most convenient access to a range of services including radio, music and video, and increasingly web access. Beyond that, mobile phones have had a great impact on mobilization and collective actions. In the run-up to the 2007 and 2013 elections, political parties used short-message service (SMS) text messaging as the cheapest and most effective way of spreading their message, while election monitoring groups also used SMS to gather data. With technical support from the Cambodian NGO Open Institute and the International Foundation for Electoral Systems, the Cambodian National Election Committee (NEC) launched a voice-based information service to provide pre-recorded details for voters, free of charge, in advance of the National Assembly election scheduled in July 2013.[10]

Language is another obstacle to access, since few online applications are coded in Khmer. Technology companies and ICT experts have made a significant investment to improve Cambodia's infrastructure, including the development of Khmer language applications. The Khmer Unicode font become widely available after the government recognized it as a standard in 2010.[11] After five

[5] O.U. Phannarith, Head of CamCERT and Permanent Member of Cybercrime Law, Working Group of National ICT Development Authority, "Cambodia Effort in Fighting Cybercime in the Absence of Law," slideshow presented at the Asia Pacific Regional Mock Court, Jakarta, Indonesia, September 18-19, 2012.
[6] "Cheap Data, Better Tech Putting More Cambodians Online," VOA News, March 25, 2013, http://bit.ly/109eoTm.
[7] Sopheap Chak, "Mobile Technology gives Cambodians a Voice," *UPI Asia Online*, 23 April 2010, http://bit.ly/a6vs0S.
[8] International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2012."
[9] Kaing Menghun and Joshua Wilwohl, "Ban on Generous Mobile Top-Up Offers Lifted," *Cambodia Daily*, May 7, 2013, http://www.cambodiadaily.com/archive/ban-on-generous-mobile-top-up-offers-lifted-22713/. See also, Menghun and Wilwohl, "Mobile Bonuses Axed after Firm Complaint," *Cambodia Daily*, May 2, 2013, http://bit.ly/16zRyyd.
[10] Open Institute, "IVR-based Information for the 2013 National Assembly Election Available," 18 March 2013, http://www.open.org.kh/en/node/528.
[11] Sebastian Strangio and Khouth Sophak Chakrya, "Unicode opens door for Khmer computing," May 2, 2008, http://www.phnompenhpost.com/special-reports/unicode-opens-door-khmer-computing.

years of collaboration by software developers, the release of Google's Khmer translation feature is anticipated by the end of 2013.[12] In addition, developers Sous Samak and Kim Sokphearum launched their own Automatic English-Khmer Translation System in March.[13] With these efforts, it is hoped that Khmer speaking netizens will be able to read non-Khmer content and vice versa, connecting Cambodian netizens to a wider audience.

The government welcomes and supports such technology and infrastructure developments. However, despite public claims to support freedom of expression by Information Minister Khieu Kanharith and others,[14] officials have taken steps to interfere in internet access. In early 2010 the government planned to introduce a state-run exchange to control all local ISPs with the declared aim of strengthening internet security against pornography, theft and cybercrime.[15] This plan, however, has been postponed due to popular opposition—even from inside the government.[16]

There is no independent regulatory body overseeing the digital landscape in Cambodia, and controls are implemented through ad hoc internal circulars.[17] In early November 2012, a government circular called for the relocation of all internet cafés within a 500-meter radius of schools and educational institutions in the capital, Phnom Penh.[18] The circular cited young people's growing addiction to "all kinds of [internet] games" which it categorized as illegal along with terrorism, economic crime, and pornography.[19] Penalties for violating the circular include forced closure, the confiscation of equipment, and arrest, though it did not specify potential sentences. The rules would affect almost every cybercafe in the city, threatening internet access for those with no personal computer, according to a map-based visualization produced by the non-profit web portal Urban Voice Cambodia, which puts nearly every building in the capital within 500 meters of one school or another.[20] Internet users worry this indicates the kind of heavy-handed regulation that might feature in an upcoming cyberlaw, which the government announced it would draft in May 2012. So far, though, the circular has yet to be implemented.

LIMITS ON CONTENT

At least three popular Cambodian blogs hosted overseas were blocked for perceived antigovernment content in 2011, and most users within the Kingdom are still unable to access them

[12] Arne Mauser, "Google Translate now Supports Khmer," *Official Google Translate Blog*, April 18, 2013, http://bit.ly/18efRin.
[13] Prak Chanseyha, "Two Young Cambodian Women Develop an Automatic Translation System" [In Khmer], March 26, 2013, http://news.sabay.com.kh/articles/391769.
[14] "Minister: Democracy Exists Without Opposition Newspapers," *Cambodia Herald,* May 3, 2013, http://bit.ly/18zuUnz.
[15] Sopheap Chak, "Cambodia's Great Internet Firewall?" *Global Voices Online*, March 2, 2010, http://bit.ly/brP14M.
[16] Brooke Lewis and Sam Rith, "Ministers Differ on Internet Controls," *Phnom Penh Post*, February 26, 2010, http://www.phnompenhpost.com/index.php/2010022632744/National-news/ministers-differ-on-internet-controls.html.
[17] A Circular is a measure endorsed by a Minister or the Prime Minister and is used to explain a point of law or to provide guidance with regards to a point of law. It is advisory in nature, and does not have binding legal force, though it can include penalties for non-compliance.
[18] LICADHO, "New Circular Aims to Shut Down Internet Cafes in Cambodia," press release, December 13, 2012, http://www.licadho-cambodia.org/pressrelease.php?perm=298.
[19] Cambodian Center for Human Rights, "Cambodian Government Seeks to Shut Down Internet Cafés in Phnom Penh Thereby Posing a Threat to Internet Freedoms," briefing note, December 14, 2012, http://bit.ly/17cObuG.
[20] Urban Voice Cambodia, "Save the Internet Cafes Campaign," March 15, 2013, http://bit.ly/1bR8pxp.

without the use of circumvention tools. While this has not yet resulted in more systematic censorship, these blocks revealed a troubling degree of cooperation between ISPs and officials, a lack of transparency, and a refusal to heed public opinion, which generally remains against government regulation of online content. In other cases, however, online activism has raised awareness of compelling issues in the public interest.

Compared to traditional media in Cambodia, new media, including online news, social networks and personal blogs, enjoy more freedom and independence from government censorship and restrictions. However, the government has proactively blocked blogs and websites, either on moral grounds, or for hosting content deemed critical of the government.

Since early 2009, websites and blogs showing pornography or sexually explicit images have been subject to blocking. Notably, Reahu, a US-based site selling images of models depicting traditional Apsara or Cambodian goddesses in erotic poses, is inaccessible in Cambodia.[21] In early 2010, news reports cited plans to gather bi-monthly meetings of a government morality committee, including MPTC, Ministry of Women's Affairs and Ministry of Interior representatives, to review websites and block those in conflict with national values. An official said this monitoring was necessary in light of the rapid spread of ICTs nationwide.[22] No restrictions have been reported as a result of such a plan, but the government's intent appears unchanged: In early 2011, So Khun, Cambodia's Minister of Posts and Telecommunication, asked mobile phone operators to "co-operate" in blocking web sites "that affect Khmer morality and tradition and the government," according to *The Phnom Penh Post,* citing internal MPTC minutes.[23]

Politically-motivated blocking has not yet been systematically applied, although it has been observed on a case by case basis. In 2009, the Cambodian Center for Human Rights (CCHR) reported the AngkorNet ISP was blocking access to a report by the UK-based NGO Global Witness, because it criticized government corruption. AngkorNet confirmed its subscribers could not access the content,[24] but said it was due to a technical error.[25] Since then, however, international NGOs and news websites have been widely available.

Blogs hosted overseas, in contrast, became subject to blocks within Cambodia in early 2011 when all ISPs blocked the international host service Blogspot, apparently in reaction to a December 2010 post on KI-Media, a blog run by Cambodians both inside and outside of the Kingdom. The site, which is often critical of the administration, described the prime minister and other officials as 'traitors' after opposition leader Sam Rainsy alleged they had sold land to Vietnam at a contested

[21] Brendan Brady, "Govt Moves Raise Censorship Fears," *Phnom Penh Post*, March 3, 2009, http://www.phnompenhpost.com/national/govt-moves-raise-censorship-fears.
[22] Sen David and Brooke Lewis, "Cambodian Government Panel to Target Racy Images," *Phnom Penh Post*, February 3, 2010, http://www.phnompenhpost.com/national/govt-panel-target-racy-images.
[23] Thomas Miller, "Ministry Denies Blocking Website," *Phnom Penh Post,* February 16, 2011, http://www.phnompenhpost.com/national/ministry-denies-blocking-website.
[24] Sebastian Strangio and Vong Sokheng, "NGO Site Barred by Local ISP," *Phnom Penh Post,* February 9, 2009, http://www.phnompenhpost.com/national/ngo-site-barred-local-isp.
[25] "Provider Denies Blocking Watchdog's Web Site," VOA Khmer, February 9, 2009, http://www.voacambodia.com/articleprintview/1354564.html.

national border. All ISPs except Metfone subsequently restored service to the sites following customer complaints, according to CCHR.[26] In February 2011, however, multiple ISPs including Online, WiCam, Metfone and EZECOM reinstated blocks on individual Blogspot sites, including KI-Media, Khmerization—another critical citizen journalist blog—and a blog by the Khmer political cartoonist Sacrava.

The government denied responsibility for ordering the blocks. However, the same month, *The Phnom Penh Post* leaked the contents of an e-mail sent from the account of Sieng Sithy, deputy director of MPTC policy regulation, extending appreciation to ten ISPs for blocking access to KI-Media, Khmerization and Sacrava, among other sites.[27] The *Post* also cited official minutes documenting the ministry asking ISPs to impose the blocks. In the leaked email, Sieng Sithy urged non-compliant service providers WiCam, Telesurf and Hello to abide by the request: "We found that you are not yet taken an action [sic], so please kindly take immediate action [...]Again and again, in case of not well cooperation is your own responsibility [sic]."[28] Sieng Sithy declined the *Post's* request to comment on the email, but other ministry officials denied its veracity, describing it as a publicity stunt by the bloggers.

ISPs proved similarly evasive when reporters tried to narrow down the source of the blocks. An EZECOM spokesman denied being asked to restrict access to specific sites, characterizing the blocking as a technical problem. An unnamed WiCam employee, on the other hand, confirmed receiving the emailed request to block the sites; WiCam users trying to visit KI-Media were notified the content was "blocked as ordered" by the MPTC until mid-February, when the notice was replaced by a generic error message, according to the *Post*.

The incident was a worrying indication to civil society groups that the government was seeking to control online content as it does traditional media.[29] Despite their protests, however, media coverage of the censorship died down in 2012, though the affected sites remained largely inaccessible within Cambodia in May 2013.

Besides blocking content, government bodies have also sought to restrict text messaging in the past. The NEC and the MPTC requested three main mobile service providers shut off SMS services nationwide the day before 2007 polls, justifying the action under a law prohibiting campaigning on the day of or the day immediately before a vote. Opposition parties and human rights groups said the ban would hamper freedom of expression.[30] Ironically, the Cambodian People's Party—who implemented the ban—themselves embraced SMS as part of a successful 2008 election campaign,

---

[26] Cambodian Center for Human Rights, "Fundamental Freedoms Series: Internet Censorship," factsheet, June 2011, http://www.cchrcambodia.org/admin/media/factsheet/factsheet/english/Internet_Censorship_Factsheet_Dove_en.pdf.
[27] T. Miller, "Tangled Web Revealed," *Phnom Penh Post*, February 16, 2011. See also, VOA News, "Cambodia Blocks Anti-Government Websites," February 16, 2011, http://bit.ly/16zRlel.
[28] Miller, "Tangled Web Revealed."
[29] Freedom House, "Cambodia Country Report," *Freedom on the Press 2013*, http://bit.ly/159AgGQ.
[30] Preetam Rai, "Cambodia: SMS blocked During Elections," *Global Voices,* March 31, 2007, http://globalvoicesonline.org/2007/03/31/cambodia-sms-blocked-during-elections/.
People Daily's Online, "Cambodian election authority bans SMS on election day," March 30, 2007, http://english.people.com.cn/200703/30/eng20070330_362308.html.

fuelled in part by a nationalistic movement stemming from disputed claims to temple on the border with Thailand. The party won acclaim when it denounced Thai claims to the temple as an invasion of Cambodian territory, though they subsequently had to distance themselves from popular SMS campaigns urging Cambodians to boycott everything Thai. No attempts to limit SMS have been documented since then. However, as the use of mobile technology continues to grow, officials cited May 2012 rumors of a violent political clash in Phnom Penh circulating via SMS among the justifications for the cybercrime law now in its draft stages.[31]

Despite these restrictions, the internet has contributed to the social and political development of Cambodia. A range of netizens and grassroots activists have used new media and other online tools to mobilize and make an impact. Facebook has a total penetration of 5.11 percent and is growing fast, with Cambodian Facebook subscriptions increasing by 31 percent between May 2012 and March 2013, according to one source.[32] Such a sharp increase—albeit from a low starting point—has evidently given the government cause for concern. As July 2013 elections approached, the NEC issued a statement in May requesting social media users to avoid providing wrong information about election procedures and dates.[33] On the same day, in remarks made to students, Information Minister Khieu Kanharith warned those who are active on Facebook not to use the tool to impugn the reputation of others.[34]

Personal blogging is popular in Cambodia. Most bloggers are aged between 20 and 29 and are well educated, but the majority blog about personal experiences, rather than political events.[35] There are a number of political blogs and websites available to Cambodian youth, however. Users continue to read even those blogs which are blocked, like KI-Media, through software that allows proxy access, although no data is available indicating how widespread this practice is. A number of blog causes have also emerged, such as "Prey Lang – It's Your Forest Too," a blog to provide public updates on conservation activities surrounding an endangered forest. [36] Several online campaigns and petitions have met with success. Veteran human rights defender and journalist Mam Sonando, who was sentenced to 20 years imprisonment after reporting on land seizures in 2012, was released on probation in March 2013 after sustained online and offline activism and international attention caused the court to drop some of the charges against him.[37] Internet users also protested against the arrest of activists from the Boeung Kak community, who defend Phnom Pehn's urban wetlands,[38]

[31] Cambodian Centre for Human Rights, "Cambodian Governmentis drafting the first ever Cyber Law," alert, May 24, 2012, http://www.cchrcambodia.org/index_old.php?url=media/media.php&p=alert_detail.php&alid=21&id=5.
[32] Social Bakers, "Facebook Statistics: Cambodia," accessed March 27, 2013, http://www.socialbakers.com/facebook-statistics/cambodia.
[33] National Election Committee of Cambodia, "Statement on the Usage of Social Media" [In Khmer], May 23, 2013, http://www.necelect.org.kh/nec_khmer/index.php?option=com_content&view=article&id=1064&Itemid=340; "NEC Says Statement on Bloggers Not Attack on Free Speech," *Cambodia Daily*, May 27, 2013, http://bit.ly/15aHXsj.
[34] *Cambodian Express News*, "Khieu Kanharith Reminds Facebook users to be Careful Writing Misinformation and Affecting Others' Reputations" [In Khmer], May 23, 2013, http://bit.ly/1biONCZ.
[35] Department of Media and Communication, "*Empowering Cambodian Women Psychologically Through Blogging,*" Cambodia Communications Review 2010, December 2010, 18.
[36] Prey Lang is the "largest primary lowland dry evergreen forest remaining both in Cambodia and on the Indochinese Peninsular." See, "Our Prey Lang," (Blog) accessed July 2013, http://ourpreylang.wordpress.com/.
[37] International Federation of Journalists, "Joint Statement: Cambodia: Mam Sonando Released," March 22, 2013, http://asiapacific.ifj.org/en/articles/joint-statement-cambodia-mam-sonando-released.
[38] See, for example, *Free the 15*, (Blog), accessed July 2013, http://freethe15.wordpress.com/.

and helped document Cambodia's rising number of traffic accidents, stirring debate on how to improve public safety.

There have been several blogosphere and technology gatherings among individuals who are passionate about ICTs and personally invested in improving Cambodia's ICT development. Organizers of events such as BarCamp have extended even beyond Phnom Penh, thanks to international donors and the private sector. Cambodia also hosted BlogFest Asia, a community-organized gathering of around 200 individuals from several Asian countries, in early November 2012.

VIOLATIONS OF USER RIGHTS

The news that the government was drafting a cybercrime law was the most concerning development for Cambodian internet users in the past year. While the legislation will ostensibly combat cybercrime, the use of existing criminal defamation and incitement laws to limit free expression and punish traditional journalists sets a troubling precedent for future abuses by the state. Neither is the government transparent about existing measures which govern the online space: a circular ordering cybercafés and telecommunications providers to store user data and provide it to police investigating threats to national security—without judicial oversight—has been in place since February 2012, though it only came to light in August 2012.

The right to freedom of expression is enshrined in Article 41 of Cambodia's constitution, and protected by international treaties that the country has ratified and incorporated into its domestic law.[39] However, Cambodia has a poor record of honoring the right in practice. Politicians past and present have sought to intimidate and suppress critics: Insofar as traditional media is concerned, Cambodia appears to be pluralistic, yet the government and its allies exercise tight control over print and broadcast news outlets, particularly those they perceive to be aligned with the political opposition.

The government uses legal provisions governing criminal defamation and incitement to punish those who use traditional media to share views that run counter to their own. In a 2012 report, Human Rights Watch, citing local NGOs, reported 12 imprisonments on those counts handed down by Cambodian courts since December 2010.[40] These punishments serve as a disincentive to individuals and organizations who wish to express their own views, encouraging self-censorship.

Since the last general election in 2008, the government has worked to increase the legislative arsenal available to the judiciary in the pursuit of government critics.[41] A new penal code, which

[39] Constitution of the Kingdom of Cambodia, Article 31 states that "the Kingdom of Cambodia shall recognize and respect human rights as stipulated in the United Nations Charter, the Universal Declaration of human Rights, the covenants and conventions related to human rights, women's and children's rights."
[40] Human Rights Watch, "*World Report 2012: Cambodia*," http://bit.ly/1dPDNdO.
[41] Cambodian Center for Human Rights and ARTICLE 19, "Cambodia: Freedom of Expression and the Point of No Return," Press Release, February 14, 2011, available at Scoop.co.nz, http://bit.ly/e6bklj.

came into force in December 2010,[42] contains nine provisions which criminalize various forms of expression, while forthcoming laws that regulate unions and non-governmental organizations threaten to further undermine freedoms of association and expression.[43]

In that context, internet users face the prospect of new legislation governing the online space with trepidation. In May 2012, the government announced it was in the process of drafting Cambodia's first ever cyber law,[44] with the stated intention of cracking down on online crimes so that it can "protect formal, private and copy-righted data from hacking, or the destruction of users' formal data, especially banks and related institutions."[45]

Besides legal measures, official harassment creates a climate of self-censorship on offensive or politically-sensitive topics among Cambodia's human rights and free expression communities. CCHR documented 123 cases of anti-media harassment between 2007 and 2011.[46] Among them, police were reported arresting journalists, preventing them from entering public events, confiscating or damaging their property, and threatening closure of their news outlets; other journalists were subject to physical violence in retaliation for their work. Cambodian publishers and editors have an active policy to cover less sensitive—and often less interesting—stories, "in order to stay out of harm's way."[47]

While bloggers have yet to be targeted in the same way as their traditional media counterparts, this restrictive information environment helps explain why comparatively few netizens are politically vocal. Furthermore, a 2010 conviction of a UN Food Program employee in Phnom Penh who printed articles from KI-Media for colleagues served as a warning to internet users. The Phnom Penh Municipal Court sentenced Seng Kunnaka to six months' imprisonment and a fine of 1 million riel ($250) on charge of incitement to commit a felony under Article 495 of the new penal code,[48] though he had shared the information with just a handful of associates. Since this is an offense anyone using digital tools to distribute information is liable to commit daily, observers believe the conviction was intended as a deterrent. A more recent case also demonstrates the extension of offline tactics of control to new media. In early 2013, after a teacher described Phnom Penh police impounding his new motorbike on his personal Facebook account, police used the threat of a

[42] Human Rights Watch, *"Cambodia: New Penal Code Undercuts Free Speech"*, December 23, 2010, http://www.hrw.org/en/news/2010/12/22/cambodia-new-penal-code-undercuts-free-speech.
[43] "Draft Law on Trade Unions," available at *Sithi,* accessed August 2013 http://www.sithi.org/temp.php?url=law_infrastructur.php&tab_id=&type=1≶ and "Draft Law on Non-governmental Organizations and Associations," available at *Sithi,* accessed August 2013 http://www.sithi.org/temp.php?url=law_infrastructur.php&tab_id=&type=1&lg.
[44] Cambodian Center for Human Rights, "Human Rights Chronology," *Sithi*, December 10, 2012, http://sithi.org/temp.php?url=crono_era.php&lg.
[45] Faine Greenwood, "As the Internet Raises Civic Voices in Cambodia, a Struggle Brews over Net Control," *Techpresident*, March 27, 2013, http://techpresident.com/news/wegov/23659/internet-civic-voices-cambodia-struggle-net-control.
[46] "Harassment of Media," *Sithi,* accessed July, 2013, http://www.sithi.org/temp.php?url=jour_case/jour_case.php&lg. No data has been published for the coverage period.
[47] "Soldiers for Free Speech," *Phnom Penh Post,* January 6, 2010.
[48] International Federation for Human Rights, "Cambodia: Assault on Freedom of Expression Continues with Conviction of UN Staff," December 23, 2010, http://www.fidh.org/Cambodia-Assault-on-freedom-of-expression.

defamation case against him to extract a signed statement that he would no longer discuss the topic over Facebook.[49]

In February 2012, a joint Ministry of Interior and MPTC circular ordered internet cafes to set up surveillance cameras and store footage for three months; phone shops and telecommunications operators were told to register subscribers' national ID cards or international passport and visas, on the grounds such measures would "better promote protection of national security, safety and social order for the country."[50] The operators "are obliged to provide necessary documents including users' identity cards and used data"—which must be stored for six days—to designated officials "for purposes of investigation of any offense which is involved in issues of national security, safety and social order." Under the internal circular—which only came to public notice in August 2012—providers must also notify existing subscribers of the new requirements and are entitled to temporarily suspend service if they fail to produce ID within a month. As of April 2013, in accordance with Cambodia's habitually slow pace of adopting new regulation, the requirements have yet to be implemented, though civil society groups fear the impact of such supervision for public debate and social activism. The circular's vague definition of what constitutes an offense involving these issues, the lack of judicial oversight over officials' requests for user data, and the threat to impose unspecified fines or revoke licenses for telecommunications operators who fail to comply, all represent a lack of respect for digital rights.

Government websites have been vulnerable to technical violence in the form of cyberattacks since 2002. Targets in 2012 and 2013 included the Supreme Court and the national police.[51] The same month, the hacktivist collective Anonymous released thousands of government documents online, including official personnel and expense records, details of lost Cambodian passports, and law enforcement exchanges with Cambodian-based embassies and consulates, in what the group described as retaliation for the arrest of the absconding Swedish founder of file-sharing website *The Pirate Bay*. Cambodian authorities deported Gottfrid Svartholm Warg under an international warrant in September 2012 to serve a one-year jail term in Sweden in relation to a 2010 conviction for copyright violations.[52] While experts say many technical attacks go unreported in Cambodia, analysts have not identified systematic targeting of civil society groups or government critics.

[49] Cambodian Center for Human Rights, "Phel Phearun Accused of Defamation over a Facebook Post," Case Study Series, March 2013, http://cchrcambodia.org/index_old.php?url=media/media.php&p=factsheet_detail.php&fsid=54&id=5.
[50] John Weeks, "Cambodia's Default Internet Law – Draft Translation," *Jinja.Apsara*, July 5, 2012, http://jinja.apsara.org/2012/07/cambodias_default_internet_law-%E2%80%93-draft_translation/.
[51] Ellyne Phneah, "Two More Cambodia Govt Sites Hacked and Defaced," *ZDNet*, January 10, 2013, http://www.zdnet.com/two-more-cambodia-govt-sites-hacked-and-defaced-7000009622/; Denise Hruby and Neou Vannarin, *Cambodia Daily*, January 10, 2013, http://www.cambodiadaily.com/archive/government-websites-a-haven-for-hackers-7577/.
[52] Conal Urquhart, "Pirate Bay Co-founder Gottfrid Svartholm Warg Arrested in Cambodia," *Guardian*, September 3, 2012, http://www.guardian.co.uk/technology/2012/sep/02/pirate-bay-founder-arrested-cambodia.

CHINA

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	18	19
Limits on Content (0-35)	29	29
Violations of User Rights (0-40)	38	38
Total (0-100)	85	86

* 0=most free, 100=least free

POPULATION: 1.35 billion
INTERNET PENETRATION 2012: 42 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Mobile replaced broadband as the number one means of accessing the internet in 2012 (see **OBSTACLES TO ACCESS**).
- China's cybercafés are now 40% owned by chains, which are easier for authorities to regulate than independent businesses (see **OBSTACLES TO ACCESS** and **VIOLATIONS OF USER RIGHTS**).
- Traffic on Virtual Private Networks (VPNs)—used to bypass censorship—was disrupted, sometimes obstructing commercial use (see **LIMITS ON CONTENT**).
- Regulators ordered online video services to censor short films in July 2012, when users adopted them to bypass film and broadcast restrictions (see **LIMITS ON CONTENT**).
- Security agents in Tibet and Xinjiang searched cellphones to pre-empt allegedly anti-state activity (see **VIOLATIONS OF USER RIGHTS**).
- A Criminal Procedure Law amendment took effect in January 2013, strengthening legal grounds for detaining anti-state suspects incommunicado (see **VIOLATIONS OF USER RIGHTS**).

KEY FIGURES

564 million: Internet users the government reported as of January 2013;

986 million: Mobile phone owners reported;

800 million: People still citing television as their main source of news (see **OBSTACLES TO ACCESS**).

94: China's position in one worldwide survey of broadband speeds;

3: Hong Kong's position in the same survey (see **OBSTACLES TO ACCESS**);

400 million: Microblog accounts registered on Sina Weibo;

46 million: Sina Weibo accounts that are actively used;

50,000: Sina Weibo accounts openly operated by ministries or officials (see **LIMITS ON CONTENT**);

24 hours: Time it takes for Sina Weibo to delete most banned posts (see **LIMITS ON CONTENT**);

12: Tibetans detained for allegedly inciting separatism, some via mobile phone (see **VIOLATIONS OF USER RIGHTS**);

20: Uighurs sentenced in March 2013 for alleged militant activity involving internet, phone and digital storage devices (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

The Chinese Communist Party's commitment to curtailing internet freedom was unwavering over the course of the leadership change that took place during the coverage period for this report, May 1, 2012, to April 30, 2013. If anything, the high-level meetings at which the handover was announced served as catalysts for tighter controls on content, measures to deliberately slow internet traffic, and intensified harassment of dissidents, as the party's propaganda and security agencies worked to eliminate any nascent political challenge. The internet restrictions Freedom House documented this year were faster and more nuanced than ever before.

The selection of Xi Jinping as the new party chief and head of state emphasized continuity, a message that was reinforced by the simultaneous promotion of party hard-liners like propaganda czar Liu Yunshan. The rhetoric of the new leadership also harkened back to the past. Party officials circulated seven "speak-nots," or taboo topics—which included "citizens' rights" and "press freedom"—to universities and media groups in May 2013. Meanwhile, Xi adopted the Maoist term "mass line" to encourage fellow cadres to remain close to the people.

This conservative discourse cannot conceal the unprecedented transformation taking place in China: More than 500 million people in the country are now online. Internet penetration is at 42 percent, compared with just 6 percent when Xi's predecessor, Hu Jintao, took office in 2003. Residents of cities like Shanghai and Beijing are the primary beneficiaries of this expanded access, while rural areas lag behind. An estimated 800 million people still rely on television outlets, like state broadcaster China Central Television (CCTV), as their main source of information.[1] But for the first time on record, more Chinese people connected to the internet via mobile phone than through any other method in the past year, meaning penetration will only continue to climb.

Internet access has provided Chinese citizens with new tools to challenge policy. This year, millions of online comments about air pollution spurred a nationwide upgrade of oil refineries. Online forums also host a surprising range of opinions on political topics. When Edward Snowden fled to Hong Kong after leaking U.S. National Security Agency secrets, users of microblog platforms in China both supported and derided him; some joked cynically that he should see how China handles its citizens' internet records.[2]

Many believe that such incremental civic gains will inevitably spark political reform. A 2013 meme imagined a future shift in the perspective of the Chinese authorities: "When there are a hundred of you, we will detain you," it read, but "when there are a hundred thousand of you—we will join you."[3] Yet the internet has also provided those authorities with an extraordinary range of tools to

[1] Hu Yong et al., *Mapping Digital Media: China* (New York: Open Society Foundations, 2012), http://www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-china-20121009.pdf.
[2] Wendy Qian, "Chinese Web Users React to PRISM: The End of the Affair with Google and Apple?" *Tea Leaf Nation*, June 11, 2013, http://www.tealeafnation.com/2013/06/chinese-web-users-react-to-prism-the-end-of-the-affair-with-google-and-apple/.
[3] Xiao Shu, "The Southern Weekly Incident, An Exercise in Citizen Action," China Media Project, January 31, 2013, http://cmp.hku.hk/2013/01/31/31034/.

contain critical conversations. A 2012 academic review of censorship across nearly 1,400 online platforms in China estimated that 13 percent of posts containing sensitive keywords were deleted, many within 24 hours of publication, some within minutes.[4]

Even with vast technological and human resources at their disposal, censors struggled to limit some online debates in the past year. Actress Yao Chen posted a quotation from Soviet-era dissident Aleksandr Solzhenitsyn, "One word of truth outweighs the whole world," to her network of 32 million microblog followers in support of *Southern Weekly* journalists in Guangzhou who were on strike against censorship in January 2013.[5] Anti-Japanese protesters also overwhelmed content controls during a flare-up in the territorial dispute between China and Japan in September 2012. Online vitriol escalated into violent rioting, which Chinese Communist Party (CCP) officials consider a threat even when it supports their position.

But Chinese information authorities are also adept at manipulation, and increasingly adaptable as complex situations unfold. In Guangzhou, propaganda officials negotiated with journalists to end the January strike without conceding to all their demands, and the story fell out of the public eye. It was a memorable achievement, but no other newsrooms were emboldened to follow suit. A state-led wave of editorials condemning anti-Japanese activity helped rein in protests the previous September. Experts even speculate that censorship can be temporarily lifted, and criticism of select officials tacitly encouraged, as a weapon in the party's internal politics. Anticorruption campaigns spread like wildfire online in China, helping the central government hold local officials in check. Yet when the *New York Times* and Bloomberg accused the families of top leaders of amassing disproportionate wealth, their websites were subjected to punitive blocking and their staff computers were hacked.

Even when content is filtered, the process is being constantly refined, often by private companies that serve as intermediaries between the state and users. The 1989 Tiananmen Square massacre is so thoroughly censored that users of the popular Sina Weibo microblogging platform are not even able to use the search term "today" on the anniversary, June 4.[6] Yet this year, Sina unblocked a handful of Tiananmen-related search terms, allowing users to access dozens of discussions—though unrelated to the 1989 protests in Beijing or the subsequent military crackdown.[7] By offering sanitized results rather than the standard message that blocked keywords usually produce, the company appeared determined to make its censorship invisible.

Far from stifling private innovation, the state has effectively harnessed it to further its own goals. Sina publicly acknowledges that it cannot yet fulfill all of the Chinese government's requirements, like registering its Weibo users' real names. But to avoid getting shut down, it will continue to try.

---

[4] Gary King, Jennifer Pan, and Margaret Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," Working Paper, June 18, 2012, http://gking.harvard.edu/files/censored.pdf.
[5] Scott Greene, "Southern Weekly Editorial Staff Goes on Strike," China Digital Times, January 6, 2013, http://chinadigitaltimes.net/2013/01/southern-weekend-editorial-staff-goes-on-strike/.
[6] "Censoring a Commemoration: What June 4-Related Search Terms Are Blocked on Weibo Today," Citizenlab, June 3, 2013, https://citizenlab.org/2013/06/censoring-a-commemoration-what-june-4-related-search-terms-are-blocked-on-weibo-today/.
[7] "Sina Testing Subtle Censorship ahead of Tiananmen Anniversary," Greatfire.org, May 31, 2013, https://en.greatfire.org/blog/2013/may/sina-testing-subtle-censorship-ahead-tiananmen-anniversary-0.

Indeed, many of the more subtle developments documented in this report did not originate with the central propaganda department, a bastion of conservative ideology not known for nuance. Instead, they were developed by service providers looking to satisfy the government's demands while maintaining the illusion of freedom for their users. Google, since it challenged the Chinese government's censorship practices in 2010, has attempted to innovate on the side of transparency, briefly informing Chinese users of blacklisted search terms in 2012.[8] But its experiments have cost it considerable market share as the authorities seek to marginalize the company.

Much is at stake for these firms, but the penalties of defying the state are far greater for individual dissidents. Security agencies make use of widespread surveillance capabilities and a politicized legal system to pursue selective prosecutions of dozens of people like Cao Haibo, whose eight-year prison sentence for publishing antistate content online was reported in November 2012. What constitutes antistate content is alarmingly broad—in Cao's case it was articles he had written about democracy—and can include material published years before a case comes to trial, whether or not it was censored at the time. Ethnic minorities in regions where CCP rule is disputed or resented, such as Tibet and Xinjiang, are particularly vulnerable. At least a dozen Tibetans and 20 Uighurs were jailed during the coverage period in relation to their sharing of information online or via mobile phone. Prosecutors' claims that they were inciting separatism or violence are impossible to verify, as their trials lack due process and are closed to observers. The state continues to pour resources into separating these perceived enemies from families, lawyers, and journalists. In 2012, China spent more on "social stability maintenance"—which includes many of the practices of information control outlined in this report—than it did on defense.

The CCP's influence online reaches far beyond China's borders. Nearly a third of cyberattack traffic worldwide in 2012 was traced to Chinese soil, and cybersecurity experts tracked one notorious hacking group to a military facility in Shanghai. Such international activity generally falls outside the scope of this report, but it is rooted in the online environment outlined here. It also serves as an added reminder that Chinese internet freedom, or the lack thereof, has ramifications for the entire world.

[8] Censors quickly disabled the feature, and the company apparently discontinued it. Bill Bishop, "Today's China Readings," *Sinocism China Newsletter*, July 11, 2012, https://sinocism.com/?p=5722; "All Blocked Keywords According to Google," Greatfire.org, June 2, 2012, https://en.greatfire.org/blog/2012/jun/all-blocked-keywords-according-google.

OBSTACLES TO ACCESS

China had the largest number of internet and mobile phone users in the world in January 2013, with an estimated 564 million and 986 million, respectively.[9] These figures, though staggering, paint an incomplete picture of China's uneven economic development and manipulated connectivity. Average broadband connection speeds are comparatively slow, leaving China in 94th place in global rankings.[10] It is stymied by poor infrastructure—particularly in the country's vast rural areas—and a telecommunications industry dominated by state-owned enterprises. Centralized control over international gateways and sporadic, localized shutdowns of internet access around sites of social unrest are significant obstructions to full and free access. Nationwide blocking, filtering, and monitoring systems further slow access to international websites.[11] The Hong Kong administrative region, free of these obstacles, enjoys the third-fastest average connection speeds worldwide, after South Korea and Japan,[12] and at a fraction of mainland prices.

The China Internet Network Information Center (CNNIC), an administrative agency under the Ministry of Industry and Information Technology (MIIT), reports that rates of internet adoption have actually slowed since 2011 as the urban market approaches saturation.[13] Moreover, the gap between penetration rates in urban and rural areas has widened since 2007.[14] The 72.2 percent of residents online in the capital, Beijing, vastly outnumber the 28.5 percent with internet access in the least-connected province of Jiangxi in the southeast.[15] This divide kept overall internet penetration at just 42.1 percent,[16] slightly higher than the global average, which was 35 percent in 2011.[17]

---

[9] CNNIC, "The CNNIC Released the 31st Statistical Report on Internet Development in China," News Release, January 15, 2013, http://www1.cnnic.cn/IDR/ReportDownloads/201302/P020130221391269963814.pdf.

[10] Lin Jingdong, "Global Speed Heavy: Mainland China Ranked 94th in the Second Half of 2012," *VentureData.org*, January 26, 2013, http://www.venturedata.org/?i480706_Global-speed-Heavy-Mainland-China-ranked-94th-in-the-second-half-of-2012.

[11] James Fallows, "The Connection has been Reset," The Atlantic, March 2008, http://www.theatlantic.com/magazine/archive/2008/03/-ldquo-the-connection-has-been-reset-rdquo/6650/.

[12] Christy Choi, "Hong Kong Has Fastest Peak Internet Speed in World," *South China Morning Post*, January 25, 2013, http://www.scmp.com/news/hong-kong/article/1135480/hong-kong-has-fastest-peak-internet-speed-world?page=all.

[13] CNNIC, *Zhong Guo Hu Lian Wang Fa Zhan Zhuang Kuang Tong* [The 28th Report on the Development of the Internet in China] (Beijing: CNNIC, 2011), http://www.cnnic.cn/research/bgxz/tjbg/201107/P020110721502208383670.pdf.

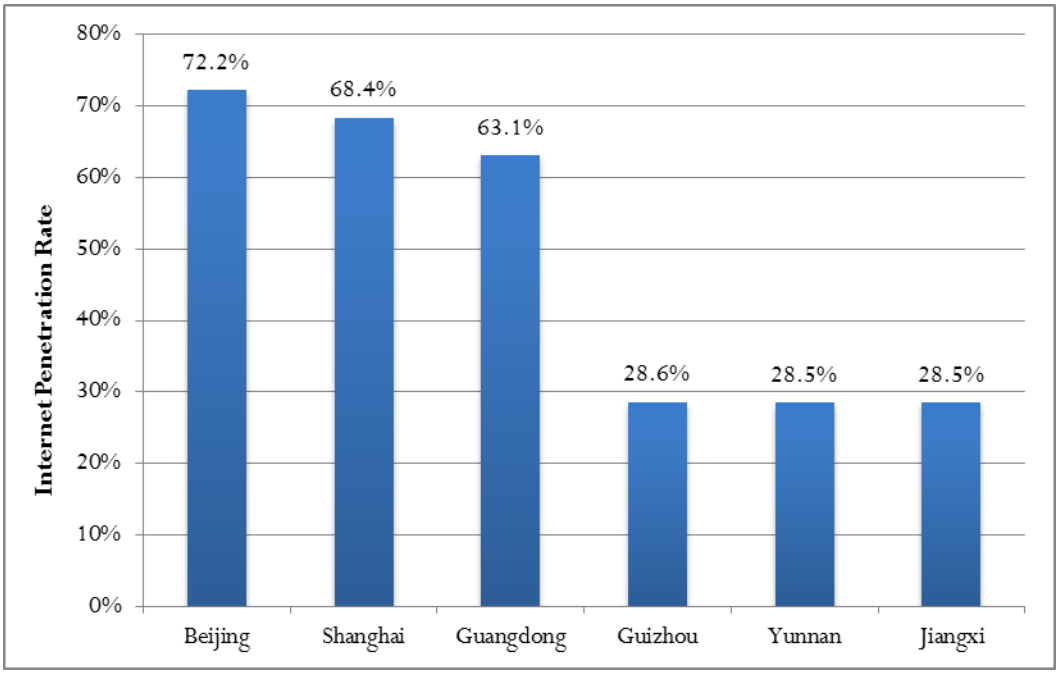
[14] CNNIC, *Zhong Guo Hu Lian Wang Fa Zhan Zhuang Kuang Tong* [The 29th Report on the Development of the Internet in China] (Beijing: CNNIC, 2012), 21, http://www.cnnic.cn/research/bgxz/tjbgdtygg/dtgg/201201/P020120116330880247967W020120116337628870651.pdf; Benat Bilbao-Osorio, Soumitra Dutta, and Bruno Lanvin, "The Global Information Technology Report 2013," World Economic Forum, 2013, http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf.

[15] CNNIC, "*Zhong Guo Hu Lian Wang Fa Zhan Zhuang Kuang Tong*," [The 31st Report on the Development of the Internet in China], January 2013, 15 http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201301/P020130122600399530412.pdf.

[16] CNNIC, [The 31st Report on the Development of the Internet in China].

[17] ITU, *The World in 2011: ICT Facts and Figures* (Geneva: ITU, 2011), http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.

Graph A. Internet Penetration Rate in Provinces of Mainland China between 2011 and 2012
(Source: CNNIC)

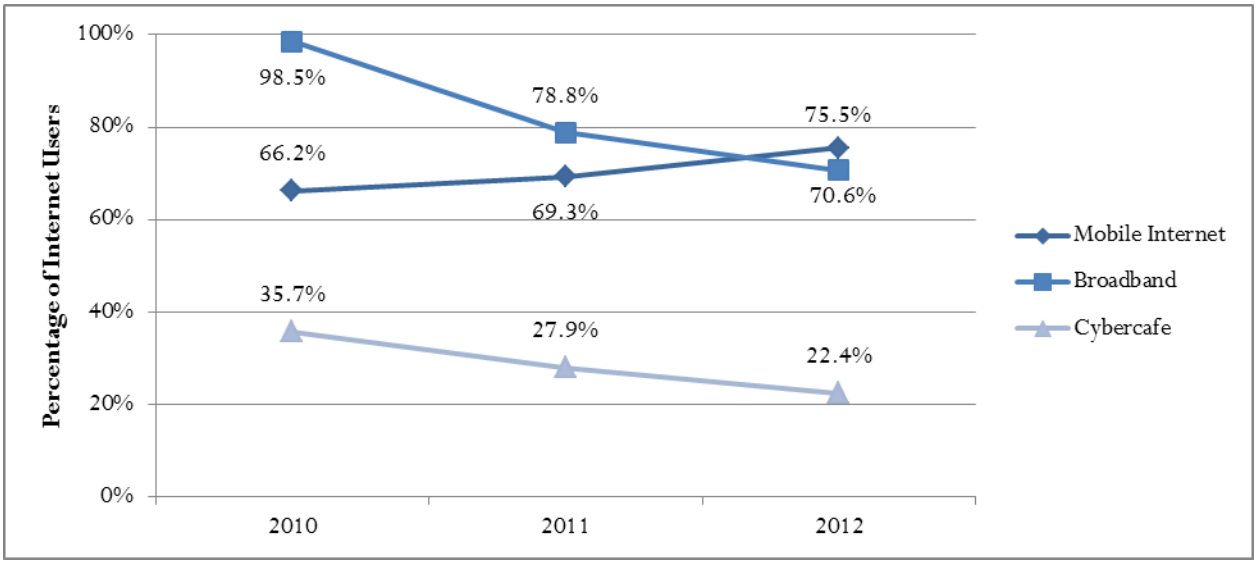


The CNNIC reported 422 million mobile internet users in December 2012. By contrast, broadband subscriptions declined from 450 million in 2010 to 380 million in 2012.[18] (Broadband subscriptions have dwarfed dial-up since 2005.[19])

Mobile replaced fixed-line broadband as China's preferred means of accessing the internet for the first time in 2012. Internet access via cybercafé declined, accounting for 22.4 percent of users, down from 27.9 percent in 2011.[20] While internet-enabled 3G (third-generation) phones are priced beyond the reach of many, platforms like the Tencent QQ instant-messaging service and Sina Weibo allow users to send and receive messages at low cost via 2G handsets.

[18] 163.com web portal visualization of CNNIC, [The 31st Report on the Development of the Internet in China], http://tech.163.com/special/cnnic30/#full.
[19] "CNNIC Releases Internet Report: China's Internet Users Exceed 100 Million," *Xinhua News*, July 22, 2005, http://news.xinhuanet.com/newmedia/2005-07/22/content_3251081.htm.
[20] CNNIC, [The 31st Report on the Development of the Internet in China], 21.

Graph B. Percentage of Internet Users Getting Internet Access Through Mobile Phones, Broadband, and Cybercafés (Source: CNNIC)



The historically high cost of broadband internet access helps to account for the shift toward mobile. The government took steps to address this when a 2011 antimonopoly investigation accused the state-owned China Telecom and China Unicom of abusing their market dominance to manipulate broadband pricing and overcharge competitors. The investigation was the first instance in which a 2008 antimonopoly law was used against state-owned enterprises, and it was announced in an unusually public way on CCTV.[21] The telecom giants swiftly revised their internetwork pricing structures to allow rivals fair access to their infrastructural resources.[22] Interestingly, one of the beneficiaries of this measure may be a government regulator, the State Administration of Radio, Film, and Television (SARFT), which said in 2012 that it would launch a national cable network, funded by the Ministry of Finance and offering telephone, broadcasting, and internet services. The plan would advance the overall integration of these three services, a goal the State Council had previously pledged to achieve throughout China by 2015, though the timetable for its implementation is not clear.[23]

While customers can now choose from among scores of private internet service providers (ISPs), the large state enterprises are widely perceived as responsible for the costly, inefficient connections

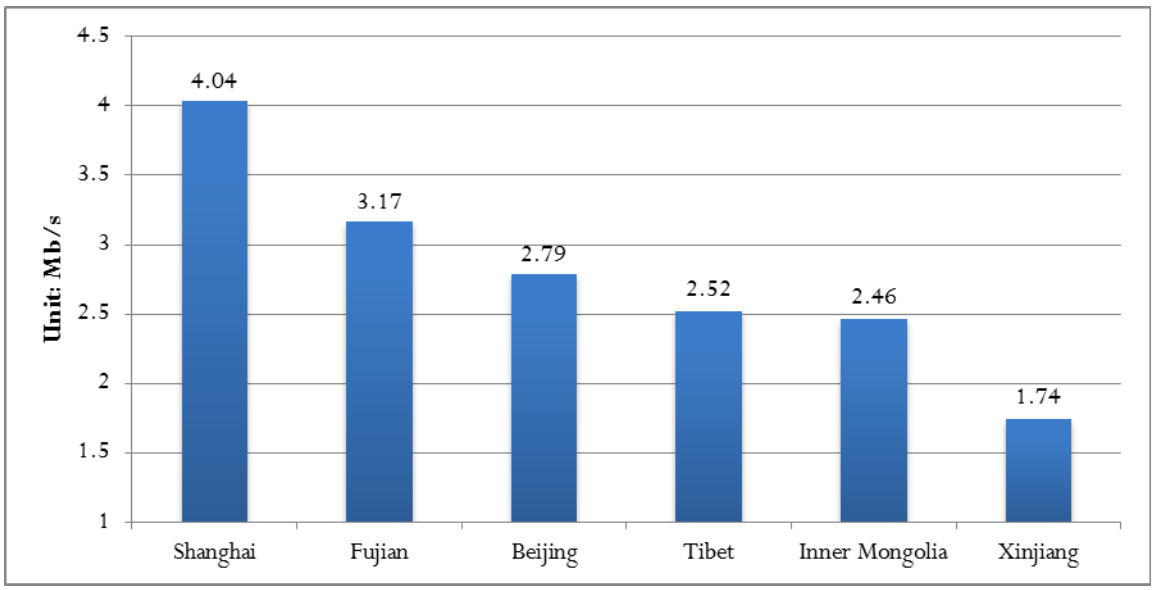
[21] Jan Holthuis, "War of the Giants – Observations on the Anti-Monopoly Investigation in China Telecom and China Unicom, HIL International Lawyers & Advisers, March 2, 2012, http://legalknowledgeportal.com/2012/03/02/war-of-the-giants-observations-on-the-anti-monopoly-investigation-into-china-telecom-and-china-unicom/..

[22] Lu Hui, "China Telecom, China Unicom Pledge to Mend Errors after Anti-monopoly Probe," *Xinhua News*, December 2, 2011, http://news.xinhuanet.com/english2010/china/2011-12/02/c_131285141.htm; "*Guo Jia Guang Dian Wang Luo Gong Si Jiang Qiang Cheng Li Zhong Yi Dong Wei Can Yu Chu Zi*" [State Radio and Television Networks Will be Set Up], *Sina*, November 15, 2012, http://tech.sina.com.cn/t/2012-11-15/03037799520.shtml..

[23] Tan Min, "SARFT Finishes Plan for National Cable Operator," *Caixin*, August 6, 2012, http://english.caixin.com/2012-08-06/100420145.html.

that continue to prevail.[24] The Beijing-based research company Data Centre of China Internet reported that the average cost of 1 Mbps of bandwidth was 469 times more on the mainland than in Hong Kong in 2011,[25] while consumers complained that broadband speeds remained slower than advertised in 2012.[26] The MIIT has sought other methods to improve internet service, such as mandating that homes constructed within reach of public fiber-optic networks be connected via a selection of service providers from April 2013 onward.[27] Whether China's infrastructure will be able to keep pace with such ambitious government projects, however, is still uncertain. Although the MIIT said all broadband users would have internet access at 100 Mbps by 2015, the average speed in the fastest city, Shanghai, was just 4.04 Mbps in 2012, compared with 2.52 Mbps in the less-developed—and more heavily censored—Tibetan Autonomous Region.[28]

Graph C. Average Broadband Connection Speed in 2012 Q4 (Source: ChinaCache)



Mobile phone communication is also dominated by state-owned enterprises, including China Mobile, China Telecom, and China Unicom. This situation, too, is under review: The MIIT issued draft proposals to open the market in January 2013, allowing private companies to buy mobile

[24] "Tighter Rules for Telecom Costs," *Shanghai Daily*, April 26, 2012, http://www.china.org.cn/business/2012-04/26/content_25241615.htm.
[25] "*Zhong Guo Kuandai Yong hu Diaocha*" [Survey of China's Broadband Users], Data Center of China Internet, 2011-2012, http://www.dcci.com.cn/media/download/905430773daab3f27453929ee140539fdc12.pdf. The center has not released data for 2012.
[26] "Chinese Internet Choked by "'Fake Broadband"' Providers," *Global Times*, October 8, 2012, http://www.globaltimes.cn/content/736926.shtml.
[27] Shen Jingting, "New Residences Required to Provide Fiber Network Connections," *China Daily*, January 9, 2013, http://usa.chinadaily.com.cn/business/2013-01/09/content_16099801.htm.
[28] "China's Broadband Speeds Show Shanghai Zooming Ahead [INFOGRAPHIC]," *Tech in Asia*, September 20, 2012, http://www.techinasia.com/china-broadband-speeds-2012-infographic/; "China Internet Report: The First Quarter of 2013," ChinaCache, May 2013, http://files.shareholder.com/downloads/ABEA-528MQE/2583814687x0x664689/2c293e5c-de24-4102-b7bd-828c0501bd94/ChinaCache_First_Quarter_2013_China_Internet_Report.pdf.

network resources and repackage them for the user over a two-year trial period.[29] China Mobile began testing faster 4G service in some eastern Chinese cities in 2013, and the MIIT said in late 2012 that it would be issuing licenses to providers to upgrade to 4G service within a year.[30]

The government has been willing to liberalize the telecommunications market in part because of the country's centralized connection to the international internet. Six state-run operators maintain the country's international gateways.[31] This arrangement remains the primary infrastructural limitation on open internet access, as it gives the authorities the ability to cut off cross-border information requests. All ISPs must subscribe via the gateway operators and obtain a license from the MIIT. Internet access via mobile phones is also monitored by the international gateway operators under MIIT oversight.

The government has shut down access to entire communications systems in response to specific events, notably imposing an astounding 10-month internet blackout in the Xinjiang Uighur Autonomous Region after an outburst of ethnic violence in the regional capital Urumqi in July 2009.[32] Since then, authorities have enforced smaller-scale shutdowns lasting several days or weeks. Officials in predominantly Tibetan areas of western China twice cut off local internet access during 2012: once in February following clashes surrounding a series of self-immolations and reports that soldiers had opened fire on civilians,[33] and again for two days around the July 7 birthday of the Dalai Lama, Tibet's exiled spiritual leader.[34] More than 100 self-immolations—suicides committed in protest against Chinese rule—have been documented since 2009.[35]

In other cases, the level of official interference with connectivity was hard to gauge. China was briefly isolated for two hours in April 2012 when users reported that all international websites were inaccessible. Hong Kong and U.S. users were unable to visit sites hosted in China during the same period. Cloud Flare Inc., a U.S.-based company that studies web performance, told the *Wall Street Journal* that the interruption appeared to have been triggered by overactive filtering, rather than a technical glitch, and that only traffic from China Telecom and China Unicom plummeted; smaller providers were unaffected.[36] In August 2012, the same company reported "increased

[29] Seng Jingting, "Telecom Plans 'Will Help Break' Industry Monopoly," China Daily, January 1, 2013, http://www.chinadaily.com.cn/bizchina/2013-01/09/content_16098031.htm.
[30] "China Mobile Launches TD-LTE Commercial Trials in Hangzhou, Wenzhou," Marbridge Daily, February 4, 2013, http://www.marbridgeconsulting.com/marbridgedaily/archive/article/63196/china_mobile_launches_td_lte_commercial_trials_in_hangzhou_wenzhou#When:12:00:00Z; Want China Times, "China Paves Way for 4G Telecom Network Expansion," November 28, 2012, http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20121128000040&cid=1502.
[31] CNNIC, [The 31st Report on the Development of the Internet in China], 21.
[32] Chris Hogg, "China Restores Xinjiang Internet," *British Broadcasting Corporation (BBC)*, May 14, 2010, http://news.bbc.co.uk/2/hi/asia-pacific/8682145.stm.
[33] Tania Branigan, "China Cut Off Internet in Area of Tibetan Unrest," *Guardian*, February 3, 2012, http://www.guardian.co.uk/world/2012/feb/03/china-internet-links-tibetan-unrest.
[34] "China Celebrates Dalai Lama's Birthday by Cutting Communications in Tibetan Region," Index on Censorship, July 10, 2012, http://www.ifex.org/china/tibet/2012/07/10/communications_cut/.
[35] "Self-Immolations by Tibetans," International Campaign for Tibet, June 19, 2013, http://www.savetibet.org/resources/fact-sheets/self-immolations-by-tibetans/.
[36] Paul Mozur, "New Clarity on China Internet Outage," *China Real Time Report* (blog), *Wall Street Journal*, April 13, 2012, http://blogs.wsj.com/chinarealtime/2012/04/13/new-clarity-on-china-internet-outage/.

difficulty with traffic out of China," but without a consistent pattern to indicate the cause.[37] An MIIT spokesperson denied rumors that China was "closing down the internet" in advance of the politically sensitive 18th Party Congress in the fall, but acknowledged conducting maintenance.[38]

Authorities exercise tight control over cybercafés and other public access points, which are licensed by the Ministry of Culture in cooperation with other state entities.[39] Consolidating these helps increase the efficiency of surveillance and censorship.[40]

By 2012, chains had absorbed around 40 percent of cybercafés following a ministry-led push to eliminate sole-proprietor locations by 2015. Over 10 different government and CCP entities, at both the national and local levels, are involved in internet censorship, with some instructions coming straight from the top. The State Internet Information Office was created in 2011 to streamline propaganda directives for online content, punish violators, and oversee telecommunications companies.[41] It has since increased controls on online video—particularly short-form "microfilms" that are commonly used to evade controls on content screened by mainstream movie theaters or news media[42]—and real-name registration for online platforms.[43] Two official regulatory entities, SARFT and the General Administration for Press and Publications (GAPP), are slated to merge, according to a plan announced in March 2013.[44]

[37] Tania Branigan, "China's Internet Users Temporarily Blocked from Foreign Websites," *Guardian*, April 12, 2012, http://www.guardian.co.uk/world/2012/apr/12/china-internet-users-foreign-websites.
[38] Brian Spegele and Paul Mozur, "China Hardens Grip before Meeting," *Wall Street Journal*, November 10, 2012, http://online.wsj.com/article/SB10001424052970204707104578092461228569642.html.
[39] These include the Public Security Bureau and the State Administration for Industry and Commerce. "Yi Kan Jiu Mingbai Quan Cheng Tu Jie Wang Ba Pai Zhao Shen Qing Liu Cheng" [A look at an illustration of the whole course of the cybercafé license application process], Zol.com, http://detail.zol.com.cn/picture_index_100/index997401.shtml.
[40] "China's 2013 Internet Café Market Down 13% YoY," 17173.com, April 28, 2013, http://www.marbridgeconsulting.com/marbridgedaily/2013-04-28/article/65634/chinas_2013_internet_caf_market_down_13_yoy.
[41] The State Internet Information Office operates under the jurisdiction of the State Council Information Office. "China Sets Up State Internet Information Office," *China Daily*, May 4, 2011, http://www.chinadaily.com.cn/china/2011-05/04/content_12440782.htm. See also "New Agency Created to Coordinate Internet Regulation," *China Media Bulletin*, May 5, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-21#3.
[42] Mathew Scott, "Censors Catch Up With China's 'Micro Film' Movement," *Agence France-Presse*, July 16, 2012, http://www.google.com/hostednews/afp/article/ALeqM5itjrPwXQFfB7ueKsg1TdiOtItR8w?docId=CNG.09667aa7e67669f6f7d1a284e78d6e1d.c1.
[43] See Congressional-Executive Commission on China (CECC), *Annual Report 2012* (Washington: CECC, 2012), 50–53, http://www.gpo.gov/fdsys/pkg/CHRG-112shrg76190/pdf/CHRG-112shrg76190.pdf.
[44] Alice Xin Liu, "China's Two Main Censorship Bodies to Merge," *Uncut* (blog), Index on Censorship, April 19, 2013, http://uncut.indexoncensorship.org/2013/04/sarft-gapp-china-censorship/.

LIMITS ON CONTENT

LIMITS ON CONTENT: AN OVERVIEW
MAY 2012–APRIL 2013

Censorship predictably intensified in advance of the leadership transitions at the November 2012 party congress and the March 2013 National People's Congress session. Reports of unrest, such as Tibetans self-immolating, were especially curtailed. The methods used were generally more precise and less visible than in the past, with the exception of a campaign against Bloomberg and the *New York Times* for their probing reports on wealth accumulation by China's first families. Instead of filtering out the individual articles, censors blocked the entire websites, depriving them of readership and advertising revenue.

Users in China can still access content hosted outside China using circumvention tools, at least until more companies follow China Unicom, which started severing connections on which circumvention was detected in December. Meanwhile, microblog users sometimes find that their posts have become invisible to others, requiring them to repost to keep their content in the public domain. These customized controls and manipulative practices are better understood thanks to some meticulous research and reporting published in 2012 and 2013.

In the past year, digital media also fueled popular participation in key debates over issues of public interest, such as smog levels in Beijing. But it is becoming harder to assess whether these movements represent a challenge to the censorship apparatus. They may be a sign that information authorities are more adept than ever at channeling outbreaks of discontent away from political issues and into local, finite, social matters.

In keeping with the unmatched size of their online population, Chinese authorities employ the most elaborate system for internet content control in the world. Government agencies and private companies employ thousands of people to monitor, censor, and manipulate content, from news reports to social-network pages. Routine censorship can be reinforced surrounding politically sensitive events, or just in response to the latest hot topic. Even this heavily censored and manipulated online environment, however, provides more space for average citizens to express themselves and air their grievances against the state than any other medium in China.

Content with the potential to delegitimize CCP rule is systematically censored. Criticism of top leaders or policies, both present and past, is almost always controlled—a category that encompasses the legacy of Mao Zedong, the 1989 military crackdown on student-led protests in

Beijing, and the Korean War. Independent evaluations of China's human rights record or CCP policies toward ethnic minorities and the banned Falun Gong spiritual group are also off-limits,[45] as are dissident initiatives that challenge the one-party regime. Names of established dissidents are frequently blocked, to prevent them gaining a wider following.

These standing taboos are supplemented by evolving, almost daily directives on negative developments or budding civic movements over issues like environmental pollution, food safety, or police brutality. Analysts increasingly agree that content control is aimed at suppressing nascent collective action, rather than comprehensively banning critical speech.[46] Individuals with significant social capital or a high international profile, which would allow them to mobilize mass support, are more likely to be censored.[47] As a result, censors can be remarkably tolerant of frustration vented at local governments or discussion of politically oriented terms like "democracy."[48] The prevalence of this term and others, like "freedom of speech," has risen in the Chinese blogosphere.[49] While that marks some progress toward openness, it also corresponds to a shift in CCP discourse. Censors first relaxed filters on the word "democracy" in 2005 after leaders redefined democratic governance as "the Chinese Communist Party governing on behalf of the people."[50]

Chinese authorities are not transparent about censorship. International critics who question limits on content receive responses ranging from denial ("the Chinese internet is open"[51]) to defiance, manifest in the phrase "internet sovereignty," meaning the right to practice censorship within Chinese borders. Domestically, leaders cite the need to curb pornography, gambling, rumors, and other harmful practices to justify content restrictions, though political topics are targeted at least as forcefully. Ironically, while burgeoning internet access has not overcome information controls, it has shone a light on the processes involved. Chinese freelance journalist Shi Tao was sentenced to ten years in prison in 2005 for e-mailing propaganda department directives to an overseas news website;[52] today, similar directives are routinely leaked online. Internal copies of a 2010 speech outlining internet management were circulated in online forums, allowing users to compare them

[45] A study conducted in 2011 by scholars at Carnegie Mellon found that up to 53 percent of microblog posts generated from Tibet were deleted. Byron Spice, "Carnegie Mellon Performs First Large-Scale Analysis of 'Soft' Censorship Media in China," Carnegie Mellon University, March 7, 2012, http://www.cmu.edu/news/stories/archives/2012/march/march7_censorshipinchina.html.

[46] "Preventing the organization of protests is as important, if not more important, than preventing users from reading unapproved content." Jedidiah R. Crandall et al., "ConceptDoppler: A Weather Tracker for Internet Censorship," Conference Paper for the 14th ACM Conference on Computer and Communications Security, October 29-November 2, 2007, http://www.csd.uoc.gr/~hy558/papers/conceptdoppler.pdf; King, Pan, and Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression."

[47] "Cyberdisappearance in Action," *China Media Bulletin*, July 14, 2011, http://www.freedomhouse.org/sites/default/files/inline_images/Cyberdisappearance%20in%20Action_special_feature-FINAL_0.pdf.

[48] King, Pan, and Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression."

[49] Ashley Esarey and Xiao Qiang, "Digital Communication and Political Change in China," *International Journal of Communication* 5 (2011), 298–319, http://ijoc.org/index.php/ijoc/article/view/688/525. Xiao Qiang was an advisor for this report.

[50] Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: Harper Collins, 2010), 20.

[51] "Saying of the Week: China's Internet Is Open," *China Digital Times*, February 6, 2013, http://chinadigitaltimes.net/2013/02/saying-of-the-week-chinas-internet-is-open/.

[52] Bob Dietz, "As Wang Is Freed, Chinese Journalist Shi Tao Still Held," Committee to Protect Journalists, August 31, 2012, http://cpj.org/blog/2012/08/as-wang-is-freed-chinese-journalist-shi-tao-still.php.

with the bowdlerized version circulated released to the public.[53] Criticism of the censorship system itself, however, is itself heavily censored. [54]

The CCP's content-control system consists of three primary techniques: **automated technical filtering**, **forced self-censorship** by service providers, and **proactive manipulation:**

> **Automated technical filtering** includes the best-known layer of the censorship apparatus: the blocking of foreign websites commonly referred to as China's "Great Firewall." The term implies a solid boundary, and in some cases, whole domain names or internet protocol (IP) addresses are blocked. "Web throttling," which slows the loading of pages to render services nearly useless, is employed as well. Internet users reported slowed broadband speeds and narrow bandwidth characteristic of web throttling during the month of the 2012 party congress.[55]
>
> More common, however, is the authorities' use of deep-packet inspection technologies to scrutinize traffic, both the user's request for content and the results returned, for an ever-evolving blacklist of keywords. If one is detected, the technology signals both sides of the exchange to temporarily sever the connection. This granular control renders censorship less noticeable to users, firstly because specific pages can be blocked within otherwise approved sites, and secondly because the interruption appears to come from the source of the information, not a third-party intrusion.[56]
>
> Of course, some censorship is designed to remind users that certain content is out of bounds.[57] One study redefines the Great Firewall as a panopticon, arguing that it need not block everything if the knowledge of monitoring suffices to promote the self-censorship that is pervasive among Chinese internet users. Other research suggests that security forces are most secretive when they are also conducting surveillance to uncover who is accessing banned content—particularly if that data can subsequently be used to justify detention or some other violation of the user's rights.[58]
>
> Filtering is heterogeneous and often inconsistent, depending on timing, technology, and geographical region. ISPs reportedly take different approaches to the placement of filtering devices, which are not only in border routers, but also in the backbone and even in

[53] Human Rights in China, "How the Chinese Authorities View the Internet: Three Narratives," China Rights Reform Issue No. 2 (2010), http://www.hrichina.org/crf/article/3240.
[54] King, Pan, Roberts "How Censorship in China Allows Government Criticism but Silences Collective Expression."
[55] "In Tandem with Slower Economy, Chinese Internet Users Face Slower Internet This Week," *China Tech News*, November 6, 2012, http://www.chinatechnews.com/2012/11/06/18835-in-tandem-with-slower-economy-chinese-internet-users-face-slower-internet-this-week.
[56] Ben Wagner, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control,'" Global Voices Advocacy, June 25, 2009, http://advocacy.globalvoicesonline.org/2009/06/25/study-deep-packet-inspection-and-internet-censorship/.
[57] The animated cartoon police officers Jingjing and Chacha, who appeared on Chinese computer screens to wag fingers at wayward users around the country in 2008, served as visible reminders of official oversight.
[58] Villeneuve, *Breaching Trust*.

provincial-level internal networks, a development that would potentially allow interprovincial filtering.[59]

China Mobile, China Telecom, and China Unicom extend automated technical keyword filtering to the mobile realm, monitoring text messages and deleting pornographic or other "illegal" content.[60] Users report that their correspondents receive blank messages in place of subject matter that contained apparently banned keywords. It is not clear exactly what content triggers deletion.[61]

The blanket blockage of select web applications isolates the Chinese public from an international network of user-generated content—and domestic internet firms from competition. The video-sharing platform YouTube and the social-media sites Facebook, Twitter, Google+, and Foursquare are consistently blocked. Like a number of other services, Twitter was initially available and widely used, then blocked in 2009 in advance of the 20th anniversary of the Tiananmen Square massacre, once its potential for galvanizing collective action became apparent. It remains popular among Chinese users who are familiar with circumvention tools.[62] More recent blocks on applications like Google's cloud storage service, Drive, were effected immediately.[63] Users of other international applications that remain unblocked complain of sporadic disruptions. Users of the online document-sharing service SlideShare, which is owned by the U.S.-based professional networking site LinkedIn, reported it was temporarily inaccessible in July 2012.[64] LinkedIn itself had been blocked for two days in February 2011.[65]

Forced self-censorship by service providers, makes commercial success contingent on compliance with content regulations. International web applications, once blocked, are quickly replaced by homegrown equivalents. Hundreds of millions of users are attracted to these domestic video-sharing websites, social-networking tools, and e-mail services.[66] As part of their licensing requirements, the companies must ensure that banned content is not

[59] X. Xu, Z. Mao, and J. Halderman, "Internet Censorship in China: Where Does the Filtering Occur?" *Passive and Active Measurement*, Springer, 2011, 133–142, http://pam2011.gatech.edu/papers/pam2011--Xu.pdf.
[60] "China Mobile Users Risk SMS Ban in Porn Crackdown," *Agence France-Presse*, January 13, 2010, http://www.google.com/hostednews/afp/article/ALeqM5jF6dl0QS_1q8Eub7W73BSRNwdJWQ; Elaine Chow, "So About that Sexting Ban in China," *Shanghaiist*, January 20, 2012, http://shanghaiist.com/2010/01/20/okay_so_that_sexting_ban_in_china.php.
[61] Elaine Chow, "An Alleged List of Banned SMS Terms from China Mobile and Co.," *Shanghaiist*, January 4, 2011, http://shanghaiist.com/2011/01/04/an_alleged_list_of_banned_sms_terms.php#photo-1.
[62] Rebecca MacKinnon, "China Blocks Twitter, Flickr, Bing, Hotmail, Windows Live, etc. Ahead of Tiananmen 20th Anniversary," CircleID, June 2, 2009, http://www.circleid.com/posts/20090602_china_blocks_twitter_flickr_bing_hotmail_windows_live/
[63] Steven Musil, "Google Drive Crashes into China's Great Firewall," *Cnet*, April 25, 2012, http://news.cnet.com/8301-1023_3-57421540-93/google-drive-crashes-into-chinas-great-firewall/.
[64] "LinkedIn's SlideShare Blocked in China," *China Media Bulletin*, July 19, 2012, http://www.freedomhouse.org/cmb/65_071912#3.
[65] Keith B. Richburg, "Nervous Unrest, Chinese Authorities Block Web Site, Search Terms," *Washington Post,* February 25, 2011, http://www.washingtonpost.com/world/nervous-about-unrest-chinese-authorities-block-web-site-search-terms/2011/02/25/ABPdw5I_story.html.
[66] Rick Martin, "Ogilvy's 'Social Media Equivalents' in China 2011," *Tech in Asia*, October 17, 2011, http://www.penn-olson.com/2011/10/17/china-social-media/.

posted or circulated; those that fail risk temporary or permanent closure.[67] Software for both censorship and surveillance is often built into their applications. For example, instant-messaging services such as Tom-Skype and QQ include programming that downloads updated keyword blacklists regularly.[68]

In addition to automated keyword filters, human censors delete postings on blogs, microblogs, comment sections of news items, and bulletin-board system (BBS) discussions before they appear to the public or shortly thereafter.[69] Experts say staff receive as many as three censorship directives per day by text message, instant message, phone call, or e-mail.[70] Local propaganda offices recruit volunteers to identify and report potentially undesirable content on social networks.[71]

Online news portals that operate without a press license are limited to reposting content that has already been approved by censors, rather than producing their own.[72] Propaganda directives to internet-based outlets often include specific instructions to amplify content from state media.[73] The search engine Baidu, which accounts for nearly 80 percent of China's search market,[74] similarly manipulates the results it offers based on government instructions, not only removing proscribed material, but also favoring state-approved information over content from nongovernmental or foreign sources. In July 2012, after internet users began circulating short documentary-style videos on social networks to avoid restrictions on news broadcasts and movies, regulators ordered online video service providers to start deleting any items that failed adhere to "correct guidance," a euphemism for censorship orders.[75]

---

[67] One, Fanfou, lost market share after a 2009 shutdown lasted several months. Melanie Lee, "Clampdown Rumored as Chinese 'Twitter' Sites Blocked," *Globe and Mail*, August 23, 2012, http://m.theglobeandmail.com/technology/clampdown-rumored-as-chinese-twitter-sites-blocked/article1368400/?service=mobile.

[68] TOM-Skype is a joint venture between Skype and Chinese wireless service TOM Online. Vernon Silver, "Cracking China's Skype Surveillance Software," Bloomberg, March 8, 2013, http://www.businessweek.com/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it; Jedidah R. Crandall et al., "Chat Program Censorship and Surveillance in China: Tracking TOM-Skype and Sina UC," *First Monday* 18, no. 7 (2013), http://firstmonday.org/ojs/index.php/fm/article/view/4628/3727; Jeffrey Knockel, "TOM-Skype Research," http://cs.unm.edu/~jeffk/tom-skype/.

[69] King, Pan, and Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression."

[70] Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space," Congressional-Executive Commission on China, November 17, 2011, http://1.usa.gov/19dzOZn.

[71] "*Web 3.0 Yuan Nian De Zhong Guo Hu Lian Wang Hang Ye Zi Lv Shi Jian Yu Xi Kao*" [Self-Disciplined Practice and Thoughts of Chinesse Internet Industry in Web 3.0], *Wenming.cn*, April 2011, http://www.wenming.cn/xwcb_pd/yjpl/201104/t20110407_142975.shtml; "*Beijing Zhao Mu Wang Luo Jian Du Zhi Yuan Zhe*" [Beijing to Recruit Volunteers for Network Monitoring], *Beijing News*, May 26, 2012, .

[72] "Interim Provisions on the Administration of Internet Websites Engaged in News Posting Operations," November 1, 2000, excerpts available at http://www.cecc.gov/pages/virtualAcad/exp/explaws.php.

[73] Keith B. Richburg, "Chinese Editors, and a Web Site, Detail Censors' Hidden Hand," *Washington Post*, April 13, 2011, http://www.washingtonpost.com/world/chinese-editors-and-a-web-site-detail-censors-hidden-hand/2011/04/01/AFpMiRSD_story.html.

[74] Phil Berlowitz, "Baidu Revenue and Profit Growth Rate Slow in Fourth Quarter," *Reuters*, February 4, 2013, http://www.reuters.com/article/2013/02/04/us-baidu-results-idUSBRE91310020130204.

[75] "Regulators Announce New Restrictions on Online Video," *China Media Bulletin*, July 12, 2012, http://www.freedomhouse.org/cmb/64_071212#2.

Microblogging services, offered by Sina, Tencent, Sohu, and other companies, saw an astonishing 300 percent growth during their peak development period from 2010 to 2011. With more than half of China's internet users registered for a microblog account by January 2013,[76] these fast-paced networks and their rambunctious user base pose a unique challenge to censors trying to rein in sensitive discussion. The CCP established party branches in the offices of four microblog providers in February 2012, according to news reports.[77] Company executives also benefit from political connections and patronage.[78]

Sina Weibo, benefiting in part from the vacuum left by the 2009 ban on Twitter, had accumulated 400 million registered accounts by November 2012,[79] though only 46 million are active.[80] Unlike on Twitter, Weibo users can develop elaborate discussion threads in response to each post, all of which are lost if the original post is censored. The comment function can also be independently shut off to prevent isolated posts from gaining traction.[81]

Sina employs both automated and human monitors to manage Weibo content. Their methods include deleting individual posts or accounts, often with 24 hours of an offending post, but sometimes long after publication;[82] making published posts visible only to the account owner; and sending personal warnings.[83] In addition, researchers counted over 800 terms filtered from Weibo search results at various times, including "Cultural Revolution" and "propaganda department."[84] Activists and other users with large followings come under particular scrutiny.[85]

---

[76] Not all accounts are active. "*Di 31 Ci Zhongguo Hulianwangluo Zhuangkuang Tongji Baogao*" [The 31st Statistical Report on China's Internet Development," China Internet Network Information Center, January 15, 2013, http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201301/t20130115_38508.htm.

[77] Qiao Long, "CCP Proposes Cells for Microblogs," *Radio Free Asia*, February 7, 2012, http://www.rfa.org/english/news/china/microblogs-02072012175742.html.

[78] "Tech Company Leaders Join Legislative, Advisory Bodies," *China Media Bulletin*, March 7, 2013, http://www.freedomhouse.org/cmb/82_030713#3.

[79] Josh Ong, "China's Sina Weibo Passes 400m Users, Acknowledges Pressure from Rival Tencent's WeChat," *The Next Web*, November 16, 2012, http://thenextweb.com/asia/2012/11/16/sina-books-152-million-in-q3-revenue-as-it-faces-tough-competition-from-tencents-wechat/.

[80] Gady Epstein, "Small Beginnings: Microblogs are a Potentially Powerful Force for Changes, But They Have to Tread Carefully," Economist, April 6, 2010, http://www.economist.com/news/special-report/21574632-microblogs-are-potentially-powerful-force-change-they-have-tread.

[81] Gady Epstein, "The Great Firewall: The Art of Concealment," *The Economist*, April 6, 2013, http://econ.st/145qZuP.

[82] Keith B. Richburg, "China's 'Weibo' Accounts Shuttered as Part of Internet Crackdown," *Washington Post*, January 3, 2013, http://www.washingtonpost.com/world/chinas-weibo-accounts-shuttered-as-part-of-internet-crackdown/2013/01/03/f9fd92c4-559a-11e2-89de-76c1c54b1418_story.html.

[83] Xiao, "From 'Grass-Mud Horse' to 'Citizen.'"

[84] Xiao, "From 'Grass-Mud Horse' to 'Citizen.'" See also Tao Zhu et al., "The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions," Paper for 22nd USENIX Security Symposium in Washington D.C. in August 2013, http://arxiv.org/ftp/arxiv/papers/1303/1303.0597.pdf; King-wa Fu and Michael Chu, "Reality Check for the Chinese Microblog Space: A Random Approach," *PLoS ONE*, Volume 8(3), 2013, http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0058356#pone.0058356-China1.

[85] David Bandurski, "Brutality and Tragedy Unseen," China Media Project, February 1, 2012, http://cmp.hku.hk/2012/02/01/18380/;
David Bandurski, "Thank Goodness for Hong Kong," China Media Project, January 31, 2012, http://cmp.hku.hk/2012/01/31/18311/.

Despite these efforts, the company has frequently fallen afoul of propaganda authorities. When the CCP's purge of Chongqing party chief Bo Xilai in early 2012 prompted unconfirmed online reports of a failed coup, comment functions were temporarily disabled on both Sina and Tencent microblogs. State media reported that the companies were "punished for allowing rumors to spread."[86] Sina subsequently closed several accounts for alleged rumor-mongering.[87] It also launched new user guidelines and a points-based system that assigned demerits to users who published banned content, leading to warnings and eventual account closure, while rewarding those who engaged in unspecified "promotional activities."[88] The intervention may have taken a toll on the company's market share. Rival microblog service Tencent announced 540 million registered users—with 100 million active daily—at the end of 2012.[89]

Foreign service providers must agree to self-censor in return for access to the immense Chinese market, and most comply. In 2012, New Tang Dynasty Television—a Chinese-language, New York–based broadcaster established by Falun Gong practitioners—reported that U.S. technology giant Apple had removed applications created by the station from its online App Store in China in July, on the grounds that their content was "illegal in China."[90] In Chinese-language versions of Apple's voice-controlled artificial intelligence system Siri, the system reportedly declined to answer questions related to the Tiananmen Square massacre, such as a query about "June," and in one test it refused even to direct the user to Tiananmen Square.[91] China accounted for 20 percent of Apple's sales in the first quarter of 2012, and the country is its second-biggest market after the United States.[92]

International service providers that refuse to censor content face an uncertain future. In 2010, Google lost significant market share when it began redirecting mainland users to its uncensored Hong Kong–based search engine. The company explained that it had made the decision after suffering sustained attacks on its intellectual property by military-grade hackers traced to Chinese computers.[93] By doing so publicly, and drawing attention to the way the same hackers had targeted Gmail accounts used by journalists and human rights

[86] "China's Major Microblogs Suspend Comment Function to 'Clean up Rumors,'" *Xinhua News*, March 31, 2012, http://english.peopledaily.com.cn/90882/7775525.html.
[87] "Boxun News Site Attacked Amid Bo Xilai Coverage," Committee to Protect Journalists, April 25, 2012, http://cpj.org/2012/04/boxun-news-site-attacked-amid-bo-xilai-coverage.php.
[88] Experts believe "promotional activities" involve reporting other users or promoting progovernment content. See, "China," OpenNet Initiative, August 9, 2012, https://opennet.net/blog/2012/05/sina-weibo-updates-user-contract-more-content-restrictions; "Sina Weibo Introduces 'User Contract,'" *Caijing*, May 9, 2012, http://english.caijing.com.cn/2012-05-09/111842544.html.
[89] "Tencent Microblog Registered User Base Hits 540 Mln," *Yangcheng Evening News*, January 21, 2013, available at http://www.marbridgeconsulting.com/marbridgedaily/archive/article/62820/tencent_microblog_registered_user_base_hits_540_mln#When:12:00:00Z.
[90] "LinkedIn's SlideShare Blocked in China," *China Media Bulletin*, July 19, 2012, http://www.freedomhouse.org/cmb/65_071912#3.
[91] "Apple's Digital Assistant Flunks Test on Taboo Topics," *China Media Bulletin*, June 21, 2012, http://www.freedomhouse.org/cmb/61_062112.
[92] Bruce Einhorn, "Apple vs. Google: Starkly Different China Experiences," *Bloomberg Businessweek*, June 12, 2012, http://www.businessweek.com/articles/2012-06-12/apple-and-google-are-having-very-different-china-experiences.
[93] David Drummond, "A New Approach to China," Google blog, January 12, 2012, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

activists focused on China issues, it also increased transparency about censorship.[94] Google retained its Chinese license and continued its less politically sensitive operations, like the AdSense advertising service and the Android mobile operating system, largely unimpeded.[95] Yet its flagship search engine has foundered in comparison with domestic competitors. In 2012, it began notifying Chinese users on which keywords were likely to trigger connectivity problems.[96] By 2013, it had turned off this notification function, which some users reported was itself subject to censorship.[97] If private companies choose not to alert readers about blocked content, censorship decisions remain both arbitrary and opaque. There are no formal avenues for appeal.

Chinese companies expanding overseas may have difficulty serving users accustomed to fewer online controls. In 2012, users of Tencent's messaging program WeChat complained that the service was applying China's censorship rules in Singapore and Thailand.[98]

Proactive manipulation is the third primary method of content control in China, and Chinese authorities view cyberspace as a field for "ideological struggle."[99] Since 2005, propaganda units at all levels have trained and hired web commentators to post progovernment remarks and lead online discussions.[100] They also report users who have posted offending statements, target government critics with negative remarks, or deliberately muddy the facts of a particular incident, such as an account of police abuse.[101] Recent reports estimate the number of paid propaganda workers in the tens of hundreds of thousands.[102] These methods are not always effective. Many commenters are more concerned about filling their quota and impressing their bosses than mounting a convincing argument, and web users are wary of content manipulation. Companies also pay for positive comments to promote their products —known in public relations circles as astroturfing— which further erodes public trust in online content.[103]

---

[94] Alexandra Stevenson, "Google's China Market Share: Declining," *Beyondbrics* (blog), *Financial Times*, April 22, 2011, http://blogs.ft.com/beyond-brics/2011/04/22/googles-china-market-share-declining/#axzz2Kj0UxcN8.
[95] Loretta Chao, "Chinese Regulators Renew Key License for Google," *Wall Street Journal*, September 7, 2011, http://online.wsj.com/article/SB10001424053111904836104576556203077777200.html.
[96] Alan Eustace, "Better Search in Mainland China," *Inside Search* (blog), Google, May 31, 2012, http://insidesearch.blogspot.co.uk/2012/05/better-search-in-mainland-china.html.
[97] "Google Turns Off China Censorship Warning," *BBC*, January 7, 2013, http://www.bbc.co.uk/news/technology-20932072.
[98] "China's Tencent Accused of Censoring App Users Abroad," *China Media Bulletin*, January 24, 2013, http://www.freedomhouse.org/cmb/78_012413#5.
[99] Oiwan Lam, "China: The Internet as an Ideology Battlefield," Global Voices Advocacy, January 6, 2010, http://advocacy.globalvoicesonline.org/2010/01/06/china-internet-as-an-ideology-battlefield/.
[100] David Bandurski, "Internet Spin for Stability Enforcers," China Media Project, May 25, 2010, http://cmp.hku.hk/2010/05/25/6112/.
[101] Propaganda workers are colloquially known as the 50 cent party, after the amount they are reportedly paid per post, though recent reports put the going rate as low as 10 cents, while some commentators may be salaried employees. See, Perry Link, "Censoring the News Before It Happens," *New York Review* (blog), *The New York Review of Books*, July 10, 2013, http://www.nybooks.com/blogs/nyrblog/2013/jul/10/censoring-news-before-happens-china/, and Rongbin Han, "Manufacturing Consent in Censored Cyberspace: State-Sponsored Online Commentators on Chinese Internet Forums," Paper for Annual Meeting of America Political Science Association, New Orleans, August 31-September 2, 2012, http://ssrn.com/abstract=2106461.
[102] Perry Link, "Censoring the News Before It Happens."
[103] Rongbin Han, , "Manufacturing Consent in Censored Cyberspace."

> Government employees also engage citizens in online discussions. In 2012, an official Sina report said 50,000 Weibo accounts were operated by government ministries and public officials.[104] Even Hu Jintao, who famously avoided unscripted encounters with the press during his presidency, engaged a cherry-picked audience of *People's Daily* readers in a live web chat in 2008.[105]
>
> The past year also offered an intriguing glimpse of CCP officials apparently wielding censorship tools against their opponents within the party ahead of the leadership shuffle. In mid-2012, Baidu returned fleetingly open results related to the 1989 crackdown and other human rights abuses associated with former president Jiang Zemin and his supporters. Observers speculated that President Hu's rival CCP faction was relaxing controls to embarrass its adversaries.[106] Meanwhile, leftist websites that had been supportive of Bo and his neo-Maoist rhetoric were shut down after his ouster.[107]

Despite the technical filtering, enforced self-censorship, and manipulation, the internet is a primary source of news and forum for discussion, particularly among the younger generation. Chinese cyberspace is replete with online auctions, social networks, homemade music videos, a large virtual gaming population,[108] and spirited discussion of some social and political issues. Overtly political organizations, ethnic minorities, and persecuted religious groups remain underrepresented, though they have used the internet to disseminate banned content, and overseas media and human rights groups report sending e-mail to subscribers in China with news, instructions on circumvention technology, or copies of banned publications. Civil society organizations involved in charity, education, health care, and other social and cultural issues often have a vigorous online presence.

The word "netizen"—a direct translation of the Chinese wangmin, or citizen of the internet—conveys the legitimate sense of civic engagement associated with online exchanges. Microblogs have amplified these dynamics and generated a strong sense of empowerment among many Chinese users, censorship notwithstanding.[109] Whereas Chinese citizens traditionally trek to the seat of power to present their grievances, microblogs and other internet technologies offer a way to overcome the geographic, financial, and physical challenges of such petitioning. Moreover, despite

---

[104] "*Shou Fen Bu Wei Weibo Yun Ying Bao Gao Mian Shi Zhuan Jia Jian Yi Bu Yi Guo Du Mai Meng* ," [The First Microblog of Government Ministry is Published. Experts Advise That It Should Not Be Overused], *Xinhua News*, August 25, 2012, http://news.xinhuanet.com/politics/2012-08/25/c_112842885.htm.

[105] The chat was an example of top leaders' efforts to avoid unscripted interactions. While *People's Daily* readers already represent a self-selecting group likely to support the CCP, news reports said many of the chat's participants were paid. David Bandurski, "FEER: China's Guerrilla War for the Web," China Media Project, July 7, 2008, http://cmp.hku.hk/2008/07/07/1098/.

[106] "Users Report Fleeting Censorship Gaps on Taboo Topics," *China Media Bulletin* March 29, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-52#Users%20report.

[107] "Microblog Comments Suspended to Allow Rumor 'Cleansing,'" *China Media Bulletin*, April 12, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-53#2.

[108] China's online gaming culture is regulated by contradictory controls. Game consoles were banned in 2000, ostensibly for health reasons, but some 120 million Chinese players access online games via computers and mobile devices. Moreover, the CCP heavily subsidizes the production of games that promote ideological themes for propaganda purposes. Some 2013 reports said the Ministry of Culture was planning to lift the console ban. Malcom Moore, "China Embraces Online Gamers," *Telegraph*, January 20, 2013, http://www.telegraph.co.uk/news/worldnews/asia/china/9814114/China-embraces-online-gamers.html.

[109] David Barboza, "Despite Restrictions, Microblogs Catch On in China," *New York Times*, May 15, 2011, http://www.nytimes.com/2011/05/16/business/global/16blogs.html.

the leadership's dread of collective action, officials frequently yield to public pressure. Weibo users forced the authorities to start addressing air pollution in 2013 by raising their concerns in multiple cities and provinces.[110] In January, the CCP dismissed leftist Central Compilation and Translation Bureau Director Yi Junqing after an ex-lover blogged about their affair, drawing widespread opprobrium, in what the *New York Times* characterized as the latest in a "spate of scandals appearing online."[111]

Online protests against official wrongdoing have gained considerable momentum and media visibility in the microblog era. One county-level party chief allegedly removed his expensive watch before appearing in photographs with Premier Li Keqiang in April 2013, perhaps to avoid becoming the latest local cadre to be censured for luxury spending. Internet users caught the tan line on his wrist and quickly found earlier photos that showed him with what seemed to be a designer timepiece.[112] In 2012, the story of a journalist's suspension for exposing officials' luxury cigarette habit in the city of Wei'an, published on his personal microblog, drew more attention than his original report.[113] Also that year, Chinese netizens expressed outrage over a case of compulsory abortion after photographs were posted online.[114] Censors do intervene if these stories and campaigns gain too high a profile or implicate overall CCP governance. After a disastrous storm in Beijing in mid-2012, resident microblog users complained about official rescue efforts and expressed fury when the municipality solicited donations for disaster relief. These comments were deleted in the tens of thousands, and flood-related search terms were blocked, despite an obvious threat to public safety.[115]

The transformative effect of online activism in China is undeniable, and yet the solutions that result from these high-pressure encounters typically fall short of systemic reform or democratic decision making. Consequently, they fail to ensure meaningful accountability.[116] After the Beijing floods, the city's mayor announced his resignation, but he was quickly promoted to Beijing party secretary.[117] One year earlier, a deadly high-speed train collision in Wenzhou was first reported by Weibo users who circulated real-time reports, calls for help, and photos.[118] But in 2012, censors obstructed

---

[110] Epstein, "Small Beginnings."
[111] Madeline Earp, "Shallow Victory for China's Journalists, Protestors," Committee to Protect Journalists, July 5, 2012, http://cpj.org/blog/2012/07/shallow-victory-for-chinas-journalists-protesters.php.
[112] Laura Zhou, "Watch Imprint on Quake Official's Wrist Goes Viral on Internet," *South China Morning Post*, April 24, 2013, http://www.scmp.com/news/china/article/1221756/watch-imprint-quake-officials-wrist-goes-viral-internet.
[113] Earp, "Shallow Victory for China's Journalists, Protestors."
[114] "Forced Abortion Stirs Netizen Outcry, Husband Missing after Interview," *China Media Bulletin*, June 28, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-62#2.
[115] "Beijing Flood Criticism Erupts Online amid Media Controls," *China Media Bulletin*, June 26, 2012, http://www.freedomhouse.org/cmb/66_072612#3.
[116] According to one study, censors stopped blocking names of villages whose residents were protesting as soon as traditional media reported on the provincial authorities' response, even though tensions had not yet fully died down and the effectiveness of the response had yet to be shown. In other words, reports on protests in the context of an ostensibly benevolent response from party officials are not perceived as a threat worthy of censorship. See, "Finish Study Analyzes Keyword Censorship during Mass Incidents," *China Media Bulletin* December 13, 2012, http://www.freedomhouse.org/cmb/77_121312#5.
[117] Gong Lei, "Beijing Gets New Party Chief," Xinhua, July 3, 2012, http://bit.ly/MH2XOG.
[118] Sharon LaFraniere, "China Finds More Bodies, and a Survivor, in Trains' Wreckage," *New York Times*, June 25, 2011, http://www.nytimes.com/2011/07/26/world/asia/26wreck.html; Michael Wines and Sharon LaFraniere, "Baring Facts of Train Crash, Blogs Erode China Censorship," *New York Times*, June 28, 2011, http://nyti.ms/nksiVy; "Train Crash Cover-Up Fuels Public Outrage," *China Media Bulletin*, July 28, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-31#1.

news coverage of the anniversary, and a promised investigation into the cause of the disaster had yet to contact its victims.[119]

Mobilization can also have a negative impact. Online thugs terrorizing officials for alleged corruption may look like a positive development, until the same forces attack ordinary internet users over a perceived insult. Nationalism and xenophobia are prominent components of Chinese cyberspace, though censorship targeting rational dissent instead of inflammatory discourse arguably magnifies their impact. In September 2012, censorship directives were either withheld or ignored following anti-Japanese protests linked to China's territorial dispute with Japan over the uninhabited Diaoyu or Senkaku Islands in the East China Sea. Many commentators interpreted the lack of censorship as a tacit endorsement of the protests, which escalated and turned violent until censors reentered the fray with a modulated message that successfully curtailed news coverage and discussion.[120] But the rioters are as likely to have influenced policymakers as any of the other competing military and foreign affairs agendas during the crisis because of the domestic security implications if they were not contained, according to the Canberra-based scholar Geremie Barmé.[121]

As high-profile events like these draw more attention to China's pervasive information controls, censors find themselves pitted against not just political activists, but also ordinary citizens. It is common for users to counter censorship with humorous neologisms that substitute for banned keywords.[122] This forces censors to work overtime, temporarily filtering seemingly innocuous vocabulary like "river,"[123] "tomato,"[124] or "porridge."[125] These overactive controls impinge further on daily life—jasmine flower sales, for instance, were affected when the word "jasmine" was blocked due to its association with Tunisia's 2011 democratic revolution[126]—and inspire further acts of creative online rebellion. This version of the Chinese internet does not resemble a repressed information environment so much as "a quasi-public space where the CCP's dominance is being constantly exposed, ridiculed, and criticized, often in the form of political satire, jokes, videos, songs, popular poetry, jingles, fiction, Sci-Fi, code words, mockery, and euphemisms."[127]

---

[119] Madeline Earp, "Propaganda Officials Miss the Boat on 'China's Katrina,'" Committee to Protect Journalists, July 26, 2012, http://cpj.org/blog/2012/07/propaganda-officials-miss-the-boat-on-chinas-katri.php.

[120] William Wan, "Chinese Government Both Encourages and Reins in Anti-Japan Protests, Analysts Say," *Washington Post*, September 17, 2012, http://wapo.st/S3yKgK.

[121] "The Chinese government […] was pushed into certain directions […] and saying, "If we go in such a direction, the masses will attack the Public Security Bureau, and the foreign affairs ministry and the army—we'll just go with the masses. And that's an extraordinary development."" "A Discussion with Geremie R. Barme," *Sinica Podcast*, March 8, 2013, http://popupchinese.com/lessons/sinica/a-discussion-with-geremie-r-barme.

[122] Brook Larmer, "Where an Internet Joke Is Not Just a Joke," *New York Times*, October 26, 2011, http://www.nytimes.com/2011/10/30/magazine/the-dangerous-politics-of-internet-humor-in-china.html.

[123] The surname of former Chinese leader Jiang Zemin means "river."

[124] The Chinese word for "tomato" is a homonym for the phrase "western red city," a reference to Chongqing and its purged party boss, Bo Xilai. Madeline Earp, "Chinese Censors Target Tomatoes amid Bo Xilai Scandal," Committee to Protect Journalists, July 5, 2012, http://cpj.org/blog/2012/04/chinese-censors-target-tomatoes-amid-bo-xilai-scan.php.

[125] "Porridge" evoked the *Southern Weekly* anticensorship protest by referring to a common southern Chinese delicacy.

[126] Andrew Jacobs, "Catching Scent of Revolution, China Moves to Snip Jasmine," *New York Times*, May 10, 2011, http://www.nytimes.com/2011/05/11/world/asia/11jasmine.html.

[127] Xiao, "From 'Grass-Mud Horse' to 'Citizen.'"

The number of internet users who challenge information controls to access political content—rather than to download pornography or pirated movies—appears to be growing. Exact numbers of people actively combatting censorship are difficult to calculate. Internet expert Xiao Qiang put the activist community at two or three million in a mid-2013 estimate.[128] Others look for indicators like the number of Chinese users who continue to access Twitter, which can only be reached via circumvention software since its 2009 ban. However, those counts vary wildly, from thousands to 35 million; experts have dismissed the latter as vastly inflated.[129]

The ad hoc techniques these users commonly adopt to flout censors include opening multiple blogs on different hosting sites and circulating banned information directly through peer-to-peer networks, which bypass central servers. Text transformed into image, audio, or video files evades keyword sensors. Software developers, both domestic and overseas, also offer technologically sophisticated tools like virtual private networks (VPNs), which direct the user's traffic—usually using an encrypted connection—through a server outside the firewall to circumvent technical filtering.

International news reports noted spikes in usage of these tools at politically important moments in early 2012—such as Bo Xilai's ouster—when heavy censorship was in place.[130] Circumvention tool developers independently corroborated this for Freedom House. Significantly, developers said the baseline number of users increased as first-time users who adopted the tools during a crisis continued to use them, even after it dissipated.[131]

The growth in the use of such tools has spawned attempts to block them. In 2011, internet security experts noticed activity indicating that Chinese ISPs may have been testing a new system for identifying the type of encrypted services often used by circumvention tools.[132] By December 2012, China Unicom was reportedly cutting connections when it detected VPN usage.[133] Even when not actively disrupted, encryption may attract surveillance. While dozens of China-based companies, as well as overseas firms, promote an evolving roster of commercial circumvention tools, not all are transparent about user privacy. In the words of internet freedom expert Rebecca Mackinnon, "most people are focused simply on accessing banned websites and aren't thinking about surveillance."[134] This leaves a growing community vulnerable to invasive rights violations.

---

[128] Rebecca MacKinnon, "The Shawshank Prevention," *Foreign Policy*, May 2, 2012, http://www.foreignpolicy.com/articles/2012/05/02shawshank_prevention?page=full&wp_login_redirect=0.
[129] Jason Q. Ng, "There Are NOT Millions of Twitter Users in China: Supporting @ooof's Result and Refuting GWI's Conclusion," *Blocked on Weibo* (blog), January 6, 2013, http://blockedonweibo.tumblr.com/post/39828699303/there-are-not-millions-of-twitter-users-in-china; Jon Russell, "No, Facebook Does Not Have 63.5 Million Active Users in China," The Next Web, September 28, 2012, http://thenextweb.com/asia/2012/09/28/no-way-jose/.
[130] MacKinnon, "The Shawshank Prevention."
[131] E-mail communication with circumention tool developer who requested anonymity, June 2012.
[132] Sharon LaFraniere and David Barboza, "China Tightens Censorship of Electronic Communications," *New York Times*, March 21, 2011, http://www.nytimes.com/2011/03/22/world/asia/22china.html; Andy Greenberg, "China's Great Firewall Tests Mysterious Scans on Encrypted Connections," *Forbes*, November 17, 2011, http://onforb.es/u9pxP2.
[133] Charles Arthur, "China Tightens 'Great Firewall' Internet Control with New Technology," *Guardian*, December 14, 2012, http://www.guardian.co.uk/technology/2012/dec/14/china-tightens-great-firewall-internet-control.
[134] MacKinnon, "The Shawshank Prevention."

VIOLATIONS OF USER RIGHTS

VIOLATIONS OF USER RIGHTS: KEY FINDINGS
MAY 2012-APRIL 2013

A 2012 amendment to the Criminal Procedure Law took effect in January 2013. While not all its provisions were negative, the amendment did appear to strengthen the legal grounds for detaining suspects incommunicado if they were suspected of anti-state activity—a category that includes individuals like Cao Haibo, a cybercafé employee sentenced in a closed trial in November 2012 to eight years in jail for discussing democracy online. Other online activists faced physical attacks, interrogation and house arrest.

Many were deprived of due process: After 2013 unrest in Xinjiang, at least twenty individuals were sentenced because they "used the Internet, mobile phones and digital storage devices" to incite terrorism, local reports alleged, without elaborating. Also in 2013, as international concern at the rising number of self-immolations in Tibet mounted, the *Times* reported at least a dozen Tibetans detained for inciting and publicizing suicides, including sending photographs of burning bodies overseas via mobile phone. International monitoring groups documented unprecedented levels of surveillance targeting Tibetans, including searches of mobile devices. Police surveillance powers were bolstered by new rules encouraging users to register their real names online in December 2012. Some Beijing businesses offering internet were told to install government spyware or disconnect.

Several U.S-based media outlets revealed in January 2013 that Chinese hackers had infiltrated their computers and staff email accounts, while analysts traced several hackers operating globally to physical locations in China—in one case, to a specific military location in Shanghai—and revealed an escalation in their technical sophistication. Less well-documented is the exposure faced by Chinese web users. A Chinese military report in May 2012 said nearly 9 million Chinese computers were infected with malicious viruses, while international hackers claimed responsibility for illegally accessing China Telecom's vast stores of personal data.

Article 35 of the Chinese constitution guarantees freedoms of speech, assembly, association, and publication, but such rights are subordinated to the CCP's status as the ruling power. In addition, the constitution cannot, in most cases, be invoked in courts as a legal basis for asserting rights. The judiciary is not independent and closely follows party directives, particularly in politically sensitive freedom of expression cases. China lacks specific press or internet laws, but government agencies

issue a variety of regulations to establish censorship guidelines. Regulations—which can be highly secretive—are subject to constant change and cannot be challenged by the courts.

Prosecutors exploit vague provisions in China's criminal code, laws governing printing and publications, and state secrets legislation to imprison citizens for online activity such as blogging, downloading censored material from overseas, or sharing information by text message, e-mail or social media platforms. Recent legislative amendments fall short of international standards for protecting defendants, and in some cases strengthen police power. In 2010, the National People's Congress amended the State Secrets Law,[135] obliging telecommunications operators and ISPs to cooperate with authorities investigating leaked state secrets or risk losing their licenses.[136] Since authorities can retroactively classify content to justify a prosecution under this law, its formalized extension to the digital realm is deeply problematic. An amendment to the Criminal Procedure Law that took effect in 2013 bolstered the legal grounds for detaining suspects in undisclosed locations in cases pertaining to national security—a category that includes online offenses against the state. It did introduce a review process for allowing police surveillance of suspects' electronic communications, which the Public Security Ministry allows in a range of criminal cases, but the wording of the amendment was vague about the procedure for that review.[137] In addition, local officials periodically use criminal defamation charges to detain and in some cases imprison whistle-blowers who post corruption allegations online.[138]

Trials and hearings lack due process, often amounting to little more than sentencing announcements, and detainees frequently report abuse in custody, including torture and lack of medical attention.[139]

Reporters Without Borders documented a total of 69 netizens in Chinese jails as of February 2013.[140] Individuals sentenced during the coverage period included Cao Haibo, a cybercafé employee who received eight years in jail 2012 for promoting democracy online.[141] Long-term detainees include 2010 Nobel Peace Prize winner Liu Xiaobo, who is serving an 11-year sentence on charges of "inciting subversion of state power" for publishing online articles, including the

[135] "*Zhong Hua Ren Min Gong He Guo Zhu Xi Ling, Di Er Shi Ba Hao*" [Presidential order of the People's Republic of China, No. 28," April 29, 2010, http://www.gov.cn/flfg/2010-04/30/content_1596420.htm.
[136] Jonathan Ansfield, "China Passes Tighter Information Law," *New York Times*, April 29, 2010, http://www.nytimes.com/2010/04/30/world/asia/30leaks.html.
[137] Luo Jieqi, "Cleaning Up China's Secret Police Sleuthing," *Caixin*, January 24, 2013, http://articles.marketwatch.com/2013-01-24/economy/36525447_1_police-abuse-police-investigations-police-officers.
[138] Justin Heifetz, "The 'Endless Narrative' of Criminal Defamation in China," Journalism and Media Studies Centre of the University of Hong Kong, May 10, 2011, http://coveringchina.org/2011/05/10/the-endless-narrative-of-criminal-defamation-in-china/.
[139] See for example, "Tortured, Dissident Christian Lawyer Talks about His Ordeal," *Asianews.it*, September 15, 2011, http://www.asianews.it/news-en/Tortured,-dissident-Christian-lawyer-talks-about-his-ordeal-22641.html; Paul Mooney, "Silence of the Dissidents," *South China Morning Post*, July 4, 2011, http://pjmooney.com/en/Most_Recent_Articles/Entries/2011/7/4_Silence_of_The_Dissidents.html.
[140] "World Report: China," Reporters Without Borders, http://en.rsf.org/report-china,57.html. Unreported cases may put the total number of jailed internet users considerably higher.
[141] "China Internet Cafe Worker Cao Haibo Jailed," *BBC*, November 1, 2012 http://www.bbc.co.uk/news/world-asia-china-20172104 Cao's sentence was reported in November after a May trial.

prodemocracy manifesto Charter 08.[142] Though these represent a tiny percentage of the overall user population, the harsh sentences have a chilling effect on the close-knit activist and blogging community and encourage self-censorship in the broader public.

Members of religious and ethnic minorities face particularly harsh treatment for transmitting information abroad and accessing or disseminating banned content.[143] In the aftermath of ethnic violence in Tibet in 2008 and Xinjiang in 2009, local courts imposed prison sentences on at least 17 individuals involved in websites that reported on Tibetan or Uighur issues, often in closed trials.[144] Many details of the charges and sentences were not reported even to the defendants' families, but at least two Uighur website managers, Memetjan Abdulla and Gulmire Imin, were jailed for life. After more unrest in Xinjiang in 2013, at least 20 individuals were sentenced because they supposedly "used the Internet, mobile phones and digital storage devices to organize, lead and participate in terror organizations, provoke incidents, and incite separatism."[145] Also in 2013, as international concern at the rising number of self-immolations in Tibet mounted, the *New York Times* reported that at least a dozen Tibetans had been detained for allegedly inciting and publicizing the protests, including by sending photographs overseas via mobile phone.[146] A Tibetan-language notice apparently posted by public security officials in Gansu Province warned that circulating banned content including "websites," "emails and audio files," and "SMS texts" would result in severe beating, according to Reporters Without Borders.[147]

Three other extrajudicial measures used to punish internet users are detention in "reeducation through labor" camps, house arrest, and covert detention.

- **Reeducation through labor**
  Public security officials can sentence suspects to up to four years in work camps without trial, an unpopular procedure that has drawn increasing calls for reform.[148] State media have become unusually vocal regarding the system's potential for abuse.[149] In November 2012, Chongqing village official Ren Jiayu, a 25-year-old who had been sentenced to two years' reeducation through labor for pseudonymous microblog comments about Bo Xilai, was

[142] Sharon Hom, "Google and Internet Control in China: A Nexus between Human Rights and Trade?" (testimony, U.S. Congressional-Executive Commission on China, Washington, DC, March 24, 2010), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg56161/pdf/CHRG-111hhrg56161.pdf .
[143] Falun Gong practitioners are often given harsh sentences for online communications, according to Patrick Poon, Executive Secretary and Director of Hong Kong Office of the Independent Chinese PEN Centre, who communicated with Freedom House by e-mail.
[144] "Attacks on the Press in 2011: China," Committee to Protect Journalists, http://www.cpj.org/2012/02/attacks-on-the-press-in-2011-china.php
[145] Chris Buckley, "China Convicts and Sentences 20 Accused of Militant Separatism in Restive Region," *New York Times*, March 27, 2013, http://www.nytimes.com/2013/03/28/world/asia/china-sentences-20-for-separatists-acts-in-restive-region.html.
[146] "Tibetans Held for Mobile-Phone Dalai Lama Images," *China Media Bulletin*, December 6, 2012, http://www.freedomhouse.org/cmb/76_120612#5.
[147] Reporters Without Borders, "Authorities Openly Threaten Those Who Circulate Information with 'Torture,'" news release, March 29, 2012, http://en.rsf.org/chine-authorities-openly-threaten-those-29-03-2012,42216.html.
[148] Dui Hua, "Reform of China's 'Re-Education Through Labor' System is Slow Work in Progress," *Dialogue* no. 36, August 29, 2009, http://duihua.org/wp/?p=2756.
[149] "Victims of Re-education Through Labor System Deserve Justice," *Xinhua News*, January 28, 2013, http://www.globaltimes.cn/content/758696.shtml.

released early after generating widespread online support; the event, and a CCTV interview with the former inmate, attracted over 1.5 million comments on Sina Weibo.[150] This minor success may reflect nothing more than the change in Bo Xilai's political fortunes. In early 2013, however, in a possible prelude to centralized reform, state media reported that provincial authorities in Yunnan and Guangdong were preparing to abolish reeducation through labor.[151] The official Xinhua news agency later backtracked, saying the media had "read too much" into these developments. The status of the reform effort remains unclear; some experts still view a major overhaul as unlikely.

- **House arrest**
  This features invasive surveillance at the detainee's home, where internet and mobile phone connections are often severed to prevent the individual from contacting supporters and journalists. This is apparently intended to reduce external interest in the detainee's welfare, though it can have the opposite effect. Liu Xia, who is married to Liu Xiaobo, has been isolated at home since his incarceration, but this has generated repeated attempts to contact her, and Associated Press journalists evaded her surveillance detail to interview her in 2012.[152] While there are several cases of long-term house arrest, it can be adjusted arbitrarily over time. In September 2012, academic and blogger Jiao Guobiao was first banned from traveling to an overseas conference and placed under strict house arrest for several days, then arrested and detained for two weeks after publishing an online article about the disputed Diaoyu (Senkaku) Islands, and finally released, to continued surveillance.[153] Some groups compile tallies of dissidents known to be held under house arrest, but there are no statistics available to show which of them may have been targeted specifically for their online activity.[154]

- **Covert detention**
  State agents can abduct and hold individuals in secret locations without informing their families or legal counsel. This long-standing practice, which initially lacked a legal foundation, came into the spotlight in 2011 as authorities reacted to the threat of Arab

[150] Oiwan Lam, "China: Campaign to End the Unconstitutional Re-Education Through Labour System," *Global Voices*, October 20, 2012, http://globalvoicesonline.org/2012/10/20/china-campaign-to-end-the-unconstitutional-re-education-through-labour-system/; Abby, "Spotlight on China's 'Re-Education Through Labor,'" *Global Voices*, November 28, 2012, http://globalvoicesonline.org/2012/11/28/spotlight-on-chinas-re-education-through-labour/.
[151] Cao Yin, "Yunnan Puts Laojiao Approvals on Hold," *China Daily*, February 7, 2013, http://usa.chinadaily.com.cn/china/2013-02/07/content_16210279.htm; Huang Jin and Chen Lidan, "Guangdong to Stop Re-education Through Labor System in China," *Xinhua News*, January 30, 2013, http://english.peopledaily.com.cn/90882/8113531.html.
[152] Isolda Morillo and Alexa Olesen, "China Nobel Wife Speaks on Detention," *Associated Press*, December 6, 2012, http://bigstory.ap.org/article/ap-exclusive-detained-china-nobel-wife-speaks-out. International news reports also follow well-known individuals like Tibetan blogger Tsering Woeser, who is periodically placed under house arrest, most recently in June 2013. See, "Tibetan Writer Woeser Again Placed under House Arrest," Radio Free Asia, June 20, 2013, http://www.rfa.org/english/news/tibet/arrest-06202013171541.html.
[153] PEN America, "Writer and ICPC Member Dr. Jiao Guobiao Released," news release, October 1, 2012, http://www.pen.org/rapid-action/2012/10/01/writer-and-icpc-member-dr-jiao-guobiao-released.
[154] "Deprivation of Liberty and Torture/Other Mistreatment of Human Rights Defenders in China," Chinese Human Rights Defenders (CHRD), June 30, 2013, http://chrdnet.com/wp-content/uploads/2013/03/FOR-WEB_Partial-data-6-30-2013-updt-7-5_VC-7-10-R-2.pdf.

Spring–style protests.[155] Among dozens of cases reported that year, prominent artist and blogger Ai Weiwei was abducted and held from April to June 2011 and subsequently fined for alleged tax evasion.[156] In 2012, as noted above, the National People's Congress enacted an amendment of the Criminal Procedure Law that strengthened the legal basis for detaining suspects considered a threat to national security in undisclosed locations, among other changes. In response to public feedback, a clause was added requiring police to inform a suspect's family of such a detention, though they need not disclose where and why the suspect is being held. Despite this improvement, the amendment maintained vague language that is open to abuse by police and security agents.[157]

Internet users have occasionally fallen victim to forced psychiatric detention, a measure used to commit individuals to mental institutions and prevent them from seeking redress for injustice or engaging in other unwelcome behavior. The whereabouts of at least one detainee, Li Qidong, who officials hospitalized in Liaoning in 2009 after he criticized the government in online articles, are not known.[158]

Law enforcement officials frequently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically online as "being invited for tea."[159] Activists have also been instructed to travel during times of political activity or heightened public awareness of their cause. Security agents sent photojournalist Li Yuanlong on a "forced vacation" from his native Guizhou Province in 2012, after he published shocking photographs of children who had died of exposure on a popular website, prompting calls for accountability from local schools and officials.[160]

Internet users sporadically report encountering violence as a result of online activity. In August 2012, masked men raided the offices of a Hong Kong citizen-journalism platform and destroyed computers, apparently in retaliation for the site's coverage of local politics. Hu Jia, a dissident who

[155] Edward Wong, "Human Rights Advocates Vanish as China Intensifies Crackdown," *New York Times*, March 11, 2011, http://www.nytimes.com/2011/03/12/world/asia/12china.html.

[156] Kate Taylor, "Arts Group Calls for Worldwide Sit-In for Ai Weiwei," *New York Times*, April 14, 2011, http://artsbeat.blogs.nytimes.com/2011/04/14/arts-group-calls-for-worldwide-sit-in-for-ai-weiwei/?scp=9&sq=&st=nyt; Wu Yu, "*Ai Wei Wei Bei Zhi 'Se Qing', Wang Min 'Ai Luo Luo'*" [Ai Weiwei was criticized for pornography, netizens fought back], *Deutsche Welle*, November 19, 2011, http://www.dw-world.de/dw/article/0,,15543929,00.html.

[157] The amendment took effect on January 1, 2013. Observers praised other aspects of the measure, including tentative steps toward increasing police accountability for surveillance "China's New Law Sanctions Covert Detentions," Committee to Protect Journalists, March 14, 2012, http://cpj.org/2012/03/chinas-new-law-sanctions-covert-detentions.php..

[158] Chinese Human Rights Defenders (CHRD), *The Darkest Corners: Abuses of Involuntary Psychiatric Commitment in China* (CHRD, 2012), http://chrd.equalit.ie/wp-content/uploads/2012/08/CRPD_report_FINAL-edited2.pdf.

[159] Oiwan Lam, "China: Bloggers 'Forced to Drink Tea' with Police," Global Voices Advocacy, February 19, 2013, http://advocacy.globalvoicesonline.org/2013/02/19/china-bloggers-forced-to-drink-tea-with-police/; Michael Sheridan, "China Offers Its Dissidents Tea and Subtle Tyranny," *Sunday Times*, January 13, 2013, http://www.thesundaytimes.co.uk/sto/news/world_news/Asia/article1193304.ece.

[160] "Photojournalist 'Sent on Holiday' After Covering Death of Five Children," Reporters Without Borders, December 5, 2012, http://en.rsf.org/china-photojournalist-sent-on-holiday-05-12-2012,43764.html.

is active online, reported that security agents beat him during an eight-hour detention in March 2013, on the day before Xi Jinping took office as president.[161]

Users hoping to avoid repercussions for their online activity face a rapidly dwindling space for anonymous communication as real-name registration requirements expand online, among mobile phone retailers, and at public internet facilities. The authorities justify real-name registration as a means to prevent cybercrime, though experts counter that uploaded identity documents are vulnerable to theft or misuse,[162] especially since some verification is done through a little-known government-linked contractor.[163]

In December 2012, the CCP's governing Standing Committee approved new rules to strengthen the legal basis for real-name registration by websites and service providers.[164] The rules threatened violators with "confiscation of illegal gains, license revocations and website closures," largely echoing the informal arrangements already in place across the sector.[165] Comment sections of major news portals, bulletin boards, blog-hosting services, and e-mail providers already enforce some registration.[166] The MIIT also requires website owners and internet content providers to submit photo identification when they apply for a license, whether the website is personal or corporate.[167] Nevertheless, the new rules are significant in extending regulation to the e-commerce and business sectors, which typically benefit from more freedom than their counterparts in the news media, civil society, or academia. The rules oblige these providers to gain consent for collecting personal electronic data, as well as outline the "use, method, and scope" of its collection; yet they offer no protection against law enforcement requests for these records.[168] Chinese providers are required to retain user information for 60 days, and provide it to the authorities upon request without judicial oversight or informing the user.[169]

---

[161] Isaac Stone Fish, "Chinese Dissident Allegedly Beaten as Xi Jinping Becomes President," *Passport* (blog), *Foreign Policy*, March 14, 2013, http://blog.foreignpolicy.com/posts/2013/03/14/chinese_dissident_allegedly_beaten_as_xi_jinping_becomes_president.

[162] Danny O'Brien, "China's Name Registration Will Only Aid Cybercriminals," Committee to Protect Journalists, December 28, 2012, http://www.cpj.org/internet/2012/12/chinas-name-registration-will-aid-not-hinder-cyber.php.

[163] "*Du Zi He Cha Wei Bo Shi Ming Guo Zheng Tong She Long Duan*" [Real-Name Verification of Weibo Suspected Monopolized by Guo Zheng Tong], *Hong Kong Commercial Daily*, December 30, 2011, http://www.hkcd.com.hk/content/2011-12/30/content_2875001.htm; "*Beijing Yao Qiu Wei Bo Yong Shi Ming Fa Yan*" [Beijing Users of Weibo Required for Real-Name Verification], BBC, December 16, 2011, http://bbc.in/t2hZme.

[164] "National People's Congress Standing Committee Decision Concerning Strengthening Network Information Protection," China Copyright and Media, December 28, 2012, http://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/.

[165] Joe McDonald, "China Real-Name Registration Is Now Law in Country," *Huffington Post*, December 28, 2012, http://www.huffingtonpost.com/2012/12/28/china-real-name-registration_n_2373808.html.

[166] "*Wen Hua Bu 2009 Jiang Da Li Zhen Zhi Hu Lian Wang Di Su Zhi Feng*" [Ministry of Culture Will Curb Trend of Internet Indecency in 2009], *Net Bar China*, January 6, 2009, http://www.netbarcn.net/Html/PolicyDynamic/01061954388252.html; Chen Jung Wang, "*Shi Min Zhi Rang Gao Xiao BBS Bian Lian*" [Real Name System Intimidates High School BBS], CNHubei, November 29, 2009, http://www.cnhubei.com/200511/ca936578.htm; "*Zhong Guo Hu Lian Xie Hui: Bo Ke Tui Xing Shi Min Zhi Yi Chen Ding Ju*" [Internet Society of China: Real Name System for Bloggers is Set], *Xinhua News,* October 22, 2006, http://www.itlearner.com/article/3522.

[167] Elinor Mills, "China Seeks Identity of Web Site Operators," *CNET News*, February 23, 2010, http://cnet.co/bXIMCp.

[168] Tim Stratford et al., "China Enacts New Data Privacy Legislation," Publication from Covington & Burling LLP, January 11, 2013, http://bit.ly/RRiMaM.

[169] "China," OpenNet Initiative, August 9, 2012, http://opennet.net/research/profiles/china-including-hong-kong.

Microblog providers have struggled to enforce identity checks. Online reports of Sina Weibo users trading defunct identification numbers to facilitate fake registration indicated that the requirements were easy to circumvent.[170] Sina's 2012 report to the U.S. Securities and Exchange Commission anxiously noted the company's exposure to potentially "severe punishment" by the Chinese government as a result of its failure to ensure user compliance.

When social-media sites offer online payment systems, many users voluntarily surrender personal details to enable financial transactions. Mobile phone purchases have required identification since 2010, so providing a phone number is a common way of registering with other services.[171] In fact, one analyst estimated that approximately 50 percent of microblog users had unwittingly exposed their identities to providers by 2012, simply by accessing the platform from their mobile phone.[172]

Implementation of the real-name policy may continue to vary, not just because it is hard to enforce, but also because registration makes it harder for the state's hired commentators to operate undetected. One study reported that some officials openly encourage commentators to use pseudonyms and fake ID to hide their affiliation with the propaganda department.[173]

Real-name registration is just one aspect of pervasive surveillance of internet and mobile phone communications in place in China. Rapidly developing phone technology offers new opportunities for the surveillance state. A 2011 Beijing city initiative to produce real-time traffic data by monitoring the location of the city's 17 million China Mobile subscribers sparked concern from privacy experts, who said it could be used to trace and punish activists.[174] The timeline for the program's implementation is not known.

The deep-packet inspection technology used to censor keywords can monitor users as they try to access or disseminate similar information. Private instant-messaging conversations and text messages have been cited in court documents. One academic study reported that queries for blacklisted keywords on Baidu automatically sent the user's IP address to a location in Shanghai affiliated with the Ministry of Public Security.[175] Given the secrecy surrounding such capabilities, however, they are difficult to verify.

Police periodically try to force mandatory surveillance software on organizations and individuals, with mixed success. Cybercafés check photo identification and record user activities, and in some

[170] C. Custer, "How to Post to Sina Weibo without Registering Your Real Name," *Tech in Asia*, March 30, 2012, http://www.techinasia.com/post-sina-weibo-registering-real/.
[171] "*Shou Ji Shi Ming Zhi Jin Qi Shi Shi, Gou Ka Xu Chi Shen Fen Zheng*" [Mobile phone real name system implemented today, SIM card purchasers have to present their ID documents], *News 163*, October 1, 2010, http://bit.ly/aIyYL4.
[172] Song Yanwang, " *Jing Hua Wang Luo Huan Jing Xin Gui Yin Huan An Cang Weibo Shi Ming Zhi Ling Yung Ying Shang Mian Lin Da Kao*" [Internet Clean-Up Regulations Conceal Obscure Issues. Weibo's New Real-Name Registration Rule Poses Challenge for Telecom Operator], *Net.China.com.cn*, March 15, 2012, http://net.china.com.cn/txt/2012-03/15/content_4875947.htm.
[173] Rongbin Han, , "Manufacturing Consent in Censored Cyberspace."
[174] "*Beijing Ni Yong Shou Ji Xin Hao Zhui Zong Shi Min Chu Xing Qing Kuang*" [Beijing plans to track mobile phone users in real-time], *Yahoo News*, March 3, 2011, http://news.cn.yahoo.com/ypen/20110303/237829.html; Cecilia Kang, "China Plans to Track Cellphone Users, Sparking Human Rights Concerns," *Washington Post*, March 3, 2011, http://wapo.st/hw6qkg.
[175] Becker Polverini and William M. Pottenger, "Using Clustering to Detect Chinese Censorware," Eleventh Annual Workshop on Cyber Security and Information Intelligence Research, Article No. 30, 2011. Extended Abstract available at: http://www.intuidex.com/whitepapers/CSIIRW_Chinese_Censorship_Paper.pdf.

regions, surveillance cameras in cybercafés have been reported transmitting images to the local police station.[176] However, users successfully resisted attempts at mandatory installation of antipornography software known as Green Dam Youth Escort in 2009, after experts voiced privacy and censorship concerns. Some Beijing companies were threatened with disconnection in 2012 if they failed to install government-designated software capable of logging web traffic, blocking sites, and communicating with local police servers.[177] A similar effort to force businesses offering wireless internet access in Beijing's Dongcheng district to purchase expensive surveillance equipment in 2011 caused some to disconnect rather than pay.[178] Others ignored the directive without repercussions.

As with censorship, surveillance disproportionately targets individuals and groups perceived as antigovernment. Reports citing anonymous government officials noted that a camera grid system known as "Skynet" may have "a camera on every road in Tibet" as part of the effort to contain self-immolations.[179] A Tibetan rights group reported police inspections of mobile phones for banned content in Lhasa in March 2013.[180] A June 2013 report by Human Rights Watch put these activities in the context of a three-year campaign by 5,000 teams of CCP personnel conducting surveillance throughout the Tibetan Autonomous Region.[181]

Beyond regional flashpoints, the national "Safe Cities" program offers security officials an advanced system for monitoring public spaces across China.[182] The "social stability maintenance" budget that supports these programs surpassed China's defense budget in 2012.[183]

Both international and local firms jockey for lucrative surveillance-related equipment contracts in China. During 2011, two lawsuits were filed in U.S. courts against the American technology company Cisco Systems, asserting that there was evidence the firm had customized its surveillance equipment to assist Chinese security agencies in apprehending Falun Gong practitioners and democracy activists. Cisco denied the allegations, and the cases were pending as of May 2013.[184]

---

[176] Naomi Klein, "China's All-Seeing Eye," NaomiKlein.org, May 14, 2008, http://bit.ly/2nf29.

[177] Kevin Voigt, "International Firms Caught in China's Security Web," *CNN*, August 24, 2012, http://edition.cnn.com/2012/08/24/business/china-foreign-companies-internet/index.html.

[178] Zhao Zhuo, "*Beijing Bu Fen Ka Fei Ting Ting Zhi Ti Gong Wu Xian Wang Luo*" [Some cafés in Beijing suspend Wi-Fi service], *Beijing Youth Daily*, July 27, 2011, http://bjyouth.ynet.com/article.jsp?oid=79986791.

[179] Malcolm Moore, "China Using Massive Surveillance Grid to Stop Tibetan Self-Immolation," *Telegraph*, November 9, 2012, http://bit.ly/TgUg0g.

[180] "China Launches Crackdown on Personal Cellphones in Lhasa," Tibetan Centre for Human Rights and Democracy, March 11, 2013, http://www.tchrd.org/2013/03/china-launches-crackdown-on-personal-cellphones-in-lhasa/#more-1288. Radio Free Asia also reported police requisitioning computers and cellphones belonging to Uighur students for inspection when they returned to the region for the school holidays. "Chinese Controls on Uyghur Students Ahead of Ramadan," Radio Free Asia, June 13, 2013, http://www.rfa.org/english/news/china/students-06132013105142.html.

[181] According to Human Rights Watch, the goals of the campaign included "categorizing Tibetans according to their religious and political thinking, and establishing institutions to monitor their behavior and opinions." Human Rights Watch, "China: 'Benefit the Masses' Campaign Surveilling Tibetans," news release, June 19, 2013, http://bit.ly/11Y8EAF.

[182] Andrew Jacobs and Penn Bullock, "Firm Romney Founded Is Tied to Chinese Surveillance," *New York Times*, March 15, 2012, http://www.nytimes.com/2012/03/16/world/asia/bain-capital-tied-to-surveillance-push-in-china.html.

[183] Edward Wong and Jonathan Ansfield, "China's Communist Elders Take Backroom Intrigue Beachside," *New York Times*, July 21, 2012, http://www.nytimes.com/2012/07/22/world/asia/chinas-communist-elders-take-backroom-intrigue-beachside.html.

[184] Somini Sengupta, "Group Says It Has New Evidence of Cisco's Misdeeds in China," *New York Times*, September 2, 2011, http://www.nytimes.com/2011/09/03/technology/group-says-it-has-new-evidence-of-ciscos-misdeeds-in-china.html; "Suit Claims Cisco Helped China Repress Religious Group," *Thomson Reuters News & Insight*, May 20, 2011, http://bit.ly/jxx6ds; Don

Uniview Technologies, a Chinese firm that offers software allowing police to share images between jurisdictions in real time, is owned by the U.S. private equity company Bain Capital.[185]

China is a key global source of cyberattacks, responsible for nearly a third of attack traffic observed by the content delivery network Akamai in a 2012 worldwide survey.[186] The survey traced the attacks to computers in China using IP addresses, meaning the machines themselves may have been controlled from somewhere else. In January 2013, following the precedent set by Google's revelation of hacking in 2010, the *New York Times* announced that Chinese hackers had infiltrated its computer systems and obtained staff passwords in the wake of the paper's censored exposé on wealth amassed by then premier Wen Jiabao's family.[187] The revelation prompted similar reports of hacking from Bloomberg, the *Wall Street Journal*, and the *Washington Post*.[188]

The scale and targets of illegal cyber activity lead many experts to believe that Chinese military and intelligence agencies either sponsor or condone it, though even attacks found to have originated in China can rarely be traced directly to the state. However, the geographically diverse array of political, economic, and military targets that suffer attacks reveal a pattern in which the hackers consistently align themselves with Chinese national goals. In one 2012 example, the *Indian Express* reported that hackers based in China had targeted computer systems of India's Eastern Naval Command headquarters in Visakhapatnam.[189] The most convincing documentation of a state connection was reported by U.S.-based cybersecurity firm Mandiant in February 2013, after the company traced sophisticated attacks on American intelligence targets to a military unit in Shanghai.[190]

Hackers, known in Chinese online circles as *heike* (dark guests), employ various methods to interrupt or intercept online content. Both domestic and overseas groups that report on China's human rights abuses have suffered from distributed denial-of-service (DDoS) attacks, which temporarily disable websites by bombarding host servers with an unmanageable volume of traffic. In a development that echoes the trajectory of China's overall information control, hackers increasingly intimidate service providers into cooperating with them. A massive DDoS attack on the exile-run Chinese-language news website Boxun in 2012 threatened the entire Colorado-based hosting company, name.com, and was accompanied by an e-mailed demand that the company

---

Tennant, "Second Lawsuit Accuses Cisco of Enabling China to Oppress Citizens," *IT Business Edge*, June 9, 2011, http://bit.ly/jnXH84; Mark Chandler, "Cisco Supports Freedom of Expression, an Open Internet and Human Rights," *The Platform* (blog), Cisco, June 6, 2011, http://bit.ly/I8fgeh.

[185] Jacobs and Bullock, "Firm Romney Founded Is Tied to Chinese Surveillance."

[186] Akamai, 3rd Quarter 2012 Executive Summary.

[187] Nicole Perlroth, "Hackers in China Attacked the Times for Last 4 Months," *New York Times*, January 30, 2013, http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

[188] Samuel Wade, "New York Times Hacking Highlights Other Cases," *China Digital Times*, February 1, 2013, http://chinadigitaltimes.net/2013/02/new-york-times-hacking-highlights-other-cases/; Nicole Perlroth, "Washington Post Joins List of News Media Hacked by the Chinese," *New York Times*, February 1, 2013, http://nyti.ms/12gEGZF.

[189] Manu Pubby, "China Hackers Enter Navy Computers, Plant Bug to Extract Sensitive Data," *Indian Express*, July 1, 2012, http://www.indianexpress.com/news/china-hackers-enter-navy-computers-plant-bug-to-extract-sensitive-data/968897/.

[190] David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking against U.S.," *New York Times*, February 18, 2013, http://nyti.ms/XZRMHo.

disable Boxun for good.[191] Name.com resisted and helped Boxun switch servers, but hackers with the power to bring down whole businesses may well find other companies more compliant.

Another well-documented tactic is spear-phishing, in which targeted e-mail messages are used to trick recipients into downloading malicious software by clicking on a link or a seemingly legitimate attachment.[192] In a 2012 analysis, the U.S.-based computer security firm Symantec linked the group responsible for the 2010 Google breach—dubbed "the Elderwood gang" after a signature coding parameter—to a series of "watering hole" attacks, in which the hackers lay in wait for a self-selecting group of visitors to specific websites. The targeted sites included defense companies as well as human rights groups focused on China and Tibet; one of the sites was Amnesty International Hong Kong.[193] Most concerning, according to Symantec, were the gang's frequent "zero day" attacks, which exploit previously unknown vulnerabilities in the source code of programs that are widely distributed by software giants like Adobe and Microsoft. Groups that can pull off these attacks are scarce, since uncovering security loopholes requires huge manpower and technical capability, or internal corporate access to the source code itself. Yet the Elderwood gang "seemingly has an unlimited supply" of zero-day vulnerabilities at its fingertips.

Chinese web users have also been victims of cybercrime perpetrated by hackers both inside and outside the country. Tibetans, Uighurs and other individuals and groups subject to monitoring have been frequently targeted with e-mailed programs that install spyware on the user's device.[194] Other attacks affect the broader population. In 2012, a military source reported that 8.9 million computers in China were infected with Trojan-horse viruses controlled from overseas IP addresses.[195] The hacker group SwaggSec announced in 2012 that it had broken into the database of the state-owned China Telecom, and that the company neglected to make a public statement or change its passwords. China Telecom subsequently confirmed the attack, but said any stolen data had "little value." However, a Chinese internet security expert acknowledged that China's internet was vulnerable, as many business owners and government officials lack the skills and awareness needed to defend themselves against cyberattacks.[196]

---

[191] "Boxun News Site Attacked Amid Bo Xilai Coverage," Committee to Protect Journalists, April 25, 2012, http://www.cpj.org/2012/04/boxun-news-site-attacked-amid-bo-xilai-coverage.php.
[192] Dennis Fisher, "Apple Phishing Scams on the Rise," *Threat Post*, June 24, 2013, http://bit.ly/GDS51j.
[193] Kim Zetter, "Sleuths Trace New Zero-Day Attacks to Hackers Who Hit Google," *Wired*, September 7, 2012, http://www.wired.com/threatlevel/2012/09/google-hacker-gang-returns/; "The Elderwood Project," *Symantec* (blog), September 6, 2012, http://www.symantec.com/connect/blogs/elderwood-project.
[194] Dylan Neild, Morgan Marquis-Boire, and Nart Villeneuve, "Permission to Spy: An Analysis of Android Malware Targeting Tibetans," Citizen Lab, April 2013, https://citizenlab.org/wp-content/uploads/2013/04/16-2013-permissiontospy.pdf.
[195] Jia Lei and Cui Meng, "*Ma Xiao Tian Yu E 'Wnag Luo Jun Bei Jing Sai*" [Ma Xiaotian Appeals for Suppressing 'Cyber Armament Race'], *Takungpao*, May 29, 2012, http://www.takungpao.com.hk/news/12/05/29/ZM-1484251.htm.
[196] Steven Musil, "Hackers Claim Breach of China Telecom, Warner Bros. Networks," *Cnet*, June 3, 2012, http://news.cnet.com/8301-1009_3-57446348-83/hackers-claim-breach-of-china-telecom-warner-bros-networks/.

CONCLUSION

Authoritarian regimes around the world look to Chinese methods of information control as a model, but activists can do the same. Anticipating what methods of censorship and control may be coming down the pipeline in China would be valuable for governments and internet users seeking to safeguard online freedoms against further encroachment. It is notoriously difficult to make accurate forecasts about China, but here are some technological developments worth watching:

- **Cross-platform censorship:** While online content has traditionally been separated from both telephony and radio and television broadcasting, experts say the three platforms are increasingly being brought under the same management and regulated by the same agencies. This could potentially streamline censorship and provide a more direct way of throttling dissent.
- **Interprovincial filtering:** At least one academic study has found evidence that internet censorship technology had been installed at the provincial level. Experts wonder whether this would enable officials to manipulate the information flowing between provinces—a more subtle and long-term alternative to total blackouts in areas of unrest.
- **Targeting circumventors by usage pattern:** Circumvention tools like VPN technology serve a broader commercial market in China, as well as users transmitting apolitical content like pirated movies. Rather than blocking the tools entirely, experts believe, censors are seeking to refine controls in order to block only circumventors with a specific usage pattern that indicates censorship evasion.

Ironically, this last example may provide some hope for online freedoms in China. So long as internet users defy censorship by creating content that current technology cannot trace or delete, propaganda agents and intermediary companies can adjust their methods in response. But if censors themselves are seeking to carve out exceptions, and grant privileges to pro-government or commercial groups, internet users benefit from what one study termed "collateral" freedom, "built on technologies and platforms that the regime finds economically or politically indispensable."[197] Collateral freedom is a poor substitute for full and free access to information and communication technologies. But the existence of such a phenomenon is proof that internet control runs counter to the public interest. By attempting to develop a partial, selective censorship apparatus, the CCP is acknowledging that internet freedom is central to China's success as a modern nation—and keeping doors open that netizens will continue to exploit.

[197] "Collateral Freedom: A Snapshot of Chinese Users Circumventing Censorship," *OpenITP*, May 21, 2013, http://openitp.org/pdfs/CollateralFreedom.pdfNews-Events/collateral-freedom-a-snapshot-of-chinese-users-circumventing-censorship.html.

CUBA

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	24	24
Limits on Content (0-35)	29	29
Violations of User Rights (0-40)	33	33
Total (0-100)	86	86

* 0=most free, 100=least free

POPULATION: 11.2 million
INTERNET PENETRATION 2012: 15 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Cuba's eagerly anticipated high speed ALBA-1 fiber optic cable, which was expected to increase data transmission speeds on the internet 3000 fold, was connected in early 2013; however, access was limited to select government offices rather than being extended throughout Cuba (see **OBSTACLES TO ACCESS**).
- The government imposed tighter restrictions on e-mail in the workplace, installing a platform that blocks "chain letters critical of the government" (see **LIMITS ON CONTENT**).
- In 2012 and 2013, the government continued its practice of employing a "cyber militia" to slander dissident bloggers and to disseminate official propaganda (see **LIMITS ON CONTENT**).
- Arbitrary detentions and intimidation of bloggers increased in late 2012 (see **VIOLATIONS OF USER RIGHTS**).
- Travel restrictions were loosened in early 2013 and some high-profile bloggers, such as Yoani Sánchez, were granted permission to leave Cuba for the first time in years (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Cuba, which bore witness to another crackdown on bloggers and citizen journalists in late 2012, has long ranked as one of the world's most repressive environments for information and communication technologies (ICTs). High prices, exceptionally slow connectivity, and prodigious government regulation have resulted in a pronounced lack of access to applications and services other than e-mail. Most users can access only a government controlled *intra*net, rather than the global *inter*net. Despite a handful of changes in Cuba's ICT landscape over the past year—including an increase in mobile phone penetration and the activation of the highly anticipated ALBA-1 fiber optic cable in January 2013—access to the internet and other ICTs remains limited. Nevertheless, a growing community of bloggers has consolidated their work, creatively using online and offline means to express opinions and spread information about conditions in the country.

Although the government appeared to loosen its restrictions on online media by unblocking a number of blogs in 2011, this period of opening was short-lived, as illustrated by a rash of arbitrary detentions in November and December 2012. Progovernment blogs that dared to be too critical of government policy were blocked, and phone numbers associated with the "speak-to-tweet" platform, widely used by activists to publicize human rights violations, were shut down. Such activity is not uncommon in Cuba; however, in 2013, the number of blocked websites remains more or less the same as it was in 2012. At least a dozen bloggers have been arrested, several nonviolent activists have been publicly beaten, and one citizen journalist was held without formal charges for six months before his eventual release (see Violations of User Rights). Surveillance remains extensive, extending to government-installed software designed to monitor and control office e-mail accounts as well as many of the island's public internet access points.[1]

OBSTACLES TO ACCESS

Internet access in Cuba is complicated by weak infrastructure and tight government control. While recent years have seen an expansion in the number of internet and mobile phone users, the ICT sector remains dominated by government firms. Restrictions on private enterprise were eased under the 2012 update of Cuba's economic model. Proposed reforms did not extend to liberalization of the communications sector, however.[2]

According to the National Statistics Office, there were 2.6 million internet users in Cuba in 2011, representing 23.2 percent of the population.[3] The latest data from the International

[1] Radio Surco, "Prestaciones Efectivas para Redes Informáticas" [Effective Features for Computer Networks], April 11, 2009, http://www.radiosurco.icrt.cu/Ciencia.php?id=415 (site discontinued); Danny O'Brien, "The Malware Lockdown in Havana and Hanoi," *CPJ Blog*, June 8, 2010, http://cpj.org/blog/2010/06/the-malware-lockdown-in-havana-and-hanoi.php.
[2] Nick Miroff, "Cuba is Reforming, but Wealth and Success are Still Frowned Upon," *Business Insider*, September 4, 2012, http://www.businessinsider.com/cubas-economic-transition-2012-9.
[3] National Office of Statistics and Information (ONEI), *Tecnología de la Información y la Comunicaciones en Cifras, Cuba 2011* [Information and Communication Technology, Cuba 2011] (Havana: ONEI, June 2012), http://bit.ly/15BVDBc.

Telecommunication Union (ITU) places Cuba's internet penetration at 25.64 percent as of 2012.[4] The vast majority of users cannot access the internet proper, but are instead relegated to a tightly controlled government-filtered *intra*net, which consists of a national e-mail system, a Cuban encyclopedia, a pool of educational materials and open-access journals, Cuban websites, and foreign websites that are supportive of the Cuban government.[5] Experts estimate that approximately 5 percent of Cubans periodically have access to the world wide web via government institutions, some foreign embassies, and black market sales of minutes by those permitted to have such accounts.[6] The National Statistics Office claimed a 46 percent gain in internet users in 2011, but only an 8 percent increase in networked computers, confirming the high percentage of people using shared computers and the lack of development in Cuba's ICT sector. Similarly, there was only a 3 percent increase in the number of domains registered, indicating that few governmental organizations are creating new websites.[7]

In 2000, the Ministry of Informatics and Communication (MIC) was created to serve as the regulatory authority for the internet. Its Cuban Supervision and Control Agency oversees the development of internet-related technologies.[8] Despite a January 2010 government announcement that national bandwidth had been expanded, there is still no broadband service and the limited number of Cubans with internet access face extremely slow connections, making the use of multimedia applications nearly impossible. [9] According to statistical findings from an April 2012 Google Analytics study, Cuba has the slowest connection speed in the Western Hemisphere and is among the worst in the world; globally, its only peers are Liberia and Sierra Leone.[10] Access over the intranet is similarly slow due to weak domestic infrastructure.

The Cuban government continues to blame the U.S. embargo for the country's connectivity problems, saying it must use a slow, costly satellite connection system and may only buy limited space. President Barack Obama eased some aspects of Washington's prolonged trade sanctions in 2009, however, allowing U.S. telecommunications firms to enter into roaming agreements with Cuban providers and to establish fiber-optic cable and satellite telecommunication facilities linking the United States and Cuba.[11] Official media ignored this important change in the U.S. legal framework, however, and Cuban leaders reiterated their demand for a complete end to the embargo.

---

[4] International Telecommunication Union (ITU), *Statistics: Percentage of Individuals Using the Internet, 2000-2012*, ITU, June 17, 2013, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls.
[5] ETECSA: Empressa de Telecomunicaciones de Cuba S.A., accessed August 28, 2010, http://www.etecsa.cu/.
[6] *Emerging Frontiers* (blog), "In Cuba Mystery Shrouds Fate of Internet Cable," May 23, 2012, http://emergingfrontiersblog.com/2012/05/23/in-cuba-mystery-shrouds-fate-of-internet-cable/.
[7] Larry Press, "Updated Cuban ICT statistics," *The Internet in Cuba* (blog), July 26, 2012, http://laredcubana.blogspot.com.es/2012/07/updated-cuban-ict-statistics.html (No figures have yet been released for 2013).
[8] For the website of The Ministry of Informatics and Communications see: http://www.mic.gov.cu/.
[9] Amaury E. del Valle, "Cuba, La Red Sigue Creciendo" [Cuba, the Network Continues to Grow], *Juventud Rebelde* online, January 6, 2010, http://www.juventudrebelde.cu/suplementos/informatica/2010-01-06/cuba-la-red-sigue-creciendo/; See also: Larry Press, "Past, Present, and Future of the Internet in Cuba," in *Papers and Proceedings of the Twenty-first Annual Meeting of the Association for the Study of the Cuban Economy (ASCE)* (Miami: ASCE, August 2011), http://bit.ly/w4nQPU.
[10] *Google Analytics* (blog), Blogspot, last modified April 19, 2012, http://bit.ly/IBvq5p.
[11] "Fact Sheet: Reaching Out to the Cuban People," The White House: Office of the Press Secretary, April 13, 2009, http://www.whitehouse.gov/the_press_office/Fact-Sheet-Reaching-out-to-the-Cuban-people.

The bilateral relationship was also affected by a 2009 incident that directly touched on the lack of open internet access in Cuba. On December 4, the Cuban authorities arrested Alan Gross, an American independent contractor who was in the country to set up individual satellite-based internet connections as part of a U.S. government–funded project. In March 2011, Gross was sentenced to 15 years in prison for committing an act "against the independence or territorial integrity of the state."[12] He is currently serving his sentence in a Cuban prison.

In February 2011, Cuban officials celebrated the installation of a 1,600 km (1,000 mile) undersea fiber-optic cable laid between Cuba and Venezuela at a cost of approximately $72 million.[13] The eagerly anticipated cable, known as ALBA-1, was expected to increase data-transmission speeds 3,000 fold, but more than two years after installation the government remains silent on its activation.[14] In the absence of official information, rumors began to spread about technical problems and corruption scandals.[15] There was also speculation that Cuban authorities had grown wary of increasing internet access due to the role of social media in the Arab Spring protests.[16] On January 24, 2013, there was finally evidence that the cable had been connected. While the development is significant, ETECSA has announced that the opening of the line will be gradual (predictably limited to select government offices at first) and that infrastructure must still be enhanced in order to facilitate widespread use of the technology.[17]

Prohibitively high costs also place internet access beyond the reach of most of the population. A simple computer with a monitor averages around CUC 722 ($722) in retail outlets, or at least CUC 550 ($550) on the black market.[18] By comparison, the average monthly Cuban salary is approximately CUC 16 ($16).[19] Even an internet connection in a hotel costs between CUC 6 and 12 ($6-12) per hour.[20] Computers are generally distributed by the state-run Copextel Corporation, yet only 31 percent of Cubans report having access to a computer. Of those with access, 85 percent noted that the computers were located at work or school.[21]

---

[12] Ellery Roberts Biddle, "Cuba: US Contractor Sentenced to 15 Years in Prison," Global Voices, April 4, 2011, http://globalvoicesonline.org/2011/04/04/cuba-us-contractor-sentenced-to-15-years-in-prison/.

[13] Ministerio de Educación Superior, "Cable de Fibra Optica Une Venezuela, Cuba y Jamaica" [Fiber Optic Cable Unites Venezuela, Cuba, and Jamaica], accessed August 13, 2012, http://bit.ly/1bhCqDV; *El Pais*, "Llega a Cuba el Cable Submarine de Fibra Optica para Ofrecer Internet de Banda Ancha" [Underwater Fiber Optic Cable Arrives in Cuba to Offer Broad Band Internet], February 10, 2011, http://internacional.elpais.com/internacional/2011/02/10/actualidad/1297292404_850215.html.

[14] Curt Hopkins, "Cuba's Internet Capacity to Increase 3,000x," *ReadWriteWeb* (blog), February 13, 2011, http://www.readwriteweb.com/archives/cubas_internet_capacity_increased_by_3000_percent.php; International Telecommunication Union (ITU) News Release, "ITU Hails Connectivity Boost for Cuba," February 11, 2011, http://www.itu.int/net/pressoffice/press_releases/2011/CM03.aspx.

[15] *Emerging Frontiers* (blog), "In Cuba Mystery Shrouds Fate of Internet Cable," May 23, 2012, http://emergingfrontiersblog.com/2012/05/23/in-cuba-mystery-shrouds-fate-of-internet-cable/.

[16] Nick Miroff, "In Cuba, Dial-Up Internet is a Luxury," National Public Radio, December 14, 2011, http://n.pr/vFmLh1.

[17] *BBC* online, "Cuba First High-Speed Internet Connection Activated," January 24, 2012, http://bbc.in/V0ggOM.

[18] Will Weissert, "Cubans Queue for Computers as PC Ban Lifted, But Web Still Outlawed," *Irish Examiner* online, May 5, 2008, http://bit.ly/197EZdn.

[19] Agence France-Presse, "Mobile Phone Use Booms in Cuba Following Easing of Restrictions," April 24, 2008.

[20] Tracey Eaton, "Cuban Dissident Blogger Yoani Sanchez Tours the United States," Florida Center for Investigative Reporting, March 20, 2013, http://fcir.org/2013/03/20/cuban-dissident-blogger-yoani-sanchez-tours-the-united-states/.

[21] National Statistics Office (ONE), Republic of Cuba, *Tecnologías de la Información y las Comunicaciones en Cifras: Cuba 2009* [Information and Communication Technologies in Figures: Cuba 2009] (Havana: ONE, May 2010), http://bit.ly/19esVBl.

Cubans can legally access the internet only by providing identification for on-site computer use at government-approved institutions, such as the approximately 600 Joven Club de Computación (Youth Computer Clubs) and points of access run by ETECSA.[22] While some ETECSA kiosks in the main cities of Havana and Santiago advertise internet access, field research has found that the kiosks often lack computers, instead offering public phones for local and international calls with prepaid phone cards. In June 2009, the government adopted a new law (Resolution No. 99/2009) allowing the Cuban Postal Service, which is under the domain of the Ministry of Computers and Communications, to establish cybercafes at its premises and offer internet access to the public.[23] Since then, a small number have been slowly established.[24]

There are only two ISPs in Cuba: CENIAI Internet and ENET (ETECSA). Both are owned by the state, though Telecom Italia previously held shares of ETECSA. In February 2011, the state-owned company Rafin S.A., a financial firm known for its connections to the military, bought Telecom Italia's 27 percent stake for $706 million.[25] As a result, the telecom company is now completely owned by six Cuban state entities. Cubacel, a subsidiary of ETECSA, is the only mobile phone carrier in Cuba.

Although the Cuban government began to allow the limited creation of private cooperatives by computer science graduates in 2012, tight internet restrictions, along with prohibitively high computer and software pricing, have resulted in a nonexistent official hardware and software market. A black market for such commodities does exist, but given the inherent challenges, Cuban ICT liberalization is mostly rhetoric and will likely have little impact on those in the communications sector.[26]

The Cuban government continues to control the legal and institutional structures that determine who has access to the internet and how much access will be permitted.[27] This regulation extends to the sale and distribution of internet-related equipment. In early 2008, after a nearly decade-long ban, the government began allowing Cubans to buy personal computers. Cuban officials or "trusted journalists" can now legally connect to an ISP with a government permit. Approved access to the internet, which is typically restricted to e-mail and sites related to one's occupation, is granted to doctors, professors, and government officials, whose offices are linked by an online network called Infomed. Home connections are not yet allowed for the vast majority of Cubans.

The government claims that all schools have computer laboratories, but in practice, internet access is usually prohibited for students or limited to very short periods of access, certain e-mail accounts, or supervised activities on the national intranet. Students at the Latin American School of Medicine

[22] For the club system's website, see: http://www.cfg.jovenclub.cu/.
[23] Resolution No. 99/2009 was published in the Official Gazette on June 29, 2009.
[24] As of May 2013, no new points of access had been established.
[25] Jerrold Colten, "Telecom Italia Sells Etecsa Stake to Rafin SA For $706 Million," Bloomberg, January 31, 2011, http://www.bloomberg.com/news/2011-01-31/telecom-italia-sells-etecsa-stake-to-rafin-sa-for-706-million.html.
[26] Various Authors, "Se Buscan Socios," *Juventud Rebelde* digital edition, December 15, 2012, http://www.juventudrebelde.cu/cuba/2012-12-15/se-buscan-socios/.
[27] Ben Corbett, *This Is Cuba: An Outlaw Culture Survives* (Cambridge, MA: Westview Press, 2002), 145.

in Havana, for example, are reportedly granted only 40 minutes a week of internet access, rendering online research or accessing academic journals infeasible.[28]

Despite the many barriers, Cubans still find ways of connecting to the internet through both authorized and unauthorized points of access. Some are able to break through infrastructural blockages by building their own antennas, using illegal dial-up connections, or developing blogs on foreign platforms. The underground economy of internet access also includes account sharing, in which authorized users sell access to those without an official account for one or two convertible pesos (CUC) per hour. Some foreign embassies allow Cubans to use their facilities, but a number of people who have visited embassies for this purpose have reported police harassment. There is also a thriving improvisational system of "sneakernets," in which USB keys and data discs are used to distribute material (articles, prohibited photos, satirical cartoons, video clips) that has been downloaded from the internet or stolen from government offices.

Cuba still has the lowest mobile phone penetration rate in Latin America, but the number is rising quickly. According to official reports, as of the end of 2012, 1.5 million Cubans—about 11 percent of the population—had mobile phones, a dramatic increase since 2009 when that figure was approximately 443,000.[29] Following its March 2008 easing of restrictions on mobile phone purchases, during 2011 and 2012 the government reduced the sign-up fee by over 50 percent—although it still represents three months' wages for an average worker. As the number of mobile phone users has grown, ETECSA has begun implementing small changes to terms of service, such as charging the caller rather than the recipient (receiving phone calls from within Cuba is now free) and cutting the cost of text messages in half.[30] In 2012, ETECSA also reduced daytime cellphone rates from CUC 0.60 to CUC 0.35 per minute.[31]

---

[28] Graham Sowa, "Why Students in Cuba Need Internet," *Havana Times*, May 23, 2011, http://www.havanatimes.org/?p=44073.

[29] Marc Frank, "More Cubans Have Local Intranet, Mobile Phones," Reuters, June 15, 2012, http://www.reuters.com/article/2012/06/15/net-us-cuba-telecommunications-idUSBRE85D14H20120615; See also: (1) "ETECSA Mobile Phone Users Cross Million Mark," Cubastandard.com, July 14, 2010 http://www.cubastandard.com/2010/07/14/etecsa-mobile-phone-users-cross-million-mark; (2) "Cuban Cellphones Hit One Million, Net Access Lags," Reuters, July 7, 2011, http://www.reuters.com/article/2011/07/07/us-cuba-telecom-idUSTRE76661920110707; (3) Amaury E. del Valle, "Cuba Aumenta Cantidad de Teléfonos Fijos y Móviles" [Cuba Increases Quantity of Fixed and Mobile Telephones], *Juventud Rebelde* online, December 26, 2011, http://www.juventudrebelde.cu/ciencia-tecnica/2011-12-26/cuba-aumenta-cantidad-de-telefonos-fijos-y-moviles/; (4) International Telecommunication Union (ITU), "Mobile-Cellular Telephone Subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#. For analysis (in Spanish): Emilio Morales, "Cuba: Teléfonos Celulares y Llamadas Costosas" [Cuba: Cellphones and Expensive Calls], Café Fuerte, January 17, 2012, http://cafefuerte.com/cuba/noticias-de-cuba/economia-y-negocios/1474-cuba-telefonos-celulares-y-llamadas-costosas.

[30] *Americas View* (blog), "Telecoms in Cuba: Talk is cheap," *The Economist* online, January 24, 2012, http://www.economist.com/blogs/americasview/2012/01/telecoms-cuba.

[31] For changes implemented by ETECSA, see: Camila Díaz Molina, "Se Extenderán los Plazos de Vigencia de Líneas de Celular en Cubacel," [Effective Period of Cubacel Cell Lines to be Extended] Cubacelular.org, December 16, 2012, http://www.cubacelular.org/2012/12/se-extenderan-los-plazos-de-vigencia-de.html; and Camila Díaz Molina, "Cubacel Anuncia Nueva Tarifa para el Servico de Teléfono Móvil en Cuba," Cubacelular.org, January 12, 2013, http://www.cubacelular.org/2013/01/cubacel-anuncia-nueva-tarifa-para-el.html.

Cuba has roaming agreements with 342 carriers in 139 countries,[32] and 2.2 million people used these services in Cuba in 2010.[33] The island's mobile network reportedly covers 78 percent of Cuban territory, with further expansions planned.[34] Most mobile phones do not include internet connections, but it is possible to send and receive international text messages and photographs with certain phones. Phones that utilize Global Positioning System (GPS) technology or satellite connections, however, are explicitly prohibited by Cuban customs regulations.[35] Additional restrictions are placed on modems, wireless faxes, and satellite dishes, which require special permits from the MIC in order to enter the country. [36]

At times of heightened political sensitivity, the government has used its complete control of the cell phone network to selectively obstruct citizens' communications. During a March 2012 visit to the island by Pope Benedict XVI, bloggers and dissidents reported that their cell phones were not working.[37] One independent journalist who investigated the situation found that calls were being automatically redirected to a phone number belonging to the Ministry of Interior.[38] All calls from dissidents' cell phones are monitored and the service is cut regularly to those working as freelance journalists or voicing views the government does not approve via citizen journalism. In October 2012, during the criminal trial concerning the wrongful death of long time civil rights activist Oswaldo Payá, dissident blogger Yoani Sánchez's phone was reportedly disconnected and her Twitter account was reportedly blocked.[39]

The Cuban government zealously pursues those who violate telecommunications access laws, and government technicians routinely "sniff" neighborhoods with their handheld devices in search of ham-radios and satellite dishes. In December 2012, the official newspaper *Granma* explicitly warned against "counterrevolutionary" and subversive use of illegal nets.[40] In an extensive report entitled: "Violations of the Cuban Telecommunications System," *Granma* detailed the criminal investigation of two highly profitable cyber-networks illegally using ETECSA's fixed and mobile market channels. The investigation is still in progress, but the information provided by the MIC and the Attorney General alleges that the illegal networks began operating in 2009 and were responsible for a loss of revenue for ETECSA totaling three million dollars. The defendants, who are being prosecuted for illegal economic activity and fraud, face fines coupled with sentences of three to ten years in prison.

---

[32] Camila Díaz Molina, "Roaming Internacional para Usarios de Cubacel," [International Roaming for Users of Cubacel] Cubacelular.org, November 10, 2012, http://www.cubacelular.org/2012/11/roaming-internacional-para-usuarios-de.html.
[33] Cuba Standard, "Syniverse Holding Back $2.5m in Cuban Roaming Charges," Cubastandard.com, October 21, 2011, http://bit.ly/1azWEaY, (These figures reflect the most recent data available)
[34] Nick Miroff, "Getting Cell Phones into Cuban Hands," *Global Post*, May 17, 2010, http://www.globalpost.com/dispatch/cuba/100514/cell-phone
[35] See: Cuban Customs Website (Aduana General de la Republica de Cuba): http://bit.ly/1hbJFOI.
[36] See: Cuban Customs Website (Aduana General de la Republica de Cuba).
[37] *Hispanically Speaking News*, "Silenced During Papal Visit, Cuban Bloggers, Dissidents Speak Out (VIDEO)," April 7, 2012, http://bit.ly/15Cqt7h.
[38] Juan O. Tamayo, "Cuba Diverts Dissidents' Phone Numbers in Pope Crackdown," *The Miami Herald* online, March 30, 2012, http://www.miamiherald.com/2012/03/30/2723658/cubas-interior-ministry-left-fingerprint.html.
[39] *BBC* online, "Cuban Dissident Blogger Yoani Sanchez Arrested," October 5,2012, http://bbc.in/WuwI9Z.
[40] Sheyla Delgado Guerra, "El 'Enredado' y Costoso Saldo de la Ilegalidad," [The "Tangled" and Expensive Balance of Illegality] *Granma* online, December 7, 2012, http://www.granma.cubaweb.cu/2012/12/07/nacional/artic07.html.

LIMITS ON CONTENT

Rather than relying on the technically sophisticated filtering and blocking used by other repressive regimes, the Cuban government limits users' access to information primarily via lack of technology and prohibitive costs. With the exception of unauthorized points of access in old Havana, Voice over Internet Protocol (VoIP) is blocked in Cuba, and social media applications, including Facebook and Twitter, are largely unavailable. Late 2012 and early 2013 witnessed tighter restrictions on e-mail in the workplace, along with an increase in the disabling of dissident websites and blogs. The cost of access to technologies that facilitate information sharing continues to be high; nonetheless, there is a vibrant community of bloggers in Cuba who utilize the medium to report on conditions within the country.

The websites of foreign news outlets—including the British Broadcasting Corporation (BBC), *Le Monde*, and *El Nuevo Herald* (a Miami-based Spanish-language daily)—are readily available; however, extremely slow connection speeds impede access to content.[41] The sites of some human rights groups, such as Human Rights Watch and Freedom House, remain largely accessible, but Amnesty International's website was recently blocked in Cuba.[42] For the most part, dissident news websites such as Payolibre, and independent journalism sites hosted on overseas servers, such as Cubanet, fall into the category of restricted access. The Association for Freedom of the Press (SIAPA) is also blocked, as are the websites of dissident organizations with a presence on the island (such as Damas de Blanco, MCL and UNPACU), which remain inaccessible from government-sponsored youth computer centers.[43] Revolico, a platform for posting classified advertisements, continues to be blocked, despite the apolitical nature of its content.[44]

Social-networking platforms such as Facebook and Twitter were recently blocked at some universities and government institutions, but may be accessed with consistent monitoring but varying reliability from some cybercafes and hotels. YouTube, by contrast, remains inaccessible from all points of access. The government has also increased control over the use of e-mail in official institutions, installing a new platform that restricts spam and specifically prevents the transmission of "chain letters critical of the government."[45]

While ETECSA does not proactively police networks and delete content, there are reportedly cases of bloggers removing posts after being threatened by officials for publishing views criticizing government actions.[46] Cases of self-censorship and removal have increased in recent months,

[41] Reporters Without Borders News Release, "Free Expression Must Go with Better Communications, Says Reporters Without Borders as Blogs Prove Hard to Access," March 31, 2008, http://bit.ly/16K5E9s.
[42] As reported by a source in Havana who wishes to remain anonymous.
[43] For *Bitácora Cubana* see: http://cubabit.blogspot.com/; For the website of Asociación pro Libertad de Prensa (the Association for Freedom of the Press) see: http://prolibertadprensa.blogspot.com/.
[44] Marc Lacey, "A Black Market Finds a Home in the Web's Back Alleys," *New York Times* online, January 3, 2010, http://www.nytimes.com/2010/01/04/world/americas/04havana.html; Peter Orsi, "Cuba's Next Step on Capitalist Road: Advertising," Boston.com, June 16, 2012, http://bo.st/KR3Kch.
[45] Café Fuerte, "Cuba Anuncia Cambio de Platforma Estatal para Correos Electronicos," [Cuba Announces Statewide Change to Email Platform] Cafefuerte.com, August 31 2012, http://bit.ly/RqHp8C.
[46] For examples, see: Café Fuerte, "Malestar por Cambio de Edificio del Partido Comunista en Camagüey," [Upset over Change

extending to blogs that published only moderate criticism of the government but were deemed "revolutionary" and subsequently blocked or disabled in late 2012. Furthermore, the wording of certain government provisions regarding content regulation is vague and allows a wide array of posts to be censored without oversight. Resolution 179 (2008), for example, authorizes ETECSA to "take the necessary steps to prevent access to sites whose contents are contrary to social interests, ethics and morals, as well as the use of applications that affect the integrity or security of the state."[47]

Beginning in 2007, the government systematically blocked core internet portal sites such as Yahoo, MSN, and Hotmail. As of 2013, these sites remain blocked in some government institutions, although they are largely accessible from hotels. Cuban authorities also restricted access to Cuban and foreign websites that contained independent reporting or views critical of the government. Among the continuously blocked sites were the *Bitácora Cubana* blog and the Voces Cubana platform, which hosts approximately 40 blogs including Yoani Sánchez's well-known *Generación Y*. While most of these sites and international portals were unblocked without explanation in February 2011, in late 2012 several other self-declared "pro-revolution" blogs were almost disabled. Facilities of access were severely restricted, and as a result bloggers from the targeted sites (which included University of Matanzas' student-run *La Joven Cuba*, and Elaine Diaz's *La Polemica Digital*) were able to publish only two or three posts.[48] *La Joven Cuba* was blocked until April 2013 but is now accessible. Content on *La Polemica Digital* remains available, however blog activity is sporadic.[49] In both cases, the associated bloggers were subject to intimidation, resulting in self-censorship.

Unable to completely suppress dissident activity on the internet through legal and infrastructural constraints, the authorities have taken a number of countermeasures, including dominating conversations within the medium itself. The Cuban government maintains a major presence on social networks via "Operación Verdad," (Operation Truth), its veritable cyber militia of approximately 1,000 trusted students from the University of Computer Sciences (UCI) who were recruited to promote the government's agenda and to slander dissident bloggers and independent journalists.[50] In February 2013, Yoani Sanchez interviewed blogger Eliécer Avila, a former UCI student—and leader of Operación Verdad.[51] Referring to the group as the "kilobyte police,"

---

to Communist Party Building in Camagüey] Cafefuerte.com, July 27, 2012, http://cafefuerte.com/cuba/noticias-de-cuba/sociedad/2050-malestar-por-cambio-de-edificio-del-partido-comunista-en-camagueey; and *El Yuma* (blog), "LJC, The Orwellian 'Memory Hole,' & Google Cache," Blogspot, July 8, 2012, http://bit.ly/RPbiC0.

[47] Sociedad Interamericana de Prensa, Inc., (Inter American Press Association), "Cuba," in *Reports and Resolutions*, accessed January 28, 2013, http://www.sipiapa.com/v4/det_informe.php?idioma=us&asamblea=22&infoid=346.

[48] *El Yuma* (blog), "La Blogosfera Cubana: 2012 Year in Review," [The Cuban Blogosphere: 2012 Year in Review] Blogspot, December 19, 2012, http://elyuma.blogspot.com.es/2012/12/la-blogosfera-cubana-2012-year-in-review.html; and Elaine Diaz, *La Polemica Digital* (blog), [The Digital Controversy] Wordpress.com, http://espaciodeelaine.wordpress.com/

[49] The site's most recent activity was a "last post" published in August 2012 accompanied by one more exceptional post in December 2012.

[50] Committee to Protect Journalists (CPJ), *After the Black Spring, Cuba's New Repression* (New York: July 6, 2011), http://cpj.org/reports/CPJ.Cuba.Report.July.2011.pdf. See also: *Cambios en Cuba* [Changes in Cuba] (blog): http://cambiosencuba.blogspot.com/; *Yohandry's blog*: http://yohandry.wordpress.com/; and the official blogger's platform CubaSí: http://www.cubasi.cu.

[51] Miriam Celaya, "The Internet Has its Own Soul: Eliecer Avila in a Revealing Interview," *Translating Cuba* (blog), February 21, 2013, http://translatingcuba.com/category/authors/eliecer-avila/.

Sanchez stated that the interview "corroborated" theories that State Security had created blogs to "denigrate and discredit the citizen who criticizes the system.[52]"

During the same month, video of a government training on social media appeared on the internet. In the footage, which was apparently leaked, a Cuban official warns agents of the potential threat that activist bloggers pose, alluding to the possibility that a popular blogger like Yoani Sanchez could organize protests in Havana similar to those that occurred in Iran in 2009. [53] He concludes by saying that the government must respond to these threats.

The government has also launched its own copycat versions of popular websites, such as Wikipedia and Facebook, and by some accounts, is delaying full connectivity of the ALBA-1 cable until the sites are fully operational so that content can be closely controlled.[54] The online encyclopedia Ecured, unveiled in December 2010, uses similar software and layout to its international counterpart, Wikipedia. However, a cursory review indicates that it is updated by only a small number of people, rather than an interactive community, and that it consists of 78,000 articles compared to several million on Wikipedia. Attempts to create an editor profile using an ".edu" or Gmail email account were reportedly rejected.[55] The government is preparing a portable version of EcuRed to be installed in cell phones in 2013.[56] In December 2011, a social-networking website called Red Social, accessible only from Cuba's intranet, was launched. Its layout matched Facebook so closely that some questioned whether it was a violation of copyright. According to one local blogger, however, shortly after its launch it no longer appeared to be functioning, possibly a reflection of the lack of server capacity to maintain it.[57]

In Cuba, the obstacles to sharing information are significant—the majority of citizen journalism is done offline, often by hand or typewriter, and uploaded and published once or twice a week. The financial cost of freedom of expression is also great; the tools that facilitate contribution to media outlets, such as paid internet access cards and international phone calls, are prohibitive and present a major obstacle.

While there is no exact count of blogs produced in Cuba, *Blogs Cubanos* reports that there are now

---

[52]Yoani Sanchez, "Operation Truth," *Translating Cuba* (blog), February 11, 2013, http://bit.ly/1bj2Ati.

[53] "Coral Negro," "La Ciber Policia en Cuba" [The Cyber Police in Cuba], Vimeo (Video), posted January 31, 2011), http://vimeo.com/19402730; English transcription: http://translatingcuba.com/?p=7111; See Also: "Acuse de Recibo: ¿Quién es el Ciberpolicía?" [Acknowledgement of Recepit: Who is the Cyber Policeman?], *Penúltimos Días*, February 5, 2011, http://www.penultimosdias.com/2011/02/05/acuse-de-recibo-18/.

[54] In May 2012, Venezuela's minister of science and technology told media that the cable was operational, but that it was up to the Cuban government to employ it. Some experts reported that internet speeds had improved in the Ministry of Interior or other government offices, adding to speculation that the government is using the cable in part to provide Venezuelan officials with acess to Cuban government databases, while deliberately postponing access to the cable for average users. See: "Venezuela: Fiber-optic Cable to Cuba is Working," Businessweek, May 24, 2012, http://www.businessweek.com/ap/2012-05-24/venezuela-fiber-optic-cable-to-cuba-is-working; Larry Press, "Hard Data on the Idle ALBA-1 Undersea Cable," *The Internet in Cuba* (blog), May 22, 2012, http://laredcubana.blogspot.com.es/2012/05/hard-data-on-idle-alba-1-undersea-cable.html.

[55] Larry Press, "Ecured is Not Open like Wikipedia," *The Internet in Cuba* (blog), December 21, 2011, http://laredcubana.blogspot.com/2011/12/ecured-is-not-open-like-wikipedia.html.

[56] Cuba Debate online, "EcuRed Se Cuela en los Celulares" [EcuRed Aneaks into the Cell], December 27, 2012, http://www.cubadebate.cu/noticias/2012/12/27/ecured-se-cuela-en-los-celulares.

[57]*The Philandrist* (blog), "The Cuban Facebook Imitation Saga – Red Social (Social Network)," December 6, 2011, http://thephilandrist.wordpress.com/2011/12/06/the-cuban-facebook-imitation-saga-redsocial/.

more that 1,600, including sites such as *Retazos* and *Convivencia*.[58] Independent websites hosted outside the country, such as *La Polemica Digital*, *Havana Times*, and *Estado de Sats*, provide the few who are able to access the net with a much richer and more robust selection of news sources and perspectives than those available from state-run media. Regional radio stations, magazines, and official newspapers are also creating online versions, though these are state-run and do not accept contributions from independent journalists. Some of these official sites recently installed commentary tools that foster discussion and allow readers to provide feedback, albeit censored.

In recent years, blogger Yoani Sánchez has become the most visible figure in an independent movement that uses new media to report on conditions that violate basic freedoms. As of March 2013, Sánchez's followers on Twitter totaled over 455,280, though only 26 percent were from within Cuba.[59] Sánchez and other online writers—including Claudia Cadelo, Miriam Celaya, Orlando Luis Pardo, Reinaldo Escobar, Laritza Diversent, and Luis Felipe Rojas—have come together on the *Voces Cubanas* blogging platform to portray a reality that official media ignores. Despite the government's open disapproval—in 2011, the daughter of President Raúl Castro's, Mariela, publicly referred to the bloggers as "despicable parasites"[60]—the movement has garnered broad support throughout society. In order to further promote freedom of expression, Sánchez has begun hosting Twitter workshops in her home, a bold move that has resulted in a crop of over 100 new Twitter users in Cuba.

Young people are increasingly using Twitter and mobile phones to document repression and voice their opinions. In a world where internet access is highly restricted, tweeting directly by SMS or a "Speak-to-Tweet" platform offers an alternate avenue for communicating with the outside world. The Speak-to-Tweet platform "Háblalo Sin Miedo" (Speak without Fear) enables Cuban residents to call a phone number in the United States and record anonymous messages describing government abuses or other grievances. The messages are automatically converted into posts shared via Twitter and YouTube.[61] At a cost of US $1.10 per tweet, Háblalo Sin Miedo is expensive; nonetheless, it is proving effective in allowing activists to denounce repressive acts and human rights violations.[62] Although the government has caught on to the phenomenon, establishing a Twitter presence of its own and blocking two phone numbers that ensure the operation of the "Speak-to-Tweet" platform in October and December 2012, new numbers have since been established.[63]

---

[58] "Blogs Cubanos – Top Alexia Cuba," *Blogs Cubanos* (blog), January 19, 2013, http://blogscubanos.wordpress.com/2013/01/19/blogs-cubanos/.

[59] Yoani Sanchez's Twitter page, accessed March 22, 2013, https://twitter.com/#!/yoanisanchez/; See also: Nelson Acosta and Esteban Israel, "Cuba Unblocks Access to Controversial Blog," Reuters, February 8, 2011, http://ca.reuters.com/article/topNews/idCATRE7175YG20110208; Monica Medel, "Bloggers Celebrate as Cuba Unblocks Their Sites," *Journalism in the Americas (*blog), http://knightcenter.utexas.edu/blog/bloggers-celebrate-cuba-unblocks-their-sites.

[60] Jeff Franks, "Castro Daughter, Dissident Blogger Clash on Twitter," Reuters, November 8, 2011, http://www.reuters.com/article/2011/11/09/us-cuba-twitter-castro-idUSTRE7A806Y20111109.

[61] Háblalo Sin Miedo, "Acerca de" [About us], accessed August, 13, 2012, http://www.hablalosinmiedo.com/p/como-funciona.html.

[62] Tracey Eaton, "Cuban Dissident Blogger Yoani Sanchez Tours the United States," Florida Center for Investigative Reporting, March 20, 2013, http://fcir.org/2013/03/20/cuban-dissident-blogger-yoani-sanchez-tours-the-united-states/.

[63] Juan O. Tamayo, "Regimen Cubano Bloquea Llamadas de Denuncia," *El Nuevo Herald* online, December 7, 2012, http://www.elnuevoherald.com/2012/12/07/1359290/regimen-cubano-bloquea-llamadas.html.

VIOLATIONS OF USER RIGHTS

Cuban legal structure is not favorable to internet freedom. Surveillance is widespread and dissident bloggers are subject to punishments ranging from fines and searches to confiscation of equipment and detentions. The constitution explicitly subordinates freedom of speech to the objectives of a socialist society, and freedom of cultural expression is guaranteed only if such expression is not contrary to the Revolution.[64]

The penal code and Law 88, known as the "Clamp Law," set penalties ranging from a few months to 20 years in prison for any activity considered a "potential risk," "disturbing the peace," a "precriminal danger to society," "counterrevolutionary," or "against the national independence or economy."[65] In 1996, the government passed Decree-Law 209, which states that the internet cannot be used "in violation of Cuban society's moral principles or the country's laws," and that e-mail messages must not "jeopardize national security."[66] In 2007, a network security measure, Resolution 127, banned the use of public data-transmission networks for the spreading of information that is against the social interest, norms of good behavior, the integrity of people, or national security. The decree requires access providers to install controls that enable them to detect and prevent the proscribed activities, and to report them to the relevant authorities. Furthermore, access to internet in Cuba generally requires identification with photo ID, rendering anonymity nearly impossible.

Resolution 56/1999 provides that all materials intended for publication or dissemination on the internet must first be approved by the National Registry of Serial Publications. Resolution 92/2003 prohibits e-mail and other ICT service providers from granting access to individuals who are not approved by the government, and requires that they enable only domestic chat services, not international ones. Entities that violate these regulations can be penalized with suspension or revocation of their authorization to provide access.

Despite constitutional provisions that protect various forms of communication and portions of the penal code that establish penalties for the violation of the secrecy of communications, the privacy of users is frequently violated. Tools of content surveillance are likewise pervasive. Under Resolution 17/2008, ISPs are required to register and retain the addresses of all traffic for at least one year.[67] The government routes most connections through proxy servers and is able to obtain all user names and passwords through special monitoring software Avila Link, which is installed at most ETECSA and public access points. In addition, delivery of e-mail messages is consistently delayed, and it is not unusual for a message to arrive without its attachments.

---

[64] Article 53, available at http://www.cubanet.org/ref/dis/const_92_e.htm, accessed July 23, 2010; See also: Article 39, d), available at http://www.cubanet.org/ref/dis/const_92_e.htm, accessed July 23, 2010.
[65] Committee to Protect Journalists, "International Guarantees and Cuban Law," March 1, 2008, http://bit.ly/1hbJO4p.
[66] Reporters Without Borders, "Going Online in Cuba: Internet under Surveillance," http://www.rsf.org/IMG/pdf/rapport_gb_md_1.pdf.
[67] "Internet en Cuba: Reglamento para Los Proveedores de Servicos de Acceso a Internet" [Internet in Cuba: Regulations for Internet Service Providers], CubanosUsa.com, December 18, 2008, http://bit.ly/19NNMfx.

Under Raúl Castro, the Cuban government appears to have shifted its repressive tactics from long-term imprisonment of bloggers to extralegal detentions, intimidation, and harassment.[68] In 2005 and 2007, two correspondents for Cubanet were charged with "precriminal social danger" and "subversive propaganda," and were sentenced to prison terms ranging from four to seven years. Both were released as part of a broader pardon of prisoners in December 2011. Bloggers are still routinely summoned for questioning, reprimanded, and detained, however, and late 2012 ushered in a resurgence of detentions.[69]

On November 7, authorities arrested numerous civil rights activists, including Yoani Sánchez and at least 12 others. Among those detained were Laritza Diversent, an attorney who runs the blog *Jurisconsulto de Cuba,* and Antonio Rodiles, curator of *Estado de Sats*. Diversent and many others were released shortly after detention, but Rodiles was held in police custody for over three weeks. Authorities gave no statement concerning the reason for his release, but Twitter users speculate that it may have been related to the hunger strike he began shortly after his arrest.[70] As it is very difficult to distinguish between independent blogging and political activism in Cuba, it is impossible to accurately pinpoint which offence triggered the detentions.

Examples of arrests and intimidation of independent journalists and bloggers in Cuba are not hard to find. Calixto Martínez, a prisoner of conscience and journalist for online news site *Hablemos Press*, was arrested for allegedly disrespecting the Castro administration. In accordance with Cuban law, which permits detainments of up to six months without charge, no formal charges were filed against Martínez, who was held in solitary confinement in response to a hunger strike he began after his September 2012 imprisonment.[71] He has since been released. Independent journalist Héctor Julio Cedeño Negrin, detained while photographing police harassment of taxi drivers, was imprisoned for 12 days before being placed under house arrest.[72]

In March 2012, during the Pope's visit to Cuba, dozens of bloggers were placed under house arrest or detained and held throughout the Pope's three-day stay, after which they were released.[73] On December 9, 2012, on the eve of International Human Rights Day, some 44 members of the nonviolent opposition group Ladies in White were publicly beaten and arrested, reportedly without

[68] Committee to Protect Journalists (CPJ), *After the Black Spring, Cuba's New Repression*, July 6, 2011, http://www.cpj.org/reports/2011/07/after-the-black-spring-cubas-new-repression.php.
[69] Daisy Valera, "This Cuban Woman and Her Online Indiscipline," *Havana Times* online, March 11, 2012, http://www.havanatimes.org/?p=64077; Steven L. Taylor, "Cuba vs. the Bloggers," *PoliBlog*, December 6, 2008, http://www.poliblogger.com/index.php?s=cuba+bloggers; Marc Cooper, "Cuba's Blogger Crackdown," Mother Jones, December 8, 2008, http://www.motherjones.com/politics/2008/12/cubas-blogger-crackdown.
[70] Biddle, Ellery Roberts "Cuba: Democracy Advocate Rodiles Released; Blogger Diversent Remains Detained," 5 December 2012, http://bit.ly/11Qsook.
[71] Amnesty International Press Release, "Cuban Journalist Named Prisoner of Conscience,"Amnesty.org, January 30, 2013, http://www.amnesty.org/en/for-media/press-releases/cuban-journalist-named-prisoner-conscience-2013-01-30; Amnesty International Press Release, "Prisoner of Conscience on Hunger Strike,"Amnesty.org, March 14, 2013, http://www.amnesty.org/en/library/asset/AMR25/002/2013/en/f2ef351c-54ab-43cb-a99e-0c39b3e9adab/amr250022013en.html
[72] Cuba Democracia y Vida, "Cuban Independent Journlaist Hector Cedeno Negrin Arrested for Doing His Job," February 8, 2013, http://www.cubademocraciayvida.org/web/article.asp?artID=20125
[73] *Hispanically Speaking News* online, "Silenced During Papal Visit, Cuban Bloggers, Dissidents Speak Out" (VIDEO), http://bit.ly/18zX2H0.

any sort of provocation.[74] Although these beatings were related to activism rather than online content, such abuse stands as a warning to the wider community of oppositionists.

In late 2012 and early 2013, online activity continued to be cause for repression. In December 2012, blogger and writer Ángel Santiesteban Prats received a five-year jail sentence on trumped-up charges of "home violation" and "injuries" at the end of a summary trial.[75] The winner of major literary prizes, Santiesteban was arrested in connection with his political views several times prior to the trial. Such harassment increased after Santiesteban's creation of the blog "The children no one wanted," in which he criticized the government. In January 2013, 25 year old blogger Daisy Valera was fired from her post as a nuclear chemist after searching the internet for information on Cuba and posting comments critical of the government on the *Havana Times* platform.[76]

Despite the abuses suffered by dissidents, 2013 brought a notable loosening of travel restrictions. As part of immigration reform, bloggers previously denied exit visas, including Yoani Sánchez, Orlando Luis Pardo, and Eliecer Ávila, were allowed to travel abroad. In early 2013, Sánchez, who was finally permitted to leave Cuba after having been denied an exit visa 21 times in the past five years, began an 80-city, 12-country tour, with the aim of brining awareness to Cuba's active civil society and blogosphere.[77] Her speeches have since received international attention.

[74] John Suarez, "Dozens of Ladies in White and Other Activists Beaten and Arrested Leaving Santa Rita Church Today," *Cuban Exile Quarter* (blog), Blogspot, December 9, 2012, http://cubanexilequarter.blogspot.com/2012/12/dozens-of-ladies-in-white-and-other.html

[75] Mary Jo Porter and Heffner Chun, site managers, "Angel Santiesteban," *Translating Cuba: English Translation of Cuban Bloggers*, April 23, 2013, http://translatingcuba.com/category/authors/angelsantiesteban; See also: Angel Santiesteban, "Prison Diary VI: Inside View of the Trial," *Translating Cuba: English Translation of Cuban Bloggers*, March 28, 2013, http://translatingcuba.com/prison-diary-vi-the-inside-view-of-the-trial-angel-santiesteban/.

[76] Daisy Valera, "Unemployed at 25 in Cuba," *Havana Times*, January 6, 2013, http://www.havanatimes.org/?p=85460

[77] Monika Fabian, "Cuban Dissident Yoani Sanchez on the Power of the Hashtag," ABC News/Univision Online, March 18, 2013, http://abcnews.go.com/ABC_Univision/News/cuban-dissident-yoani-sanchez-embarks-world-tour/story?id=18749528

ECUADOR

	2012	2013
INTERNET FREEDOM STATUS	N/A	PARTLY FREE
Obstacles to Access (0-25)	n/a	10
Limits on Content (0-35)	n/a	11
Violations of User Rights (0-40)	n/a	16
Total (0-100)	**n/a**	**37**

* 0=most free, 100=least free

POPULATION: 14.8 million
INTERNET PENETRATION 2012: 45 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The Organic Law on Communications—proposed during the coverage period and later approved—tasks website owners with "ultimate responsibility" for all content. This law, combined with government pressure, resulted in the removal of the reader comments sections from two prominent news sites (see **LIMITS ON CONTENT**).
- A new telecommunications act issued in July 2012 established the right to privacy and security for ICT users, while also authorizing the National Telecommunications Council to track IP addresses without judicial order (see **VIOLATIONS OF USER RIGHTS**).
- Reports of advanced surveillance technology in Ecuador were confirmed by Speech Technology Center, a Russian tech company, in December 2012. The company revealed that it had completed the installation of a biometric identification system capable of generating and storing both "voiceprints" and facial recognition data in Ecuador (see **VIOLATIONS OF USER RIGHTS**).
- In August 2012, Ecuador extended diplomatic asylum to WikiLeaks founder Julian Assange, a decision that attracted worldwide attention in part because it appeared to contradict the administration's attitude toward free speech and media freedom (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

In June 2013, Ecuador's Organic Law on Communications was passed. The law, which human rights organizations fear will stifle critical voices in the media, utilizes vague wording, arbitrary sanctions, and the threat of civil and criminal penalties in an effort to halt the spread of information that discredits public officials, even when such information is supported with evidence.[1] *The law also provides for the creation of a new media regulator led by a presidential appointee to prohibit the dissemination of "unbalanced" information and bans non-degreed journalists from publishing, effectively outlawing investigative reporting and citizen journalism.*

INTRODUCTION

Ecuador, which has historically lagged behind other Latin American nations in terms of technological growth, has witnessed substantial improvement in internet penetration over the past two years. Despite recent progress, however, Ecuador still faces challenges related to information and communication technology (ICT) development. These include: market penetration, especially in rural areas; high consumer costs; poor quality of ISP service; and high taxes on mobile phones, particularly those with internet access. While the government has begun a campaign to increase internet access across the country, opening a number of public internet access centers known as Infocentros in remote regions, to date there have been no measures predicated on improving quality of service or lowering access rates.

Although Ecuador's ICT landscape is in need of further expansion and upgrade, its current capacity facilitates use of social media platforms such as Facebook and Twitter, and also supports a lively blogging community. Social media are used for conversations on a wide variety of topics, including daily news, sports, entertainment, personal interest, and politics. During the February 2013 elections for president and National Assembly, the internet provided a real-time forum for candidates to launch proposals, solicit votes, discuss issues, and increase the scope of their publicity campaigns.

While President Correa's re-election has facilitated continued economic stability via social welfare programs and other initiatives, media freedom advocates are fearful that the proposed Organic Law on Communications will exacerbate the restrictions he has already placed on the press. Over the past few years, newspapers and other traditional media have had serious confrontations with the government often resulting in lawsuits filed against major media outlets at the behest of the president. Critics have expressed concern that President Correa's new term will result in an

[1] Gina Yauri, "Ecuador Passes Controversial Communications Law," Global Voices Online, June 19, 2013, http://globalvoicesonline.org/2013/06/19/ecuador-passes-controversial-communications-law/.

expanded executive, a less independent judiciary, and continued attacks on the media and political opposition at the hands of the government.[2]

In August 2012, Ecuador extended diplomatic asylum to WikiLeaks founder Julian Assange, who had been staying at the Ecuadorian Embassy in London since June and, as of May 2013, had not yet left the building for fear of arrest and extradition. Correa's offer of asylum allows the Ecuadorian president to temper his administration's history of media violations by portraying his government as a defender of free speech.[3]

OBSTACLES TO ACCESS

By the end of 2012, internet penetration in Ecuador had reached an all-time high of 35 percent,[4] although some sources within the country cite penetration rates as high as 55 percent.[5] This surge was largely the result of government efforts to increase connectivity nationwide in keeping with the November 2011 "Digital Strategy 2.0 Ecuador" plan, which set goals for increased internet access and enhanced technology that included the extension of internet connectivity to 50 percent of households by 2015.[6] Developments have largely been on track with projected deadlines, with Infocentros—community centers that offer free internet access and technological training—among the most successful initiatives.[7] Internet cafes are also becoming increasingly common, providing an alternative means of access for Ecuadorians, most of who use the internet for educational purposes, communication, and obtaining information.[8]

Three groups of fiber-optic cable run through Ecuador, offering connectivity to 23 of the country's 24 provinces: (1) from the north through Colombia towards the Andean region, (2) from the coast in the province of Guayas, and (3) from the south through the province of El Oro.[9] Ecuador is home to 22 internet service providers (ISPs), most of which offer internet service via these points of connection without activation fees. Of Ecuador's ISPs, ETAPA and GroupTvCable hold the

[2] William Neuman, "President Correa Handily WinsRe-Election in Ecuador," *The New York Times*, February 17, 2013, http://www.nytimes.com/2013/02/18/world/americas/rafael-correa-wins-re-election-in-ecuador.html?_r=0.
[3] Irene Cassell, "Julian Assange will be Granted Asylum, Says Official," The Guardian, August 14, 2012, http://www.theguardian.com/world/2012/aug/14/julian-assange-asylum-ecuador-wikileaks.
[4] International Telecommunication Union (ITU), *Statistics: Percentage of Individuals Using the Internet, 2000-2012*, ITU, June 17, 2013, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls.
[5] *Diario Hoy*, "El Acceso a Internet en el País Sobrepaso el 54% de la Población durante 2012," [Access to Internet in the Country Exceeded 54 Percent of the Population during 2012], *Diario Hoy*, January 1, 2013, http://www.hoy.com.ec/noticias-ecuador/el-acceso-a-internet-en-el-pais-sobrepaso-el-54-de-la-poblacion-durante-2012-570287.html.
[6] Roberta Prescott, "In New Digital Plan, Ecuador Aims for Internet Access to Half of all Households by 2015," RCR Wireless, November 16, 2011, http://www.rcrwireless.com/americas/20111116/networks/in-new-digital-plan-ecuador-aims-for-internet-access-to-half-of-all-households-by-2015/.
[7] MINTEL, *Infocentros*, MINTEL, Republica del Ecuador, coverage through 2012, http://www.infocentros.gob.ec/infocentros/index.php?option=com_content&view=category&layout=blog&id=38&Itemid=56.
[8] Ecuador Travel Guide, *Communications*, accessed August 8, 2013, http://www.ecuador-travel-guide.org/services/Communications.htm.
[9] Roberta Prescott, "Ecuador Announces US $8.2M Investment in Fiber Optics, RCR Wireless, August 2, 2011, http://www.rcrwireless.com/americas/20110802/networks/ecuador-announces-us-8-2m-investment-in-fiber-optics/; Specific information regarding cables provided by interview with Carlos Correa Loyola, March 2013.

greatest percentage of market share.[10] Under a provision prioritizing essential technology, computers, which range from approximately $800 to$1000, are tax-free when imported from other countries. As compared to an average wage of $318 per month, however, computers are not easily affordable.[11] For those fortunate enough to own computers, there are multiple subscription options, ranging from dial-up pay-per-minute plans to cable and radio modems and satellite connections.[12] Broadband (commonly used in urban zones) and satellite connections (often used in rural areas) have become increasingly popular in recent years, eclipsing dial-up plans.

According to industry estimates, between 33 and 66 percent of internet users have broadband speeds between 2 to 3Mbps, at a cost of $20 to $25 per month.[13] In May 2012, Superintendent of Telecommunications Fabian Brito indicated that the overall average speed of an internet connection in Ecuador is 128Kbps, although speeds are lower in rural areas. While the price of access is consistent in both rural and urban settings, representatives from the government's office of telecommunications predict a significant decrease in subscription prices across the board along with an attendant increase in connection speed in coming years.[14]

In 2011, mobile penetration in Ecuador was measured at 47 percent, a significant increase from 2010 figures, which came in at 24 percent. Regional variations still persist, however, with the lowest number of subscribers, 30 percent, found in the Andean highlands of Bolivar, and the greatest number, 55 percent, found in the province of Pichincha, which counts Ecuador's capital, Quito, among its cities. Mobile phone subscriptions vary greatly among income level, with 54 percent of those above the poverty line enjoying active subscriptions as compared to 28 percent of those below the poverty line. Of those with mobile phones, only 8 percent have smartphones, 36 percent of which are concentrated in the provinces of Guayas, El Oro, and Azuay. Those with post-graduate degrees are most likely to own smartphones.[15]

Ecuador is home to three mobile service providers: one state-run operator, CNT, and two private providers, Claro (CONECEL) and Movistar (OTECEL). The total number of active cellular accounts exceeds 14 million, distributed as follows: Claro leads the pack with 69 percent of subscribers, followed by Movistar with 29 percent, and finally, state-run CNT, with almost 2

[10] El Tiempo, "Internet Aumentara Velocidad" [Internet Speed will Increase], May 17, 2012, http://www.eltiempo.com.ec/noticias-cuenca/96903-internet-aumentara-velocidad/.
[11] *El Diario*, "Correa Anuncia que el Sueldo Básico Aumenta a $318"[Correa Announces that the Base Salary is Increasing to $318], December 22, 2012, http://www.eldiario.ec/noticias-manabi-ecuador/250696-correa-anuncia-que-el-sueldo-basico-aumenta-a-318/.
[12] Tempest Telecom, *Coverage Guide: Ecuador – Dialup Internet Access*, accessed August 8, 2013, http://www.tempestcom.com/guide/guide.aspx?Id=60&view=1.
[13] CNT, National Corporation of Telecommunications, *Products and Services*, CNT, 2012, http://www.cnt.gob.ec/cntwebregistro/04_cntglobal/productos_detalle.php?txtCodiSegm=1&txtCodiLine=4&txtCodiProd=34&txtCodiTipoMovi=0#valDes.
[14] El Tiempo, "Internet Aumentara Velocidad" [Internet Speed will Increase], May 17, 2012, http://www.eltiempo.com.ec/noticias-cuenca/96903-internet-aumentara-velocidad/.
[15] INEC, National Center for Statistics and Censuses, "Reporte Anual de Estadisticas sobre Tecnologias de la Information y Comunicaciones (TICs) 2011" [Annual Report of Statistics about Information and Communications Technologies (ICTs) 2011], http://www.inec.gob.ec/sitio_tics/presentacion.pdf.

percent of subscribers.[16] While some data packages include internet access, Movistar's full navigation package imposes certain limitations on the applications subscribers may use.[17] Movistar states that it retains the right to restrict access to certain sites without prior warning, should the sites generate content that could "affect the proper functioning of its system." Such vague language leaves the rationale behind the restriction of certain websites rather opaque, although it appears to be a policy related to security concerns rather than one driven by censorship.[18]

Despite their popularity, the Ecuadorian government classifies mobile phones as luxury items. In addition to being excluded from the tax exemption extended to computers, a June 2012 ruling (No. 67) issued by the Committee on Foreign Trade (COMEX)[19] also imposes quotas on the importation of mobile telephones.[20] According to the edict, the limitation is predicated on preventing further environmental degradation resulting from residual cell phone waste.

Social networks are not widely used in Ecuador. A national survey revealed that as of 2011, only 3 percent of Ecuadorians utilized such platforms, most of whom were concentrated in coastal, urban areas and held university degrees.[21] The Ecuadorian blogosphere has largely followed in the footsteps of conventional media, witnessing a slight decrease in the quantity of voices represented in recent years while still supporting discussion on a wide array of issues, including politics, sports, and daily news. Isolated communities in rural areas have less of a presence online due to connectivity issues, and therefore less representation in terms of advocating for matters such as water rights and indigenous land issues, leading to potential marginalization in online communities.

In recent years, the Ministry of Telecommunications (MINTEL) has initiated a handful of projects predicated on increasing digital literacy and general internet access. To that end, Infocentros have been installed in 377 (48 percent) of Ecuador's 810 rural parishes, with a projection of 100 percent by 2014. [22] As mentioned above, Infocentros provide free access to computers, telephones, and the

[16] SUPERTEL, "Operadoras Reportaron 17.133.539 Líneas Activas de Telefonía Móvil Prestadas a Través de Terminales de Usuario"[Operators Report 17,133,539 Active Mobile Telephone Lines Provided to Users], Superintendencia de Telecomunicaciones, February 20, 2013, http://www.supertel.gob.ec/index.php?option=com_content&view=article&id=1182%3Aoperadoras-reportaron-17133539-lineas-activas-de-telefonia-movil-prestadas-a-traves-de-terminales-de-usuario&catid=44%3Aprincipales&Itemid=344.

[17] Movistar, "Aplicaciones Restringidas - Plan Full Navegación" [Restricted Applications – "Full Navigation" Plan], Movistar Mobile Phone Company, http://movistar.com.ec/pdf/Aplicaciones_restringidas_IM_Full_Navegacion.pdf.

[18] Movistar, Aplicaciones Restringidas Plan Full Navegacion" [Restricted Applications in Full Navigation Plan], Movistar, accessed August 1, 2013, http://movistar.com.ec/pdf/Aplicaciones_restringidas_IM_Full_Navegacion.pdf.

[19] COMEX, "Resolución Nº67 del Comité de Comercio Exterior" [Legal Ruling # 67 of the Committee for External Business Relations], June 11, 2012, http://www.produccion.gob.ec/wp-content/uploads/downloads/2012/09/RESOLUCION-67.pdf

[20] *La Hora Nacional*, "Restricciones de Comercio Limitarán Acceso a Internet" [Trade Restrictions will Limit Access to the Internet], June 26, 2012, http://www.lahora.com.ec/index.php/noticias/show/1101351932#.UTONqahgbME.

[21] Carlos Correa Loyola, "Aprobacion de la Ley de Comunicación en Ecuador y su impacto en Internet" [Approval of the Communications Law in Ecuador and its Impact on the Internet], *Bitacora de Calu* (blog), June 17, 2013, http://calu.me/bitacora/2013/06/17/aprobacion-de-la-ley-de-comunicacion-en-ecuador-y-su-impacto-en-internet.html; See also: INEC, National Center for Statistics and Censuses, "Reporte Anual de Estadisticas sobre Tecnologias de la Information y Comunicaciones (TICs) 2011" [Annual Report of Statistics about Information and Communications Technologies (ICTs) 2011], http://www.inec.gob.ec/sitio_tics/presentacion.pdf.

[22] MINTEL, *Infocentros – Sobre*, MINTEL, Republica del Ecuador, coverage extended through 2012, http://www.infocentros.gob.ec/infocentros/index.php?option=com_content&view=category&layout=blog&id=38&Itemid=56.

internet, and also offer ICT training.[23] During 2012, teams from the National Plan of Digital Recruitment (PLANADI) utilized Infocentros to train a reported 34,500 people to be technical managers.[24] To date, 445,000 visitors have accessed the internet from such centers in rural districts. The project appears to be meeting its goals of expanding demand for the internet to rural areas, as well as increasing the percentage of the population that enjoys digital literacy.

In rural areas, cybercafes, which generally provide internet access at a rate of $1 per hour, are often relied upon. Such establishments face the same requirements as other businesses, including registering with the government. In order to utilize the services provided by cybercafes, the national secretary of telecommunications, SENATEL, requires that users register with the following: full name, phone number, passport number, voting certificate number, email address, and home address. Users must also agree to terms that stipulate that all information entered into the database during use falls under the jurisdiction of SENATEL and the superintendent of telecommunications, SUPERTEL. If a user infringes on the terms and criminal charges are applicable to the transgression, the user will be prosecuted under Ecuador's penal code.[25]

Ecuador's backbone is not highly centralized. There have been no reported incidents of the government placing restrictions on applications from new companies in the ICT sector, however high registration costs and administrative hurdles can make it difficult to begin operating a new telecommunications business. New ISPs and mobile companies often face fees as high as $100,000 as well as legal obstacles, each of which can complicate their attempts to enter the market.[26] Private ISPs sometimes engage in bandwidth throttling (the intentional slowing down of internet service) to specific sites when excessive amounts of bandwidth are being consumed. It appears as though Ecuadorian ISPs utilize this strategy for traffic management rather than for censorship, however they are not transparent about such restrictions and there are likewise no laws to protect against preferential treatment of certain sites in times of high traffic.

Ecuador's state regulatory agency is called the National Telecommunications Council (CONATEL).[27] It is part of the Telecommunications Ministry, the head of which is nominated by the president and also serves as the head of CONATEL, a process which demonstrates close alignment with the executive body.[28] In July 2012, CONATEL issued the Telecommunication Service Subscribers and Added Value Regulation Act.[29] Internet subscribers have taken issue with

[23] MINTEL, *Infocentros – Sobre*, MINTEL, Republica del Ecuador, coverage extended through 2012, http://www.infocentros.gob.ec/infocentros/index.php?option=com_content&view=category&layout=blog&id=38&Itemid=56.
[24] Alvaro Layedra, MINTEL, reported via Twitter account @alayedra, Twitter, January 2013, https://twitter.com/alayedra.
[25] SENATEL, *Registro de Cibercafes On Line* [Registration of Cybercafes Online], Republica del Ecuador, accessed August 6, 2013, http://www.regulaciontelecomunicaciones.gob.ec/registro-de-cibercafes/.
[26] AEPROVI, general information available at: http://www.aeprovi.org.ec.
[27] *El Universo*, "Presidente del CNE: Hay que regular a las redes sociales y a eso vamos" [President of CNE: We have Regular Social Networks], *El Universo*, October 18, 2012, http://www.eluniverso.com/2012/10/18/1/1355/presidente-cne-hay-regular-redes-sociales-eso- vamos.html
[28] SENATEL, "CONATEL - Consejo Nacional de Telecominicaciones" [CONATEL – National Telecommunications Council], accessed August 5, 2013 http://www.regulaciontelecomunicaciones.gob.ec/conatel/.
[29] Carlos Correa Loyola, "Carta Impresa a Domingo Paredes, Presidente del CNE, sobre Intención de Regular las Redes Sociales" [Printed Letter to Domingo Paredes, President of CNE, about the Intention to Regulate Social Networks], *Bitácora de Calú* (blog), October 18, 2012, http://calu.me/bitacora/2012/10/18/carta-impresa-a- domingo-paredes-presidente-del-cne-sobre-intencion-de-regular-las-redes-sociales.html.

some of the act's main provisions, namely: discretionary exemption relating to use of infrastructure against state security (Article 24.9) and the granting of authority to CONATEL to request users' IP addresses without court order (Article 29.9).[30]

LIMITS ON CONTENT

There have been no widespread instances of blocking or filtering of websites or blogs in Ecuador, but there has often been restraint of political and government-related content both in print and, increasingly, online. Attempts to censor statements made in times of heightened political sensitivity have been witnessed, as have alleged instances of censorship via the overly broad application of copyright protection principles to content critical of the government. The population is able to access diverse sources of national and international information, however, anti-government commentary has been subject to governmental repercussions in recent years.

While access to blogs and social media platforms such as Facebook, Twitter, and YouTube is generally free and open in Ecuador, during the February 2013 presidential elections, the National Electoral Council (CNE) announced that it would begin making efforts to police social networks, though the mechanism by which such censorship would occur are unclear. This attempt led to online mobilization and protests by web users, which resulted in a guarantee from CNE not to regulate citizens' personal expression or opinions on social networks.[31]

Another contentious case involves the trial of the Luluconto 10, a group of young social protestors suspected of planting pamphleteering bombs—mini explosions designed to distribute political pamphlets in crowded areas. Among the 10 activists who were arrested are a lawyer, a dentist, an engineer, a young mother, and a law student—all of whom were imprisoned on the day of their arrest and held without charges for four months. After they were finally brought to trial on terrorism charges, the group's defense lawyers were banned from reporting on the case through social networks.[32] The order came on the heels of growing social mobilization advocating for a free and fair trial, much of which was carried out online, illustrating the impact of social media networks even in a country in which only a small minority of citizens have such accounts.[33]

The Ecuadorian government has periodically sought to block critical content on grounds of copyright infringement. A controversial 2012 documentary about President Correa was subject to such treatment when clips of the film were posted on YouTube and Vimeo. The videos were removed after Spanish anti-piracy firm Ares Rights filed a copyright infringement lawsuit on behalf of Ecuador's state-run TV channel, claiming that the documentary included unauthorized images of

[30] *El Comercio*, "Jueces Ordenan que Juicio del Caso Luluncoto no se Transmita por Redes Sociales" [Judges Ordered that Case of Luluncoto is not to be Transmitted by Social Networks], January 23, 2013, http://www.elcomercio.com/seguridad/Jueces-ordenan-Luluncoto-transmita- sociales_0_852514906.html.
[31] Website of CONATEL (National Telecommunications Council), http://www.conatel.gob.ec/.
[32] CONATEL, "Resolución TEL-477-16-CONATEL-2012", [Resolution TEL-477-16-CONATEL-2012], July 11, 2012, available here: http://www.regulaciontelecomunicaciones.gob.ec/.
[33] Manuela Picq, "Criminalizing Social Protests," *Al Jazeera*, February 14, 2013, http://www.aljazeera.com/indepth/opinion/2013/02/20132128651511241.html.

the president.[34] Distribution of the documentary has been riddled with problems both within Ecuador and abroad ever since. After interviewing the filmmaker, Santiago Villa, on an Ecuadorian radio show, host Andres Carrion was forced to shut down his radio program.[35] When Villa attempted to broadcast the documentary on American TV channel American TeVe, he was asked to make changes to the film's content, allegedly due to fears of legal reprisal. The documentary is now available only on the Russian website smotri.[36]

The Ecuadorian government has occasionally been accused of manipulating digital media via the use of progovernment commentators employed to counter opposition voices. In February 2012, Fernando Balda, a former member of President Correa's socialist Alianza PAIS political party, blogged about government "troll centers" dedicated to defending the president and slandering the opposition on social media. Balda describes a digital "army" tasked with such work, which, he says, is comprised of workers with pseudonymous Facebook and Twitter accounts. Although Communications Secretary Fernando Alvarado refuted Balda's claims,[37] reporters at *El Comercio* echoed such accusations in March 2012. Citing Balda's statements as well as complaints made to the NGO Fundamedios, *El Comercio* claims that an investigation into tax records revealed that a number of accounts associated with inflammatory comments about journalists were in fact not registered to real people but appear to exist solely to slander journalists on social media platforms.[38] Over the years, reports have also surfaced of intense government pressure on media outlets to silence critical opinions during elections and at other times of heightened political interest.[39]

Although formal rules governing online activity have only been discussed in recent years, self-censorship has long been encouraged by the ramifications associated with the publication of critical comments. In January 2013, for example, President Correa (@MashiRafael) called for the National Secretary of Intelligence (SENAIN) to investigate two Twitter users who had published disparaging comments about him, an announcement which sent a warning to others not to post comments critical of the president.[40] In recent years, the Ecuadorian state has issued complaints and filed court

[34] Mike Masnick, "Spanish Anti-Piracy Firm Ares Rights History of Censorship by Copyright for Ecuador and Argentina," Techdirt.com, June 28, 2013, http://www.techdirt.com/articles/20130628/17335823665/spanish-anti-piracy-firm-ares-rights-appears-to-specialize-censorship-copyright-latin-american-countries-like-ecuador.shtml.

[35] Human Rights Ecuador, "Journalist Andres Carrion Forced to Leave Radio After Interview with Author of Correa Documentary," Human Rights Ecuador, December 6, 2012, http://www.humanrightsecuador.org/2012/12/06/journalist-andres-carrion-forced-to-leave-the-radio-after-interview-to-author-of-correa-documentary/.

[36] Silvia Higuera, "YouTube, Vimeo Remove Documentary on Rafael Correa for Alleged Copyright Infringement," Knight Center for Journalism in the Americas, December 19, 2012, https://knightcenter.utexas.edu/blog/00-12416-youtube-vimeo-remove-documentary-rafael-correa-alleged-copyright-infringement.

[37] *El Universo,* "Dirigente de SP Revela Supuesto 'Ejercito' de Cuentas Falsa en Ecuador" [SP Reveals Alleged 'Army' of Fake Accounts in Ecuador], February 28, 2012, http://www.eluniverso.com/2012/02/28/1/1355/dirigente-sp-revela-supuesto-ejercito-cuentas-falsas-ecuador.html; Maca Lara-Dillon, "Inedito: Gobierno de Ecuador Habria Montado un 'Troll Center'" [Unpublished: Government of Ecuador has Set Up a Troll Center], Pulso Social, March 1, 2012, http://pulsosocial.com/2012/03/01/inedito-gobierno-de-ecuador-habria-montado-un-troll-center/.

[38] *El Comercio*, "El Supuesto 'Troll Center' Tuvo en su Mora a El Comercio" [The Alleged 'Troll Center' Seen at El Comercio], *El Comercio*, January 3, 2012, http://www.elcomercio.com/politica/supuesto-troll-center-mira-COMERCIO_0_655734472.html.

[39] Milton Ramirez, "Ecuador: The Departure of a Television Anchor, Global Voices Online, April 25, 2009, http://globalvoicesonline.org/2009/04/25/ecuador-the-departure-of-a-television-anchor/; See also: Ecuador Sin Censura, http://ecuadorsincensura.blogspot.com/2009/04/cero-independencia.html.

[40] *Ecuador Times*, "Rafael Correa Asked the SENAIN to Investigate Twitter Accounts," *Ecuador Times*, January 25, 2013, http://www.ecuadortimes.net/2013/01/25/rafael-correa-asked-the-senain-to-investigate-twitter-accounts/.

proceedings against certain mainstream media outlets that maintain a digital presence via websites or social networks, including *El Comercio* and *La Hora*. Critics allege that reporters and journalists associated with the digital branches of these publications have exemplified a marked shift in tone, resorting to pro-government expression following state seizures of printing press equipment and supplies, as well as threats of legal action for online posts.[41]

After receiving criticism from the government, news site *La Hora* indefinitely suspended the reader comments section on its website. Such action was taken in order to avoid "publishing offensive comments" that might violate a clause in Ecuador's proposed communications law (since approved) that imposes "ultimate responsibility" on publishers for any content that "threatens the honor or name of a good person"—a clause which extends to the reader commentary section of a newspaper's website.[42] Despite *La Hora*'s efforts, one month later, the newspaper found itself at the center of a governmental dispute over content. The newspaper was forced by court order to publish an apology to the government, both on its website and in print, for having published a story based on data from an independent monitoring center that claimed the government had spent $71 million on propaganda.[43]

Print and digital news outlet *El Comercio* faced similar pressure related to its readers' comments; like *La Hora*, the comments section was ultimately disabled, although in this instance the catalyst was a letter from President Correa. In July 2012, the president accused *El Comercio* of censoring progovernment commentary and allowing only inflammatory, anti-Correa rhetoric from commentators to be posted on its website. The newspaper subsequently apologized to Correa, stating that it was an "error [on the part of the newspaper] not to have filtered the offensive comments to the president."[44] At the president's request, the comments section has since been shut down completely.

In Ecuador, social networks have been utilized to coordinate meetings held in real life to organize, protest, or propose actions. To date, there have been no official governmental constraints on internet-mediated mobilization; however, the impact of such movements has been limited. Warnings from the president stating that the act of protesting will be interpreted as "an attempt to destabilize the government" have undoubtedly discouraged some from participating in protest movements.[45]

---

[41] *The Telegraph*, "Ecuador President Wins Libel Case Against Newspaper," July 21, 2011, *The Telegraph*, http://www.telegraph.co.uk/news/worldnews/southamerica/ecuador/8651676/Ecuador-president-wins-libel-case-against-newspaper.html.

[42] Silvia Higuera, "Government of Ecuador asks Paper to 'Filter' Reader Comments," Knight Center for Journalism in the Americas, January 30, 2013, https://knightcenter.utexas.edu/blog/00-12744-government-ecuador-asks-paper-"filter"-reader-comments.

[43] *El Diario*, "Diario *La Hora* Publica Sus Disculpaspara el Gobierno," *El Diario*, November 14, 2012, http://www.eldiario.ec/noticias-manabi-ecuador/247818-diario-la-hora-publica-sus-disculpas-para-el-gobierno/; See also: Silvia Higuera, "Ecuadorian Newspaper Complies with Court Order, Apologizes to Government," Knight Center for Journalism in the Americas, November 16, 2012, https://knightcenter.utexas.edu/blog/00-12104-ecuadorian-newspaper-complies-court-order-apologizes-government.

[44] *El Comercio*, "Correa Da Su Version del Desfile Olimpico" [Correa Gives His Version of the Olympic Parade], July 28, 2012, http://www.elcomercio.ec/politica/Rafael-Correa-da-version-desfile-Olimpico-juegos-olimpicos_0_745125557.html.

[45] Carlos Andres Vera, "Protesta Tuitera: #El8ALasCalles" [Twitter Protest: #El8ALasCalles], *Polificcion* (blog), March 6, 2012, http://polificcion.wordpress.com/2012/03/06/protesta-tuitera-el8alascalles/.

VIOLATIONS OF USER RIGHTS

Ecuador's media freedom standards continue to be contradictory, balancing positive provisions such as universal access to ICTs with concerning developments relating to user privacy and manipulation of the press. While President Correa has had a hand in influencing some of the media via a direct line to reporters, he has also made a show of purportedly supporting free speech without condition, going so far as to grant diplomatic asylum to WikiLeaks founder Julian Assange much to the chagrin of some members of the international community.[46] The incongruity of the president's strategy points to a dual desire to limit domestic media while simultaneously asserting a world image as a supporter of free speech. Ecuador's new communications law, however, is poised to overshadow the nation's foreign policy.

While the Organic Law on Communication does contain some positive provisions, such as recognizing the right to communication, it also contains numerous articles of concern for advocates of online expression. One rule greatly compromises user anonymity by forcing media companies to collect and store user information.[47] Another vaguely worded article prohibits "media lynching," which appears to extend to any accusation of corruption or investigation of a public official—even those that are supported with evidence. Websites are also subject to "ultimate responsibility," which makes them liable for all hosted content. A new body with oversight authority, to be appointed by the executive, has also been described in vague language, which may leave the door open to arbitrary actions against bloggers, journalists, and users of social media.[48]

Article 16.2 of Ecuador's constitution guarantees "universal access to information technologies and communication.[49] Article 384 similarly confers the ability to exercise one's right to communication, information, and freedom of expression. However, a discretionary loophole in Resolution TEL-477-16-CONATEL-2012 grants ISPs a wide margin for the implementation of "actions they deem necessary to the proper administration of the service network," and by extension, threatens net neutrality. [50]

In July 2012, Ecuador's Ministry of Telecommunications issued a resolution (The Telecommunication Service Subscribers and Added Value Regulation Act) establishing a framework for ICT user rights and ISPs. Among its provisions are articles stating that telecommunications is considered a "strategic sector" by the Ecuadorian government, and that the state is tasked with the

[46] *El Telégrafo*, "Ecuador Concede Asilo Diplomático a Julian Assange" [Ecuador Grants Diplomatic Asylum to Julian Assange], August 16, 2012, http://www.telegrafo.com.ec/actualidad/item/ecuador-concede-asilo-diplomatico-a-julian-assange.html.
[47] Analia Levin, "Mechanisms of Censorship in Ecuador's Communication Law," Global Voices Online, July 22, 2013, http://advocacy.globalvoicesonline.org/2013/07/22/mechanisms-of-censorship-in-ecuadors-communications-law/.
[48] Alejandro Martinez, Ecuador's Controversial Communications Law in 8 Points," Knight Center for Journalism in the Americas, June 20, 2013, https://knightcenter.utexas.edu/blog/00-14071-8-highlights-understand-ecuador's-controversial-communications-law.
[49] MINTEL, "Autoridades del MINTEL se reunieron con usuarios digitales" [MINTEL Authorities Met with Digital Users], Ministerio de Telecomunicaciones y Sociedad de la Información, August 13, 2012, http://www.telecomunicaciones.gob.ec/autoridades-del-mintel-se-reunieron-con-usuarios-digitales-2/.
[50] See Article 15.6 of CONATEL's Telecommunication Service Subscribers and Added Value Regulation Act: http://www.elcomercio.com/seguridad/Jueces-ordenan-Luluncoto-transmita- sociales_0_852514906.html.

"administration, regulation, control and management" of such technologies, while also being responsible for ensuring that the public has access to ICTs. Article 14 further establishes a state guarantee of privacy and security for users, prohibiting third party interception of communications.[51] Despite such positive provisions, however, Article 29.9 of the same act authorizes CONATEL to track IP addresses from ISP customers without judicial order.[52]

There are no specific laws criminalizing online content, however, standard defamation laws apply to content posted online, and are sometimes invoked by the government.[53] While lawsuits have been filed against digital news sites for comments critical of the current administration, detentions of regular ICT users are not as common. Calls for investigations into Twitter users who post content critical of the government, have, however, been levied by governmental authorities, including President Correa, a form of legal intimidation that stands to result in greater self-censorship online.[54] The only recent arrest related to internet activity concerned an activist who created a fake identity on the government site "Dato Seguro" and posed as the president, allegedly with the aim of revealing to the public that state information and systems are not sufficiently secure. Paul Moreno, the man responsible for illustrating the ease of breaching state digital security, was arrested in Riobamba in November 2012 under accusations of identity theft.[55] No details are available regarding the investigation of Moreno, however, his supporters were very active on social networks after he was detained (see, for example, tweets under the hashtag #LiberenAPaulCoyote), a factor that appears to have influenced the judiciary. Moreno was released four days after his arrest following his publication of a public letter of apology. [56] Although he was never brought to trial Moreno commented that during his detention, there were no acts of intimidation and due legal process was followed.[57]

Anonymous communication is not prohibited in Ecuador, nor are there restrictions against citizens who choose to maintain encrypted communications or use security tools. While the state guarantees privacy of communications, identification and registration are required to purchase a new cell phone, a regulation which has come into the spotlight following allegations of widespread secret state surveillance.

---

[51] See Article 14 of CONATEL's Telecommunication Service Subscribers and Added Value Regulation Act: http://www.elcomercio.com/seguridad/Jueces-ordenan-Luluncoto-transmita- sociales_0_852514906.html.

[52] Carlos Correa Loyola, "Carta Impresa a Domingo Paredes, Presidente del CNE, sobre Intención de Regular las Redes Sociales" [Printed Letter to Domingo Paredes, President of CNE, about the Intention to Regulate Social Networks], *Bitácora de Calú* (blog), October 18, 2012, http://bit.ly/18l0dBH.

[53] Asamblea Nacional de Ecuador, "Constitución del Ecuador" [Constitution of Ecuador], Asamblea Nacional de Ecuador, October 20, 2008, http://www.asambleanacional.gob.ec/documentos/constitucion_de_bolsillo.pdf.

[54] *Ecuador Times*, "Rafael Correa Asked the SENAIN to Investigate Twitter Accounts," *Ecuador Times*, January 25, 2013, http://www.ecuadortimes.net/2013/01/25/rafael-correa-asked-the-senain-to-investigate-twitter-accounts/.

[55] Paul Moreno, *Viajes* [Travel] (Blog), http://paulcoyote.tumblr.com/; Paul Moreno, Twitter page, @paulcoyote; See also: Paul Moreno, "www.DatoSeguro.gob.ec No es Seguro" [www.DatoSeguro.gob.ec is Not Safe], Ecualug, November 26, 2012, http://www.ecualug.org/?q=20121126/blog/paulcoyote/wwwdatosegurogobec_no_es_seguro.

[56] DINARDAP , "Boletín de Prensa de DINARDAP" [DINDARP Press Bulletin], *El Comercio*, November 30, 2012, http://www.elcomercio.com/%20politica/Boletin-prensa-DINARDAP_ECMFIL20121130_0003.pdf; *El Universo*, "Bloguero Detenido por Usar Datos del Presidente Correa en Sistema Dato Seguro" [Blogger Detained for Using Data of Presiden in System Data Insurance], *El Universo*, November 30, 2012, http://m.eluniverso.com/2012/11/30/1/1355/detiene-tuitero-advirtio-posibles-fallas-sistema-dato-seguro.html.

[57] Paul Moreno, Letter Detailing Arrest and Detention, *Calu* (blog), December 1, 2012, http://calu.me/sandbox/cartapaul.jpg.

In December 2012, Russian tech company Speech Technology Center revealed that it had been contracted to provide Ecuador with a nationwide "biometric identification platform" capable of facial and voice recognition. The controversial database of "voiceprints" and facial features created by the country allegedly stores information only on known or suspected criminals or "persons of interest."[58] Although the government claims not to listen to phone calls for "political purposes," human rights advocates have cautioned that the technology holds the potential for abuse and could be used to track down political dissidents, advocates, or investigative journalists. [59]

Instances of verbal and physical harassment against journalists appear to be on the raise. In fact, verbal threats often come from the president, who uses his weekly *sabatina* (report) to insult journalists and others who have displeased him. The president, who has referred to journalists as "assassins with ink[60]" has also filed—and won—court proceedings against print journalists who have made critical comments about him or about presidential orders that resulted in the harming of civilians. In one landmark case from 2011, newspaper *El Universal* was charged $40 million in damages for publishing a critical article. Emilio Palacio, author of the column, and the directors of the newspaper were all sentenced to three years in prison. Palacio's sentence was overturned in August 2012, but he and his family were already in the process of applying for political asylum in the United States which was granted the following month.[61]

Recent years have also been witness to two murders—one of a photojournalist, and one of an online reporter. In August 2012, Orlando Gomez Leon, a Quito based journalist from Colombia who writes for a Colombian weekly newspaper and also serves as an internal editor at print and digital newspaper *La Hora*, was the target of intimidation and violence. After contributing to an article discussing Ecuador's free speech issues and its contradictory extension of asylum to WikiLeaks creator Julian Assange, Gomez began receiving threats. Later in the day, he was attacked by two assailants with a steel bar but managed to drive away unharmed. Given the nature of the threats he received, which included a warning to "stop saying bad things about Ecuador," the attack appears to be connected directly to Gomez's journalism.[62]

In April 2013, Fausto Valdivieso, a public relations consultant and journalist of nearly 30 years who wrote widely on social networks and reported for a small online TV station, was murdered after numerous threats and a previous attempt on his life a day earlier. Although a link to his journalistic work has not been proven, his murder occurred while he was investigating issues related to the

[58] Ryan Gallagher, "Ecuador Implements 'World's First' Countrywide Facial- and Voice-Recognition System," *Slate*, December 12, 2012, http://slate.me/T9E6WV.
[59] Rosie Gray and Adrian Carrasquillo, "Ecuador Defends Domestic Surveillance," Buzzfeed, June 27, 2013, http://www.buzzfeed.com/rosiegray/ecuador-defends-domestic-surveillance.
[60] Summer Harlow, "Ecuador President Blasts New Media during Speech at Columba University in New York," Knight Center for Journalism in the Americas, Septemeber 28, 2011, https://knightcenter.utexas.edu/blog/ecuador-president-blasts-news-media-during-speech-columbia-university-new-york.
[61] Human Rights Ecuador, "Caso El Universal," accessed August 7, 2013, http://www.humanrightsecuador.org/casos-destacados/caso-el-universo/?lang=es See also: Emilio Palacio, "Mi Vida en 830 Palabras," *Emilio Palacio en Internet* (blog), September 2011-August 2012, https://sites.google.com/site/emiliopalacioeninternet2/home/trayectoria-de-Emilio-Palacio.
[62] Reporters Without Borders, "Colombian Journalist Threatened, Attacked with Steel Bar," Reporters Without Borders, August 22, 2012, http://en.rsf.org/ecuador-colombian-journalist-threatened-22-08-2012,43257.html.

government. Accordingly, his work has been suspected as one possible motive in the killing.[63] The suspects, currently in custody, are reputed to be members of a criminal drug-trafficking ring.[64]

Cyberattacks in Ecuador are generally sporadic rather than systematic, although they appear to be on the rise. These assaults include modifications to webpages (defacements), phishing, the spread of malware, and DDoS attacks. The websites of independent human rights organizations have occasionally been subject to disabling attacks and unexplained disruptions, and although their administrators suspect government involvement, no party has yet taken responsibility. In February 2013, the Twitter accounts of human rights organization Fundamedios (Andean Foundation for Media Observation and Study) and the online activism site Polificcion were suspended without explanation.[65] Following a press conference held by Fundamedios which detailed the dangers of arbitrary suspension, the organization's Twitter account was reinstated in March, 2013.[66]

In January 2013, immediately following the publication of an article alleging that President Correa had two offshore bank accounts in Switzerland, website BananaLeaks.co was the target of disabling cyberattacks. Although administrators were able to get the site back up and running one day later, BananaLeaks says its site was "immediately sabotaged by the Ecuadorian government with DDoS attacks."[67] Independent media outlets have not been the only targets of such attacks, however. In August 2012, "hacktivist" group Anonymous hacked into 45 websites belonging to the Ecuadorian government in protest of Article 29 of CONATEL's July 2012 resolution allowing government agencies to request users' IP addresses.[68] Operation #OpInternetSurkishka wreaked utter and widespread havoc on governmental websites for two days. [69]

---

[63] For more on Valdivieso's writings, see: YouTube, *Patuchobalcon*, last updated August 2011, http://www.youtube.com/user/patuchobalcon.

[64] *Diario Extra*, "Fausto Valdiviezo 'Conocia' a Sus Presuntos Asesinos" [Fausto Valdiviezo 'Knew' his Alleged Murderers], *Diario Extra*, June 3, 2013, http://www.diario-extra.com/ediciones/2013/06/03/cronica/fausto-valdiviezo-conocia-a-sus-presuntos-asesinos/; See also: Reporters Without Borders, "Journalist Slain in Guayaquil, a Day after Escaping Earlier Murder Attempt," Reporters Without Borders, April 12, 2013, http://en.rsf.org/ecuador-journalist-slain-in-guayaquil-a-12-04-2013,44372.html.

[65] *La República*, "Correa Pide a Inteligencia que Investigue a Dos Tuiteros" [Correa Calls on Intelligence to Investigate Two Tweeters], *La República*, January 24, 2012, www.larepublica.ec/blog/politica/2013/01/24/correa-pide-a-la-senain-que-investigue-a-dos-tuiteros/; See also: Carlos Andres Vera, "Sobre la Suspensión de mi Cuenta Twitter", [About the Suspension of my Twitter Account], *PoliFiccion* (blog), March 4, 2013, http://polificcion.wordpress.com/2013/03/04/sobre-la-suspension-de-mi-cuenta-twitter/.

[66] Fundamedios, "Twitter Suspende Cuenta de Organización Ecuatoriana" [Twitter Suspends Account of Ecuadorian Organization], IFEX, February 26, 2012, http://www.ifex.org/ecuador/2013/02/26/fundamedios_cuenta_twitter/es/.

[67] Fundamedios, "Website Hacked by Ecuadorian Government After Story on President," Fundamedios/IFEX, February 14, 2013, http://www.ifex.org/ecuador/2013/02/14/bananaleaks_sabotage/.

[68] Europa Press, "Anonymous Hackea 45 'Webs' de Gobierno Ecuatoriano" [Anonymous Hack '45' Webs of the Ecuadorian Government] Europa Press, August 11, 2012, http://www.europapress.es/latam/ecuador/noticia-ecuador-anonymous-hackea-45-webs-gobierno-ecuatoriano-20120811063017.html.

[69] Storify, "#OpInternetSurkishka en Ecuador" [#OpInternetSurkishka in Ecuador], Digital Users of Storify EC, August 2012, http://storify.com/ecuadorinternet/opinternetsurkishka.

EGYPT

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	14	15
Limits on Content (0-35)	12	12
Violations of User Rights (0-40)	33	33
Total (0-100)	**59**	**60**

* 0=most free, 100=least free

POPULATION: 82.3 million
INTERNET PENETRATION 2012: 44 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Authorities repeatedly throttled mobile internet service in the areas around political protests, preventing activists from communicating through social networks and VoIP services (see **OBSTACLES TO ACCESS**).
- Courts ordered the temporary blocking of YouTube and permanent blocking of pornography sites, though the decisions have not been implemented (see **LIMITS ON CONTENT**).
- An unprecedented number of liberal bloggers and online activists have been prosecuted by special courts for insulting the president. Several users were also charged for insulting religion over social networks (see **VIOLATIONS OF USER RIGHTS**).
- Administrators of antigovernment and anti-Muslim Brotherhood Facebook groups were targeted in cases of extralegal abductions and killings (see **VIOLATIONS OF USER RIGHTS**).
- Senior Muslim Brotherhood officials working in the office of President Morsi reportedly met with an Iranian spy chief in December 2012 to seek assistance in the development of new surveillance capabilities outside of the traditional military-controlled structure (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

This report covers events between May 1, 2012 and April 30, 2013. On July 3, 2013, President Mohamed Morsi was removed from power by General Abdul Fatah al-Sisi, the Defense Minister and head of the armed forces. Millions of Egyptians had taken to the streets since June 30 in a protest coordinated by a grassroots campaign known as Tamarod, the Arabic word for "rebel." Tamarod, which is supported by the Egyptian Movement for Change, threatened widespread civil disobedience if Morsi did not resign by July 2. More significantly, the army issued a 48-hour ultimatum to the country's political groups to "meet the demands of the people" and threatened to intervene if the political crisis was not solved. When Morsi refused to back down, the army took him under detention and appointed the head of Egypt's highest court, Adly Mansour, as interim president. Together with religious and secular opposition leaders, General al-Sisi set out a roadmap for the drafting of a new constitution as well as the holding of parliamentary and presidential elections. Supporters of Morsi remained camped out in two large protest sites until August 14, when security forces raided the camps, killing hundreds in the process. Senior Muslim Brotherhood figures were taken under arrest and a temporary state of emergency was declared.

INTRODUCTION

Since the internet was introduced in the country in 1993, the Egyptian government has invested in information and communications technology (ICT) infrastructure as part of its strategy to boost the economy and create jobs. Until 2008, authorities showed a relaxed attitude toward internet use and did not censor websites or use high-end technologies to monitor discussions. However, with the rise of online campaigns to expose government fraud, document acts of police brutality, and call for large-scale protests, the government began to change its stance. Between 2008 and 2011, state police admitted to engaging in surveillance, online censorship, and cyberattacks – especially against sites related to the Muslim Brotherhood and other opposition movements.[1]

The significant role of ICTs in the 2011 protests that toppled the 30-year regime of President Hosni Mubarak led some to label the event as the Facebook[2] or Twitter revolution.[3] After the Supreme Council of Armed Forces (SCAF) took control of the government, the military administration maintained many of its predecessor's tactics by keeping mobile phones, social media, and opposition activists under vigorous surveillance. Even as several activists and bloggers were intimidated, beaten, or tried in military courts for "insulting the military power" or "disturbing social peace," social networks continued to grow as a democratizing tool. Online, Egyptians launched debates about the fate of their emerging democracy and exerted pressure on SCAF to end

[1] Galal Amin, *Whatever happened to the Egyptian Revolution*, Cairo: Al Shorook, 2013.
[2] Abigail Hauslohner, "Is Egypt About to Have a Facebook Revolution," Time, January 24, 2011, http://www.nbcnews.com/technology/jon-stewart-questions-egypts-twitter-revolution-125446.
[3] Helen A.S. Popkin, "Jon Stewart questions Egypt's 'Twitter revolution'," NBC News, January 28, 2011, http://www.nbcnews.com/technology/jon-stewart-questions-egypts-twitter-revolution-125446.

decades under emergency rule. On May 31, 2012, the state of emergency was finally lifted[4] and one month later, power was officially handed over to a civilian government in a controversial election that pitted a former Mubarak official with an Islamist candidate.[5]

After the election of President Mohammed Morsi, a candidate from the Muslim Brotherhood's Freedom and Justice Party, Egypt has failed to make any gains in internet freedom. The passage of a new constitution did not allay concerns over threats to free speech and a record number of citizens were prosecuted for insulting the president. The rise of Islamist forces has also contributed to an increase in online blasphemy cases being tried in Egyptian courts, resulting in several users receiving jail sentences. Countless other web activists and social media users have been harassed and detained. Police authorities and Muslim Brotherhood thugs engaged in extralegal violence against liberal activists and revolutionary youths who voice dissent online. Finally, distrust between the military and the Muslim Brotherhood led the latter to seek Iranian assistance in the development of parallel security and intelligence arms outside of the existing military-controlled structure. Despite these obstacles, online journalists and commentators have continued their dynamic role, pushing the boundaries of free speech and protesting against the undemocratic actions of the civilian president.

OBSTACLES TO ACCESS

The development of Egypt's ICT sector has been a strategic priority since 1999, when former president Mubarak created the Ministry of Communications and Information Technology (MCIT) to lead Egypt's transition into the information age.[6] Since then, ICT use has increased rapidly, with internet penetration growing from 16 percent in 2007 to 44.1 percent in 2012.[7] Mobile internet, either using smartphones or USB modems, accounts for roughly 44 percent of all internet use, with ADSL use at around 38 percent. Egypt's mobile phone penetration rate was 113.2 percent in the first quarter of 2013, amounting to over 94 million mobile subscriptions.[8]

Although these figures are promising, there are a number of obstacles hindering access to ICTs, including an adult literacy rate of only 72 percent,[9] poor telecommunications infrastructure in rural areas and urban slums, and flagging economic conditions. Moreover, ICTs and online culture are often viewed with suspicion and women's access to technology has become a growing concern after

[4] "Egypt state of emergency lifted after 31 years," BBC News, May 31 2012, http://www.bbc.co.uk/news/world-middle-east-18283635.
[5] Osman El Sharnoubi, "Egypt's President Morsi in power: A timeline (Part I)," AhramOnline, June 28 2013, http://english.ahram.org.eg/News/74427.aspx.
[6] "Historical Perspective," Ministry of Information and Communication Technologies, Accessed April 16, 2013, http://www.mcit.gov.eg/TeleCommunications/Historical_Prespective.
[7] "Percentage of Individuals Using the Internet" and "Mobile-cellular subscriptions," International Telecommunications Union, accessed July 23 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[8] Ministry of Information and Communication Technologies, "Information and Communications Technology Indicators" March 2013, available at http://mcit.gov.eg/Indicators/indicators.aspx, accessed July 23 2013.
[9] United Nations Development Program, "Egypt, Country Profile: Human Development Indicators," accessed July 23, 2013, http://hdrstats.undp.org/en/countries/profiles/EGY.html.

the revolution.[10] In some cases, marginal religious figures have issued 'fatwas' against women using the internet without the presence of a male chaperone.[11]

Broadband prices in Egypt are relatively cheap if compared to neighboring Arab Countries. However, with more than 25 percent of the Egyptian population living under the national poverty line, internet access is not universally affordable.[12] As an indication of what prices are like, a 2 Mbps connection costs $11 per month for a download limit of 4 GB, whereas an unlimited plan costs $30 per month.[13] In an index that compares ICT prices to gross national income (GNI) per capita, Egypt ranks 77th out of 161 countries.[14]

Recent investment in telecommunications infrastructure has been limited since the revolution. The country's economic crisis halted plans for a fourth mobile operator license and many foreign investment projects have ceased due to the increase in violence and political instability. Moreover, several training programs and collaborations with international and private entities were halted.[15] Many cybercafés and ISPs have closed down upon increased threats to their operations and continued pressure from the government and non-state actors.[16] Frequent electricity blackouts also disrupted internet access in major cities.

Documents recovered from the Ministry of Interior after the fall of the Mubarak regime revealed how the Egyptian government centralized internet infrastructure and fiber-optic cables into highly-controllable "chokepoints."[17] In addition, virtually all of Egypt's telecommunications infrastructure is owned by Telecom Egypt, a state-owned company. Egypt's five main ISPs lease lines from Telecom Egypt and resell bandwidth to over 200 smaller ISPs. The arrangement makes it easy to suspend internet access or decrease speeds, as was the case during the 2011 revolution. From January 27 to February 2, 2011,[18] authorities disabled the country's Border Gateway Protocol Routes, shutting down all internet traffic in less than one hour.[19] Telecommunications companies were then ordered to cut mobile internet and text-messaging service under the terms of strict agreements they had signed with regulators. At the time, state intelligence agencies claimed that

[10] Ahmed El Gody, 2008, "New Media New Audience New Topics and New forms of Censorship in the Middle East" in Philip Seib New Media New Middle East New York: Palgrave
[11] Sanaa Al Tawila, 2013, The most vocal Women Fatwas http://bit.ly/19MveMJ, accessed June 11, 2013
[12] World Bank, "Data—Indicators: Poverty Headcount Ratio at $2 a Day," http://data.worldbank.org/country/egypt-arab-republic?display=default, accessed June 13, 2013
[13] "Home ADSL Price List," TE Data, accessed July 24, 2013, http://www.tedata.net/eg/en/Home-ADSL/Home-ADSL-Prices-List.
[14] "Measuring the Information Society," International Telecommunication Union, 2012, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf.
[15] B. O. Adegbemi Onakoya, A. Sheriffdeen Tellaand M. Adenike Osoba Investment in Telecommunications Infrastructure and Economic Growth British Journal of Economics, Management & Trade 2(4): 309-326, 2012 www.sciencedomain.org/download.php?f=1354167302.pdf.
[16] Asma Alsharif and David Stamp, "Egyptian reassurance may fail to woo investment dollars," CNBC, March 21, 2013, http://www.cnbc.com/id/100578204.
[17] James Glanz and John Markoff, "Egypt Leaders Found 'Off' Switch for Internet," The New York Times, February 15, 2011, http://www.nytimes.com/2011/02/16/technology/16internet.html?_r=2&pagewanted=all&.
[18] Erica Chenoweth, "Backfire in the Arab Spring," Middle East Institute, September 1, 2011, http://www.mei.edu/content/backfire-arab-spring.
[19] Iljitsch van Beijnum, "How Egypt did (and your government could) shut down the internet," Ars Technica, January 30, 2011, http://arstechnica.com/tech-policy/2011/01/how-egypt-or-how-your-government-could-shut-down-the-internet/.

"foreign intelligence [was] using communication technologies to plan terrorist actions."[20] Steps to limit bandwidth and temporarily cut off service in targeted areas were also taken by the interim SCAF administration and, more recently, under President Morsi.

Mobile users and activists have complained of throttled internet speeds in areas of protests, most likely due to government efforts to limit their ability to organize and document police brutality.[21] In November and December 2012, during demonstrations outside the president's office and clashes on Mohamed Mahmoud Street, users reported the temporary cutting off of Voice over Internet Protocol (VoIP) applications and mobile internet access more generally. A more widespread disruption to connectivity occurred in March 2013 during heightened protests against President Morsi and the Muslim Brotherhood. However, Egypt's National Telecommunications Regulatory Authority clarified that the disruption was due to a cut in an undersea cable that also affected internet speeds across the region.[22] The poor legal and regulatory environment has led to several campaigns calling for a boycott of government-linked ISPs[23] and for the establishment of an independent entity to monitor the ICT sector.[24]

Mobile service providers and ISPs are regulated by the National Telecommunication Regulatory Authority (NTRA) and governed by the 2003 Telecommunication Regulation Law. The NTRA's board is chaired by the ICT minister and includes representatives from the defense, finance, and interior ministries; the state security council; the presidency; workers' unions; as well as public figures, experts, and other military figures.[25] Officially, the NTRA is responsible for regulating the telecommunications industry[26] and furthering ICT development through projects like the "eMisr" National Broadband Plan outlined in late 2011.[27] The NTRA also conducts analysis of the telecommunication market and publishes research to encourage investment. However, there have been some reports revealing the NTRA's ties to online control and surveillance activities. Through its control of the mobile subscriber database, it has been accused of monitoring mobile and social media applications, such as WhatsApp.[28]

---

[20] Ameera Fouad, "Saying no to mobile phones," Al-Ahram Weekly Online, Issue No. 1083, February 2-8, 2012, http://weekly.ahram.org.eg/2012/1083/eg402.htm.

[21] Al Wafd, "Cairo Police Chief: No power cutoff in Tahrir Square" 24 November 2012 http://www.alwafd.org/أخبار-التحرير-عن-الاتصالات-قطع-ينفي-القاهرة-مدير أمن-311559/محلية-10/وتقارير.

[22] Ahmed El Bermawy "Urgent: Internet Cable major cutoff" Al Tahrir newspaper22 March 2013 http://tahrirnews.com/news/view.aspx?cdate=22032013&id=d0e2c3c4-cdf4-4d9b-a444-d438f00dcac8

[23] Campaign for Fair Internet Use http://www.almstba.com/vb/t12717.html.

[24] The People demand Fair Internet https://www.facebook.com/KefayaSer2a.

[25] "About Us: NTRA Board: Board Members," National Telecommunication Regulatory Authority, accessed April 16, 2013, http://www.tra.gov.eg/english/DPages_DPagesDetails.asp?ID=175&Menu=5.

[26] "About Us: NTRA Board: NTRA Function & Role," National Telecommunication Regulatory Authority, accessed April 16, 2013, http://www.tra.gov.eg/english/DPages_DPagesDetails.asp?ID=176&Menu=5.

[27] "eMisr National Broadband Plan," National Telecommunication Regulatory Authority, http://www.tra.gov.eg/emisr/Presentations/Plan_En.pdf.

[28] Ahmed El Bermawy "NTRA deny monitoring social media and sms" Masress, January 20, 2013, http://masress.com/dostor/65762.

LIMITS ON CONTENT

While the Egyptian government does not block unfavorable or controversial websites, it does manage to place significant limits on online content through more nuanced means. There have also been contentious court decisions to block YouTube and pornography, though so far the MCIT has refused to implement these on the grounds that they are unfeasible. In the country's highly-polarized environment, Egypt's political parties and social movements vie for online supremacy. The heads of state media companies were replaced with sympathizers of the Muslim Brotherhood, who have also built their own formidable online media apparatuses to spread propaganda and rally supporters. Nonetheless, citizen journalism and social media activism have retained their importance in the country, where official statements by the presidency, the opposition, and the military are often made on Facebook before they are presented on traditional sources.

Web 2.0 tools such as YouTube, Facebook, Twitter and international blog-hosting services are freely available. VoIP services are largely available, even if it is technically illegal to make international calls from mobile networks under Article 72 of the Telecommunications Law, which forbids the "by-passing [of] international telephone calls by any means whatsoever."[29] Thus, VoIP calls through services such as Skype and Viber can only officially be placed over fixed-line or Wi-Fi networks, not through 3G.[30] However, as mentioned above, VoIP tools are often temporarily blocked or rendered inaccessible through the throttling of bandwidth.

Egypt's courts have made a number of high-profile rulings to block online content. In late 2012, Egypt's prosecutor-general ordered government ministries to implement a 2009 ban on pornographic websites. While no action has yet been taken, its feasibility was reportedly debated at the MCIT. The cost of implementing such a ban is estimated at around EGP 25 million ($4 million), a hefty figure when considering the country's economic woes.[31] Several civil society organizations have criticized the court decision, stating that the banning of content for cultural or religious grounds could eventually lead to increased censorship. Nevertheless, several ISPs have already implemented the court decision on a voluntarily basis, offering a "safe internet service" to subscribers.

Another controversial court decision involved the banning of YouTube for a month in retaliation to the site hosting the offensive "Innocence of Muslims" video clip.[32] The February 9, 2013 order was not implemented by the MCIT, which claimed the block would be too expensive and did not fall under the ministry's legal authority. Appeals were filed by both the ministry and the Association for Freedom of Thought and Expression in Egypt, a local rights group.[33]

---

[29] "Telecommunication Regulation Law, Law No. 10 of 2003," February 2003, Arab Republic of Egypt.
[30] "Egypt banks VoIP services from operators such as Skype," BBC News, March 24, 2010, http://news.bbc.co.uk/2/hi/technology/8585998.stm.
[31] Ingy Hassieb, "Egypt moves to block access to pornography," LA Times, April 4, 2013, http://www.latimes.com/news/world/worldnow/la-fg-wn-egypt-access-pornography-20130404,0,1516553.story.
[32] Al Balad "Banning YOUTUBE for 30 days " http://albaladoman.com/?p=8446.
[33] "Egypt telecoms authority says can't block YouTube," The Daily Star (Lebanon), February 16, 2013, http://bit.ly/1bXbFaA.

While the courts have yet to force the blocking or deletion of these sites, users have taken up more informal tactics to force the deletion of social media accounts or groups that express views to which they are opposed. Facebook groups like "Ana Asf ya Rayes" have had their accounts suspended by Facebook users sympathetic to the Muslim Brotherhood, citing fabricated copyright or terms of use violations.[34] The group had also received threats after calling for protests against the Brotherhood's acquisition of power.[35]

In a separate tactic, online posts and comments are also censored by webmasters and page moderators. The editors of state media websites deliberately delete posts that are critical toward the government and actively drum up support for state policies. This echoes the degree of self-censorship exercised in traditional media, where journalists employ a sense of caution when tackling subjects such as the presidency, the military, and Muslim-Christian relations. Nonetheless, the generation of online activists and bloggers that has grown from the January 25 revolution has become increasingly vociferous in their coverage of sensitive subjects.

As social media has exploded, so too have attempts by political parties, the military, and the government to communicate and often spread propaganda on their official Facebook and Twitter accounts. All emerging political parties, social movements, government offices, and military bodies have started to actively participate in online discussions on the state of the country.[36] The popularity of social media has also galvanized the spread of gossip and rumors, further polarizing the country's politics.

More unofficially, armies of micro-bloggers writing in English and Arabic have steered online discussions in favor of the Morsi government, [37] reportedly with control and even payment from the Muslim Brotherhood.[38] Several pro-Muslim Brotherhood figures have been installed into leadership positions within the media and telecommunication industries, including Salah Abdel Maksoud, the former director of Morsi's presidential campaign who was later appointed Information Minister. Online media outlets have hinted at the mounting pressure they receive from the government,[39] the Muslim Brotherhood, Salafists, and their sympathetic groups to regulate content.[40] In addition, Islamists have created a "Committee for the Promotion of Virtue and Prevention of Vice," modeled after their counterparts in Saudi Arabia, to monitor access to ICTs and ensure "moral" use of the internet, particularly at cybercafés.[41] A Facebook page linked to the

[34] El Fagr "The suspension of Ana Asf ya Rays and the Brotherhood" http://new.elfagr.org/Detail.aspx?nwsId=301412&secid=1&vid=2.
[35] Mohamed ashour "Our page is closed, we got threats of beat and dragging in the streets from the Brotherhood" 14 March 2013 Al Watan news http://www.elwatannews.com/news/details/146611.
[36] "Internet in Eypt: from an Opposition avenue to a political playground," DW.de, March 21, 2012, http://dw.de/p/14N4s.
[37] See for example: "Twitter Discussions & Trends," Isqat Al-Nizam, last modified March 5, 2012, accessed June 30, 2012, http://wiki.aucegypt.edu/isqatalnizam/index.php/Twitter_Discussion_%26_Trends.
[38] Nady Atef "Youth of Egypt create their own website to Defend the brotherhood," El Gomaa, December 12, 2012, http://www.elgomaa.com/article.php?id=82640, and Sshar Khamis et al. "Beyond Egypt's 'Facebook Revolution' and Syria's 'YouTube Uprising': Comparing Political Contexts, Actors and Communication Strategies," *Arab Media and Society* http://www.arabmediasociety.com/articles/downloads/20120407120519_khamis_gold_vaughn.pdf, accessed 12 June 2013.
[39] Revolution Youth "It is not safe to work as a journalist in Egypt under Brtherhood rule" http://bit.ly/GzrozK.
[40] Diaa Rashwan "Journalism is in real threat" http://www.copts-united.com/article.php?I=410&A=88186, and "National Movement warns from journalism siege", Masrawy, http://bit.ly/1fDhUmA.
[41] Katerina Nikolas, "Egypt unleashes Islamic morality police force," Digital Journal, March 3, 2013, http://bit.ly/1fX6NCu.

committee was closed in July 2012 after its members claimed responsibility for the killing of a student in Suez.[42]

The Muslim Brotherhood's online strength was clear during the May-June 2012 presidential election. Users linked to the Brotherhood's Rassd News Network (RNN) provided live updates and published a Google spreadsheet of the election results before all ballots were counted.[43] Several entities accused the Muslim Brotherhood and Freedom and Justice Party (FJP) micro-bloggers of manipulating the election by pushing voters towards an acceptance of Morsi as the new president.[44]

After the elections, the FJP continued to invest in digital strategies to manipulate popular opinion.[45] RNN has grown from a Facebook page[46] to become one of the main online news portals in post-Mubarak Egypt.[47] In addition, a leaked document from the office of the president revealed a policy in which news was first circulated to media outlets sympathetic to the Brotherhood.[48] Similar techniques were used by Morsi's predecessors.

Online news websites have begun to replace traditional news sources due to their immediate and interactive nature, and because they allow for audience participation and cover topics not tackled by the traditional media. Regionally, Egyptian online news outlets are some of the most visited websites in the Middle East, representing 45 percent of online news content from the Arab world.[49] Through state media and independent news outlets, Egyptians can access a variety of viewpoints from the different political and social groups of society.

Content from citizen journalism and blogs have even become the raw material for private and independent media. Egyptian bloggers collect and disseminate information about the arrests of activists and acts of torture by the government or non-state actors.[50] Bloggers such as Alaa Abdel Fattah, Wael Abbas, Ahmed Doma, and Asmaa Mahfouz have become media celebrities in recognition of their work. Numerous well-known figures who write under their real names continue to push the limits of freedom of expression online, even at great risk to their personal safety.[51]

---

[42] "Facebook group shut down after members claim responsibility for Suez death," Egypt Independent, July 5, 2012, http://www.egyptindependent.com/news/facebook-group-shut-down-after-members-claim-responsibility-suez-death.
[43] Anadol "Egypt cancels all Google services within days" http://www.aa.com.tr/ar/rss/132539
[44] Omar Aysha "How Egypt is Discussing the Presidential Elections on Facebook and Twitter," Wamda, June 17, 2012, http://www.wamda.com/2012/06/how-egypt-is-discussing-the-presidential-elections-on-facebook-and-twitter.
[45] See video "Amr Adibb exposes the network of electronic monitoring and commities of the Brotherhood," uploaded by user "benetton zamalek," July 12, 2012, YouTube, http://www.youtube.com/watch?v=yjmxPNeV6xU.
[46] The English language page for RNN can be found at https://www.facebook.com/RNN.World.
[47] See http://www.rassd.com.
[48] AlWatan "Mistaken message reveals that the president prefers Youm 7 and Al Shurook over the rest of the newspapers" http://www.elwatannews.com/news/details/148174.
[49] Ahmed El Gody, *Journalism in a Network: The Role of ICTs in Egyptian Newsrooms* (Örebro: Örebro University Press, 2012).
[50] Osama Diab, "New Egypt, new media," The Guardian, March 10, 2011, http://www.guardian.co.uk/commentisfree/2011/mar/10/egypt-media-newspapers-mubarak-propaganda.
[51] Khan, A. A (2012). "The Role Social of Media and Modern Technology in Arabs Spring". *Far East Journal Of Psychology & Business http://econpapers.repec.org/article/fejarticl/v_3a7a_3ay_3a2012_3ai_3a4_3ap_3a56-63.htm.*

Egyptian human rights groups and civil society organizations make extensive use of social media and blogs in order to document human rights violations and expose government hypocrisy. With over 11 million accounts,[52] Egyptians represent a quarter of all Facebook users in the Arab world.[53] Furthermore, groups like "The Egyptian Movement for Change" (*Kefaya*), the 6th of April Movement, and *Shayfenkom* ("We Can See You") have been successful in rallying for political causes through the use of social-networking sites.[54] The "No Military Trials for Civilians" campaign has been successful in garnering support, using Google Spreadsheets to chronicle hundreds of instances of arbitrary detention in military courts since the revolution.[55] Finally, the "Morsi Meter" website gained notoriety as it evaluated the first 100 days of President's Morsi's term of office and his lack of success in meeting a number of promises he made upon being elected.[56]

VIOLATIONS OF USER RIGHTS

Violations against users continued to grow between May 2012 and April 2013, with several bloggers and activists threatened, beaten, harassed, and killed. The government prosecutes and intimidates users through the continued use of Mubarak-era laws to silence dissent.[57] The number of lawsuits related to insulting the office of the president skyrocketed in the first six months of President Morsi's term, eclipsing the total number of citizens that were convicted during former president Mubarak's entire 30 years in office.[58] In another trend, blasphemy charges continue to pose a threat in the post-Mubarak period, with several users arrested and charged for insulting religion. Most worryingly, the period from May 2012 through April 2013 has seen an increase in extralegal abductions and targeted killings, with several administrators of Facebook groups reportedly singled out and shot by snipers during protests. These actions are reflective overall of the deteriorating environment in Egypt, in which documented attacks on journalists have gone up tremendously since the January 2011 revolution, including three deaths and 42 cases of temporary detentions.[59] In line with some observers' perceptions that the Muslim Brotherhood sought to transform existing state structures in an attempt to remain in power, senior officials in the office of President Morsi staged a high-profile meeting with Iran's spy chief, in which they reportedly sought Iranian assistance in developing new security and intelligence arms. The move was interpreted by some as an attempt to build surveillance capabilities directly under control of the president, thereby reducing institutional reliance on the military.

---

[52] "Study: Egypt ranks 19th in Facebook users," July 31, 2012, http://www.egyptindependent.com/news/study-egypt-ranks-19th-facebook-users.
[53] "Egypt, the Biggest Facebook User Population in the Region," MCIT, November 28, 2012, http://www.mcit.gov.eg/Media_Center/Latest_News/News/2491.
[54] Naayem Saad Zaghloul, *Electronic Mass Communication in Egypt: Reality and Challenges* (Cairo: Egyptian Cabinet, Information and Decision Support Center, February 2010), 38.
[55] See "No to Military Trials for Civilians," http://en.nomiltrials.com/p/detainees-list.html.
[56] "Morsi Meter!" http://www.morsimeter.com/en.
[57] Hannah Grigg, 2013, "Freedom to Criticize Under Attack in the Middle East and North Africa" *Atlantic Council* http://www.acus.org/viewpoint/freedom-criticize-under-attack-middle-east-and-north-africa.
[58] Nick Gjorvad, "The 'insult' of political criticism," Daily News Egypt, February 20, 2013, http://www.dailynewsegypt.com/2013/02/20/the-insult-of-political-criticism/.
[59] "Hundreds of journalists attacked in Egypt since revolution, study finds," FoxNews.com, May 30, 2013, http://www.foxnews.com/world/2013/05/30/hundreds-journalists-attacked-in-egypt-since-revolution-study-finds/.

Although President Morsi and the Muslim Brotherhood-led government pay tribute to concepts such as free speech and freedom of the press in their rhetoric, the reality has proven otherwise. While freedom of expression and religion are guaranteed by the Egyptian constitution, it is forbidden to insult religion or religious prophets. Similarly, media freedom is guaranteed, though the press must respect individuals' privacy, the essential elements of state and society, and the requirements of national security. Censorship is officially forbidden except for times of war or "public mobilization." The constitution also grants the right to privacy and states that no telecommunications activity can be intercepted or inspected without a court order.[60]

Local civil rights advocates have argued that any new constitutional rights are inexistent in practice, due to the continued presence of restrictive laws such as the Press Law, the Law on the Protection of the Nation and Citizens, the Law on Security of National Unity, the Publications Laws, the Telecommunications Law, and the Emergency Law. While the emergency law was not renewed on May 31, 2012, the president retains broad powers to confiscate, suspend or shutdown all means of communication during emergencies.

A series of actions by President Morsi have weakened the independence of the judiciary, leading to the harsh application of existing laws against political opponents of Morsi.[61] In November 2012, President Morsi established a special court and prosecution office for crimes such as insulting state authorities, destroying public property, blocking transportation flows, as well as "press crimes, intimidation and terrorizing."[62] At the same time, Morsi published a constitutional declaration which prohibited the judiciary from challenging his authority or appealing his decrees. Morsi also contravened existing laws by dismissing the public prosecutor before his term had ended.[63]

The new prosecutor has been blasted by local civil society organizations for consistently and disproportionately targeting liberal activists, members of Egypt's independent media, and online users who criticize the president.[64] A case was launched against video blogger Ahmed Anwar in March 2013 over a satirical video he uploaded one year previously, in which he made fun of the police.[65] He was charged with insulting the Ministry of Interior, "abuse of the internet," and provocation, liable to a fine ranging from 20,000 to 100,000 Egyptian pounds ($2,900 to $14,000)

[60] "The 2012 Constitution of Egypt, Translated by Nivien Saleh, with Index," Nivien Saleh, Accessed April 17, 2013, http://niviensaleh.info/constitution-egypt-2012-translation/.
[61] David D. Kirkpatrick, "Block to Transition as Court Dissolves Egypt's Parliament," *New York Times*, June 14, 2012, available at http://www.nytimes.com/2012/06/15/world/middleeast/new-political-showdown-in-egypt-as-court-invalidates-parliament.html?pagewanted=all.
[62] "Egypt: Morsy Decree Undermines Rules of Law," Human Rights Watch, November 26, 2012, http://www.hrw.org/news/2012/11/26/egypt-morsy-decree-undermines-rule-law.
[63] "Egypt's judges call for national strike over Mursi decree," BBC News, November 24, 2012, http://www.bbc.co.uk/news/world-middle-east-20476693.
[64] "Egypt's top judicial body urges prosecutor to quit," Reuters, April 7, 2013, http://www.reuters.com/article/2013/04/07/us-egypt-prosecutor-idUSBRE93605S20130407.
[65] Brian Dooley, "Dancing Cops' Video Blogger Says Freedom of Expression Under Attack in Egypt," Huffington Post, May 15, 2013, http://www.huffingtonpost.com/brian-dooley/dancing-cops-video-blogge_b_3280569.html.

and possible imprisonment.[66] Local rights groups highlighted the case as yet another example of the government's attempts to silence its critics.[67]

In total, 24 cases and complaints of "insulting the president" have been filed in the first 6 months of Morsi's time in office, compared to only 4 cases during former president Mubarak's 30 years in power. Three of these cases were filed directly by the office of the Egyptian president. Bloggers, human rights defenders, members of civil society organizations, and journalists have been summoned by the public prosecutor and investigated under special courts of the state security apparatus, rather than the normal judiciary,[68] in contravention of Article 198 of the new constitution.[69]

As mentioned previously, several of Egypt's high-profile political activists also maintain a social media presence to interact with followers, document human rights violations, and mobilize protests. In many cases, their online activities have been key in building a local following and, conversely, in bringing unwanted attention from the police and security forces. Among many examples, veteran blogger and human rights activist Alaa Abd al-Fattah was arrested in March 2013 on charges of "provoking violence," related to clashes between government protestors and Muslim Brotherhood supporters outside the organization's headquarters in Moqattam.[70] It was reported by several outlets that Abd El Fattah was detained over a Twitter post by a user under the name "Princess Joumana" in which he was mentioned, sparking concerns from the government that the blogger was collaborating with Gulf Arab monarchs against the Brotherhood.[71] In July 2013, he was acquitted of all charges.[72]

On April 30, 2013, state prosecutors in the northern city of Tanta detained popular blogger and activist Ahmed Douma on charges of insulting the president and disseminating false news.[73] One month later, he was sentenced to six months in prison for calling President Morsi a murderer and a criminal.[74] He was eventually released on July 6, though he remains on trial for inciting violence during the March 2013 protests outside of the Muslim Brotherhood's headquarters.[75]

---

[66] Ahmed Aboul Enein, "Blogger faces trial for mocking interior ministry," Daily News Egypt, April 7, 2013, http://www.dailynewsegypt.com/2013/04/07/blogger-faces-trial-for-mocking-interior-ministry/.
[67] "Joint Statement Blogger Ahmed Anwar to be tried for insulting Minister of Interior New evidence of government's hostility towards freedom of expression," The Arabic Network for Human Rights Information, April 7, 2013, http://www.anhri.net/en/?p=12131.
[68] "Increasing crackdown on fundamental freedoms," International Federation for Human Rights (FIDH), April 3, 2013, http://www.fidh.org/Increasing-crackdown-on-fundamental-freedoms-13119.
[69] "The 2012 Constitution of Egypt, Translated by Nivien Saleh, with Index," Nivien Saleh, Accessed April 17, 2013, http://niviensaleh.info/constitution-egypt-2012-translation/#art-198.
[70] Aswat Masrya "Update: Egypt prosecutor orders activists arrested," Aswat Masriya, 25 March 2013 http://en.aswatmasriya.com/news/view.aspx?id=b6f07087-3b9f-4e8b-8fe8-20e5378e329d.
[71] Jillian C. York, "Egypt's Key Bloggers Face Absurd Legal Charges, Harassment," Electronic Frontier Foundation, April 2, 2013, https://www.eff.org/deeplinks/2013/04/egypt-blogger-crackdown.
[72] "Court acquits 12 activists in march violence at Brotherhood HQ," Egypt Independent, July 7, 2013, http://www.egyptindependent.com/news/breaking-prosecutor-orders-release-activist-alaa-abdel-fattah.
[73] "Egyptian activist Ahmed Douma detained for insulting president," Ahram Online, April 30, 2013, http://bit.ly/11BZEOU.
[74] "Activist Douma gets 6 months in prison for 'insulting president'," Ahram Oneline, June 3, 2013, http://bit.ly/18MCzjM.
[75] "Prominent Egyptian blogger released from jail, remains on trial," Reuters, July 6, 2013, http://www.reuters.com/article/2013/07/06/us-egypt-blogger-idUSBRE96506A20130706.

The fall of the Mubarak regime has also resulted in a greater openness to prosecute citizens for religious-based offenses, particularly as Islamist parties have gained in popularity and prominence amid the state apparatus. In July 2012, Beshoy Kamel was sentenced to six years in jail for allegedly insulting religion, President Morsi, and a Salafist man's family over Facebook.[76] Kamel, a Christian teacher in the central Egyptian city of Sohag, had previously posted a warning on his Facebook page that his account had been hacked. Nonetheless, Mostafa Safwat, a local Salafist, filed a complaint after receiving a private message from Kamel's account in which his family was allegedly insulted. Kamel's conviction was upheld in September 2012.[77]

Ahmed Saber, a computer science graduate and online activist, was sentenced to three years imprisonment for "defamation of religion" on December 12, 2012.[78] Saber was arrested on September 13 after an angry mob had showed up at his house and accused him of posting the "Innocence of Muslims" video which mocks the Prophet Mohammed. After Saber alerted the police to protect him, he was instead detained and had his personal belongings confiscated without a warrant.[79] While investigators found no evidence that he had posted the video, he was prosecuted for a video found at his home in which he is seen questioning the value of organized religion.[80] Prosecutors also charged Saber, an atheist who comes from a Christian family, with fomenting religious discord through the publication of writings, images, and videos to social networks, such as his Facebook page "Egyptian Atheists."[81]

In a largely symbolic gesture, seven Egyptian citizens of the Coptic faith were sentenced to death in absentia for their role in the making of the "Innocence of Muslims" video. The sentence was passed on November 28, 2012, two months after massive protests outside of the American Embassy. Thousands of Egyptians had marched on the embassy in Cairo in anger over the short, offensive video, climbing the walls and replacing the American flag with a black flag containing the words, "There is only one God but God and Mohammed is His messenger.[82] All seven of those convicted were living outside of the country.[83]

In addition, Gamal Abdou Massoud remains in jail after being sentenced in April 2012 to three years in jail for posting cartoons to his Facebook page that allegedly insulted Islam and the Prophet Mohammed. Massoud, a Coptic Christian from the central city of Assiut, was 17 years old at the

[76] Ben Hubbard and Mayy El Sheikh, "Islamists Press Blasphemy Cases in a New Egypt," The New York Times, June 18, 2013, http://www.nytimes.com/2013/06/19/world/middleeast/islamists-press-blasphemy-cases-in-a-new-egypt.html?pagewanted=all.
[77] Kristen Chick, "Egypt pursues blasphemy cases as Morsi defends ban at UN," The Christian Science Monitor, September 27, 2012, http://bit.ly/TIvcU5.
[78] "Egypt: 'Outrages' guilty verdict in blasphemy case an assault on free expression," Amnesty International, December 12, 2012, http://www.amnesty.org/en/news/egypt-outrageous-guilty-verdict-blasphemy-case-assault-free-expression-2012-12-12.
[79] Kristen Chick, "'Insulting religion': Blasphemy sentence in Egypt sends a chill," The Christian Science Monitor, December 12, 2012, http://www.csmonitor.com/World/Middle-East/2012/1212/Insulting-religion-Blasphemy-sentence-in-Egypt-sends-a-chill.
[80] Kristen Chick, "Egypt pursues blasphemy cases as Morsi defends ban at UN," The Christian Science Monitor.
[81] "Blogger put on trial for insulting religion," Egypt Independent, September 24, 2012, http://www.egyptindependent.com/news/blogger-put-trial-insulting-religion.
[82] "US envoy dies in Benghazi consulate attack," Al Jazeera English, September 12, 2012, http://www.aljazeera.com/news/middleeast/2012/09/20129112108737726.html.
[83] Jackey Fortin, "Egypt Sentences Christians to Death for Insulting Islam, Charges US Pastor Terry Jones," International Business Times, November 28, 2012, http://bit.ly/V1cS5b.

time. The posting of the cartoons led to attacks by groups of Muslims against Christians, who also saw their homes torched.[84]

There were also numerous cases in which prominent activists, well-known for their online activities, were detained for suspicious or weak charges related to their offline activities. Human rights defender Hassan Mustafa was sentenced to two years imprisonment in March 2013 on charges of allegedly assaulting a member of the Alexandria Prosecution Office.[85] Mustafa is an activist and campaigner who was heavily involved in the rights movement "Hashd" and the online campaign "We Are All Khaled Said." Later in March, Mahinour al-Masry and 12 other activists were arrested on charges related to the storming of the Raml Police Station in Alexandria. Mahinour al-Masry is a well-known human rights defender and a contributor to the news website Ahram Online. Clashes had broken out earlier between activists from the Freedom and Justice Party (FJP) and the *al-Dostour* (Constitutional) party, after an FJP member objected to being filmed by activists from the latter party. That same day, photographer Sameh Mashali, a youth activist known for documenting protests, was arrested. Protestors at the scene claimed that Brotherhood members had captured Mashali and beaten him before handing him over to the police.[86]

Extralegal violence by police authorities in Egypt has become commonplace, with reports of officers using excessive force against demonstrators and seeking vigilante justice for attacks on their colleagues with no respect for the rule of law.[87] In the first six months of President Morsi's term, there have been 11 documented cases of targeted abductions and instances of torture reported by the Al-Nadeem Center for Rehabilitation of Victims and Violence.[88] Rights groups have complained that public prosecutors refuse to investigate these abductions and arbitrary detentions.[89] Countless activists have also been targeted and tortured by thugs affiliated to the Muslim Brotherhood or its political arm, the Freedom and Justice Party (FJP).[90] Reports indicate the Brotherhood has created its own parallel security apparatuses to monitor online dissidents, target specific activists at protests, and attempt to force confessions from individuals held captive in their hidden torture chambers.[91] Several key figures in the FJP stated that they hold "recordings" of opposition figures and have "records" of online dissidents.

---

[84] Ahmed Tolba and Mohamed Abdellah, "Egypt jails Christian student to three years in jail for insulting Islam," Reuters, April 4, 2012, http://blogs.reuters.com/faithworld/2012/04/04/egypt-jails-christian-student-to-three-years-in-jail-for-insulting-islam/.
[85] El Nadeem, 2013, Egypt: Human rights defender Mr Hassan Mustafa sentenced to two years imprisonment March 14, 2013 https://www.facebook.com/notes/el-nadeem/egypt-human-rights-defender-mr-hassan-mustafa-sentenced-to-two-years-imprisonmen/10151564974389365.
[86] Sara Abou Bakr, "Targeting Activists in the Ikhawni state," Daily News Egypt, March 30, 2013, http://www.dailynewsegypt.com/2013/03/30/targeting-activists-in-the-ikhawni-state/.
[87] "State crimes remained unpunished: the Interior Ministry is above the law and the Prosecution is missing in action," Egyptian Initiative for Personal Rights, January 22, 2013, http://eipr.org/en/report/2013/01/22/1602.
[88] Mai Shams El-Din, "Violence against activists becomes more systematic, observers say," Egypt Independent, March 11, 2013, http://www.egyptindependent.com/news/violence-against-activists-becomes-more-systematic-observers-say.
[89] Mai Shams El-Din, "No to Military Trials slams state thuggery," August 7, 2012, http://www.egyptindependent.com/news/no-military-trials-slams-state-thuggery.
[90] Mohamed El-Garhi, "Al-Masry Al-Youm goes inside the Brotherhood torture chambers," December 7, 2012, http://www.egyptindependent.com/news/al-masry-al-youm-goes-inside-brotherhood-s-torture-chambers.
[91] Yasser Abdel Aziz "Muslim Brotherhood seeks to Control Egyptian Media" http://www.al-monitor.com/pulse/iw/contents/articles/politics/2012/11/muslim-brotherhood-dream-tv.html.

Gaber Salah, known as "Jika," was shot dead by police during demonstrations on Mohamed Mahmoud Street in November 2012.[92] Salah, a 17-year-old online activist and member of the 6th of April Movement,[93] was the administrator of a Facebook group called, "Together Against the Brotherhood." Similarly, Mohamed Hussein Korani ("Christie"), the administrator of the "Ikhwan are liars" page on Facebook, was assassinated in demonstrations in front of the Presidential palace in February 2013.[94] Several activists claimed that Christie was targeted by pro-government militias who posted on their Facebook status that they will take revenge against liberals calling for a change in the new government. Mohamed al-Gendy, an activist from the Popular Current movement that also administered an anti-Brotherhood Facebook group, was killed on February 4th, 2013. It is widely rumored that al-Gendy died in prison after being tortured by state authorities.[95]

In Mahalla, a city in the northern Gharbiya Governorate, Mohamed al-Masry reported that he was kidnapped, beaten, and stabbed by six perpetrators in early March 2013 during an ordeal that lasted one day. Al-Masry is the administrator of the Facebook page "Generation of Change." Mohamed Hassanein, the administrator of "The official page of the union of revolutionary groups" on Facebook, was abducted and beaten by unidentified assailants that month as well. The body of activist Sherif El Serafy was found dead on the Cairo Ismailia highway after being kidnapped on his way to Tahrir square.[96] El Serafy belonged to a youth group calling itself Black Bloc Egypt, which was highly active online in criticizing the Muslim Brotherhood and staging protests.[97] Eight members were detained for 45 days in April 2013 for "spreading terrorism and banned ideas online, possessing firearms, using violence against public servants, and burning down Muslim Brotherhood buildings."[98] Human rights lawyers and researchers have claimed that these low-profile activists were targeted by police as part of a wider campaign to intimidate youth activists while avoiding high-profile news coverage.[99]

Numerous other activists and citizen journalists have been beaten or killed while participating in or filming demonstrations. Photographer Mohamed Nabil suffered a broken leg for documenting a protest outside the Muslim Brotherhood headquarters.[100] A video of a veiled woman being slapped to the ground during the protest went viral on YouTube and led to widespread news coverage.[101]

---

[92] Middle East News Agency "More protestors in Gika's funeral" http://www.almasryalyoum.com/node/1268581.
[93] Sara Abou Bakr, "Jika pronounced dead," Daily News Egypt, November 26, 2012, http://www.dailynewsegypt.com/2012/11/26/jika-pronounced-dead/.
[94] Heba Abdel Sattar "The assassination of Kristi is intentional and authorities are covering the reasons" 7 February 2013 http://gate.ahram.org.eg/News/305728.aspx.
[95] "Popular Current member dies in hospital after being 'tortured'," Egypt Independent, February 4, 2013, http://www.egyptindependent.com/news/popular-current-member-dies-hospital-after-being-tortured.
[96] H Yalla Share "Activist Sherif El Serafy body was found dead" *Yalla Share* http://www.yallashare.com/politicals/2011-11-30-12-03-33/12091----q-q-----.html.
[97] Jared Malsin, "Egypt's Black Bloc – an exclusive interview," Vice, February 2013, http://www.vice.com/read/we-met-some-members-of-egypts-black-bloc.
[98] Zeinab El Guindy, "Meet the Black Bloc: Egypt's most talked about radical opposition group," Ahram Online, June 13, 2013, http://english.ahram.org.eg/NewsContent/1/151/73889/Egypt/Features/Meet-the-Black-Bloc-Egypts-most-talked-about-radic.aspx.
[99] Mai Shams El-Din, "Violence against activists becomes more systematic, observers say," Egypt Independent, March 11, 2013, http://www.egyptindependent.com/news/violence-against-activists-becomes-more-systematic-observers-say.
[100] Mohamad Adam, "Brotherhood headquarters proves to be dangerous territory for protestors," Egypt Independent, March 21, 2013, http://www.egyptindependent.com/news/brotherhood-headquarters-proves-be-dangerous-territory-protesters.
[101] A version of the video can be found at http://www.youtube.com/watch?v=x-SRrP-x5LA.

The woman, Mervat Moussa, is a member of former presidential candidate Hamdeen Sabbahi's Popular Current movement.[102]

Restrictions on anonymity and the use of encryption devices make it easier for these activists to be monitored and singled out by the authorities. Under Article 64 of the 2003 Telecommunications Law, the use of encryption devices is prohibited without the written consent of the NTRA, the military, and national security authorities.[103] In addition, cybercafé customers must provide their names, e-mail addresses, and mobile numbers to receive a personal identification number (PIN) to access the internet. Further, the Telecommunications Law allows the offices of the Presidency, Security, Intelligence, and the Administrative Control Authority to obtain citizens' online information without prior consent for cases that concern national security. In 2013, disputes between the military and the presidency, controlled by the Muslim Brotherhood, led to a politicization of intelligence sharing.

In December 2013, high-level intelligence officials from Egypt and Iran reportedly met in Cairo to discuss the development of new Egyptian surveillance and security capabilities similar to Iran's Islamic Revolutionary Guard Corps (IRGC).[104] The meeting took place between Essam al-Haddad, an advisor to President Morsi, and Qassem Soleimani, Commander of the IRGC Quds Force responsible for external clandestine operations. Observers noted that Egypt's Muslim Brotherhood may have been looking to the IRGC as an example to follow; the IRGC was created in the wake of the 1979 Islamic Revolution as a counterweight to the power of Iran's traditional military, which the late Supreme Leader Ruhollah Khomenei saw as a threat to his power.[105] Similarly, the creation of separate security and intelligence structures, independent from the Egyptian military and under the direct control of the president, would be an important victory in the ongoing power struggle between the military – Egypt's strongest institution – and the Muslim Brotherhood.

Regarding cooperation between state security structures and the private sector, ISPs and mobile operators are obliged to maintain a database of their customers and to allow the government to access their databases. After the ending of a grace period issued by the MCIT, customers who do not have their National ID numbers registered with their phone companies will have their phone lines cut. The NTRA suggested that it would suspend additional phone numbers for mobile operators who fail to abide by the new rules.[106] In the past, details emerged that mobile operators Vodafone, Mobinil, and Etisalat had to sign terms of agreement that bound them to cooperate with government officials when requested to tap any conversation or monitor any discussion. In an

[102] Activist slapped outside Brotherhood office speaks out," Egypt Independent, March 18, 2013, http://www.egyptindependent.com/news/activist-slapped-outside-brotherhood-office-speaks-out.
[103] "Telecommunication Regulation Law, Law No. 10 of 2003," February 2003, Arab Republic of Egypt.
[104] Hugh Tomlinson, "Iranian spy chief's visit to Cairo was meant to 'send a message to America'," *The Times*, January 8, 2013, http://www.thetimes.co.uk/tto/news/world/middleeast/article3650461.ece.
[105] Greg Bruno, Jayshree Bajoria, Jonathan Masters, "Iran's Revolutionary Guards," Council of Foreign Relations, June 14, 2013, http://www.cfr.org/iran/irans-revolutionary-guards/p14324.
[106] "Mobile operators forced to register customer data," Egypt Independent April 1, 2010, http://www.egyptindependent.com/news/mobile-operators-forced-register-customer-data.

interview, Mobinil founder Naguib Sawiris stated that under the company's terms of agreement, the government had the right to cancel any or all mobile services in the absence of cooperation.[107]

Documents also revealed that the Egyptian government signed agreements with Canadian, German, British, and American software companies that allow close monitoring and hacking into activists' online information. For example, GAMMA and the Boeing/Narus Company supplied the Egyptian government with software equipment to hack dissidents' computers, e-mail, and social media accounts.[108] Egyptian security reportedly used software programs like FinFisher to hack computer systems and perform real-time decryption of social media activities and VoIP communications.[109] As an indication of the government's capabilities, news reports speculated that the authorities only decided to unblock internet access during the revolution in order to make it easy to monitor dissidents' discussions and plans of action online.

Cyberattacks are a widespread concern in Egypt. Several independent outlets, including Youm7 and El Badil, as well as social media pages have accused the authorities of hacking into their sites during times of political unrest, especially during the May-June 2012 presidential election and the March 2013 demonstrations against President Morsi.[110] Furthermore, in March 2013, a report came out indicating that a Pakistani hacker attacked over 200 Egyptian websites, including the site of a government agency and a university.[111] The international hacktivist group "Anonymous" also launched distributed denial-of-service (DDoS) attacks against 30 high-profile Egyptian government websites in December 2012 in protest of the policies of President Morsi.[112]

[107] Stephanie Baker and Mahmood Kassem, "Billionaire Facing Death Threats Says Egypt Risks Becoming Iran," Bloomberg, October 26, 2011, http://bloom.bg/rXPGQE.
[108] Evgeny Morozov, "Political Repression 2.0," September 1, 2011, http://www.nytimes.com/2011/09/02/opinion/political-repression-2-0.html.
[109] Parker Higgins, "Elusive FinFisher Spyware Identified and Analyzed," Electronic Frontier Foundation, July 25, 2012, https://www.eff.org/deeplinks/2012/07/elusive-finfisher-spyware-identified-and-analyzed.
[110] Ahmed El Gody Online Journalism, Citizen Participation and Engagement in Online Journalism in Africa: Trends, Practices and Emerging Cultures (Routledge Advances in Internationalizing Media Studies). Eds. Mabweazara, Hayes, Okoth Mawindi, Jason Whittaker London:Routledge
[111] Sabari Selvan, "Egypt Government, University and 180+ other sites hacked by P@KhTuN," E Hacking News, March 10, 2013, http://www.ehackingnews.com/2013/03/egypt-government-university-sites-hacked.html.
[112] Mohit Kumar, "Anonymous hit Egyptian Government Websites as #OpEgypt," The Hackers News, December 9, 2012, http://www.ehackingnews.com/2013/03/egypt-government-university-sites-hacked.html.

ESTONIA

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	2	1
Limits on Content (0-35)	3	3
Violations of User Rights (0-40)	5	5
Total (0-100)	**10**	**9**

* 0=most free, 100=least free

POPULATION: 1.3 million
INTERNET PENETRATION 2012: 79 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Estonia continues to be one of the most wired countries in the world, with increasing internet access and online participation among citizens (see **OBSTACLES TO ACCESS**).
- The appeal of a 2008 court case involving content host liability for comments posted online is still pending at the European Court of Human Rights (see **LIMITS ON CONTENT**).
- In 2012, the Ministry of Justice initiated the process of amending Estonia's penal code to comply with an EU directive related to the criminalization of hate speech, which became the topic of significant public debate within Estonia (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Estonia ranks among the most wired and technologically advanced countries in the world. With a high internet penetration rate, widespread e-commerce, and e-government services embedded into the daily lives of individuals and organizations, Estonia has become a model for free internet access as a development engine for society. When the country regained independence in 1991 after nearly 50 years of Soviet rule, its infrastructure was in a disastrous condition. The country's new leadership, however, perceived the expansion of information and communication technologies (ICTs) as a key to sustained economic growth and invested heavily in their development.

The first internet connections in the country were introduced in 1992 at academic facilities in Tallinn and Tartu. The national telecommunication monopoly was privatized with the inclusion of Finnish and Swedish telecommunication companies, and a fiber-optic backbone was built with modern fixed and mobile communications services. The government subsequently worked with private and academic entities to initiate a program in 1996 called Tiger Leap, which aimed to establish computers and internet connections in all Estonian schools by 2000. This program helped to build a general level of technological competence and awareness of ICTs among Estonians. Today, with a high level of computer literacy and connectivity already established, the program's focus has shifted from basic concerns such as access, quality, and cost of internet services to discussions about security, anonymity, the protection of private information, and citizens' rights on the internet. Children's safety on the internet is a high priority, and the special program "Targalt Internetis" (Wiser Internet) is dedicated to country-wide training and awareness-building activities on internet safety issues for parents and children. In addition, a majority of users conduct business and e-government transactions over the internet: in 2013, 99.6 percent of banking transactions were done with e-banking services and 95 percent of people declared their income electronically.[1]

Over the past two years, the issue of copyright protection on the internet became a widely debated topic in Estonia, and various organizations that represent the interests of authors and other copyright holders have come forward in an effort to remove copyright-protected content from popular services such as YouTube. Moreover, the issue of legal liability of online forums for the comments posted by anonymous users continues to be watched by free expression advocates, with an important ruling by the European Court of Human Rights expected during 2013.

OBSTACLES TO ACCESS

The number of internet and mobile telephone users in Estonia has grown rapidly in the past 20 years. According to statistics from the International Telecommunication Union (ITU), internet

[1] Estonian Information System's Authority, "Facts about e-Estonia," accessed June 15, 2013, https://www.ria.ee/facts-about-e-estonia/ .

penetration in Estonia reached 79 percent in 2012 (approximately 994,000 people).[2] There were also over 2 million mobile phone subscriptions, translating into a mobile phone penetration rate of 155 percent.[3] This figure is commonly attributed to the widespread use of mobile internet access devices, the growing popularity of machine-to-machine (M2M) services, and the use of more than one mobile phone by individual Estonians.

The first public Wi-Fi area was launched in 2001, and since then the country has developed a system of mobile data networks that enable widespread wireless broadband access. In 2011, the country had over 2,440 free, certified Wi-Fi areas meant for public use, including at cafes, hotels, hospitals, schools, and gas stations, and the government has continued to invest in public Wi-Fi.[4] In addition, a countrywide wireless internet service based on CDMA technology has been deployed and is priced to compete with fixed broadband access. Three mobile operators cover the country with mobile 3G and 3.5G services, and as of May 2013, 4G services covered over 95 percent of Estonian territory. Municipalities in rural areas have been subsidizing local wireless internet deployment efforts, and the country's regulatory framework presents low barriers to market entry, enabling local startups to proliferate.

Estonians use a large variety of internet applications, including search engines (85 percent of users), e-mail (83 percent of users), local online media, news portals, social-networking sites, instant messaging, and Voice over Internet Protocol (VoIP) services.[5] Estonian Public Broadcasting delivers all radio channels and its own TV production services, including news in real time over the internet; it also offers archives of its radio and television programs at no charge to users.

The Estonian Electronic Communications Act was passed in late 2004 and a number of amendments have been added to help develop and promote a free market and fair competition in electronic communications services.[6] Today, there are over 200 operators offering such services, including six mobile phone companies and numerous internet service providers (ISPs). ISPs and other communications companies are required to register with the Estonian Technical Surveillance Authority (ETSA), a branch of the Ministry of Economic Affairs and Communications, though there is no registration fee.[7]

In 2009, the Estonian Internet Foundation was established to manage Estonia's top level domain, ".ee."[8] With its multi-stakeholder foundation, the organization represents the Estonian internet

[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2012, accessed July 1, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[3] International Telecommunication Union (ITU), "Mobile-cellular subscriptions," 2012, accessed July 11, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
[4] Public Wi-Fi Hotspot database in Estonia, accessed July 30, 2013, http://kaardistajad.wifi.ee/avalik.php.
[5] Pille Pruulmann-Vengerfeldt, Margit Keller, and Kristina Reinsalu, "1.1.4 Quality of Life and Civic Involvement in Information Society," *Information Society Yearbook 2009* (Tallinn: Ministry of Economic Affairs and Communications, 2010), http://www.riso.ee/en/pub/2009it/#p=1-1-4.
[6] "Electronic Communications Act," Ministry of Economic Affairs and Communications, accessed March 26, 2009, http://www.mkm.ee/index.php?id=9576.
[7] Estonian Technical Surveillance Authority (ETSA), "Commencement of Provision of Communications Service," accessed February 21, 2013, http://www.tja.ee/index.php?id=11703.
[8] Estonian Internet Foundation, accessed July 30, 2013, http://www.internet.ee/en/.

community internationally and has succeeded in overseeing various internet governance issues such as the domain name registration process. After initial concerns over the foundation's domain registration pricing policy[9] and management capabilities,[10] the foundation's substantive work has been stabilized in 2012-2013. In February 2012, the Estonian Internet Foundation was admitted to the Council of European National Top Level Domain Registries (CENTR).

LIMITS ON CONTENT

Restrictions on internet content and communications in Estonia are among the lightest in the world. YouTube, Facebook, Twitter, LinkedIn and many other international video-sharing and social-networking sites are widely available and popular. Moreover, 32 percent of Estonians use the internet for uploading and sharing original content such as photographs, music, and text—the highest level of shared public communication in Europe.[11] Nevertheless, due in part to Estonia's strong privacy laws, there are some instances of content removal. Most of these cases involve civil court orders to remove inappropriate or off-topic reader comments from online news sites. Comments are similarly removed from online discussion forums and other sites. Generally, users are informed about a given website's privacy policy and rules for commenting, which they are expected to follow. Most of the popular online services have established policies that outline a code of conduct for the responsible and ethical use of their services and have enforcement policies in place.

In 2008, a debate over self-censorship and pre-publication censorship took center stage when the victim of unflattering and largely anonymous comments on a news story filed suit, claiming that web portals must be held responsible for reader comments and screen them before they become public.[12] Website owners argued that they did not have the capacity to monitor and edit all comments made on their sites. Nonetheless, the Estonian courts ruled in favor of the plaintiff, making web portals responsible for all comments posted. The ruling is currently under appeal at the European Court of Human Rights and a decision is expected later in 2013.

In January 2010, a new law on online gambling came into force, requiring all domestic and foreign gambling sites to obtain a special license or face access restrictions. As of June 2012, the Estonian Tax and Customs Board had placed 771 websites on its list of illegal online gambling sites, requiring Estonian ISPs to block them.[13] The list of blocked sites is transparent and is available to the public.

---

[9] The activities of the Estonian Internet Foundation are not subsidized from the state budget; the registration fee covers infrastructure investments, operating costs, and reserve funds.

[10] "Marek-Andres Kauts resigns as board member," Eesti Internet, May 23, 2012, http://www.internet.ee/news/?year=2012&month=5.

[11] "Individuals Using the Internet for Uploading Self-Created Content to Any Website to Be Shared," Eurostat, accessed June 11, 2013, http://appsso.eurostat.ec.europa.eu.

[12] Kaja Koovit, "Big Businessman Goes to War Against Web Portals," Baltic Business News, March 18, 2008, http://www.balticbusinessnews.com/?PublicationId=48694078-50cc-4fe1-b3e4-6e10bc6a5ec1.

[13] The list of restricted websites can be found on the Estonian Tax and Customs Board website: "Ebaseadusliku kaughasartmängu serverite domeeninimed" [Illegal gaming servers, domain names], Tax and Customs Board, accessed June 10, 2013, http://www.emta.ee/public/Kontroll/Must_nimekiri_17.04.2013.pdf .

In 2012, the removal of online content related to possible copyright infringement on YouTube and other streaming services increased, resulting in the removal of over 80,000 videos. This process was greatly facilitated by requests of copyright enforcement organizations representing Estonian authors.[14] Hundreds of videos have been removed from YouTube for copyright violations even though some of the videos were posted by the authors themselves who were apparently not aware of the activities of copyright enforcement organizations representing their rights.[15] All of these requests came from individuals or companies; the Estonian government has not issued any requests for removal of content on any of Google's platforms, including YouTube, since at least 2010.[16]

There are over 70,000 active Estonian-language blogs on the internet, including an increasing number of group, project, and corporate blogs. The vibrancy and activities of the blogosphere are frequently covered by traditional media, particularly when blog discussions center on civic issues. The fact that so many Estonians are both computer literate and connected to the internet has created unique opportunities for the Estonian government. In addition to hosting virtual trade fairs and an online embassy, the Estonian president's office has its own Twitter and Facebook accounts, and releases messages on its YouTube channel.[17]

Estonia has the largest functioning public-key infrastructure[18] in Europe, based on the use of electronic certificates maintained on the national identification (ID) card.[19] More than 1.2 million active ID cards are in use, which enable both electronic authentication and digital signing, and over 40 percent of active ID cards have been used for authentication and digital signature purposes.[20] The Digital Signature Act, adopted in 2000,[21] gives an individual's digital signature the same weight as a handwritten one and requires public authorities to accept digitally-signed documents. Estonian ID cards were used to facilitate electronic voting during the parliamentary elections in 2007 and were used again in the 2009 municipal and European Parliament elections. During the 2011 national parliamentary elections, 140,846 votes were cast over the internet, representing over 20 percent of all votes. In 2013, 95 percent of citizens filed their taxes online, making the web services offered by the tax department the most popular public e-service. Over 63 percent of internet users regularly use e-government services, and 77 percent have indicated their satisfaction with such services.[22]

---

[14] "Preliminary report," Project 451, Institute of Digital Rights, accessed June 17, 2013, http://451.ee/en/preliminary-report/.
[15] "Autorite ühing laseb YouYube'ist videoed eemaldada," ERR News, February 2, 2011, http://uudised.err.ee/index.php?06223519.
[16] Google Transparency Report, "Estonia – Removal Requests," accessed July 11, 2013, http://www.google.com/transparencyreport/removals/government/EE/
[17] "Estonia Launches Embassy in Virtual World Second Life," Sydney Morning Herald, December 5, 2007, http://www.smh.com.au/news/Technology/Estonia-launches-embassy-in-virtual-world-Second-Life/2007/12/05/1196530704693.html; "Estonian President Launches YouTube Video Blog," TopNews.in, December 9, 2008, http://www.topnews.in/estonian-president-launches-youtube-video-blog-297028.
[18] A public-key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates, which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates that map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed.
[19] See the web portal for the ID-card system, http://id.ee/?lang=en.
[20] Ibid., accessed July 15, 2013.
[21] "Digitaalallkirja seadus" [Digital Signature Act], Riigi Teataja, accessed May 21, 2013, https://www.riigiteataja.ee/akt/694375.
[22] Kristina Randver, *Kodanike rahulolu riigi poolt pakutavate avalike e-teenustega, Jaanuar 2010* [Citizens' Satisfaction with the Provision of Public E-Services, January 2010] (Tallinn: TNS Emor, 2010), http://www.riso.ee/et/files/kodanike_rahulolu_avalike_eteenustega_2010.pdf.

VIOLATIONS OF USER RIGHTS

Freedom of speech and freedom of expression are protected by Estonia's constitution and by the country's obligations as an EU member state. Anonymity is unrestricted, and there have been extensive public discussions on anonymity and the respectful use of the internet. Internet access at public access points can be obtained without prior registration.

The Personal Data Protection Act (PDPA), first passed in 1996, restricts the collection and public dissemination of an individual's personal data. No personal information that is considered sensitive—such as political opinions, religious or philosophical beliefs, ethnic or racial origin, sexual behavior, health, or criminal convictions—can be processed without the consent of the individual. The Data Protection Inspectorate (DPI) is the supervisory authority for the PDPA, tasked with "state supervision of the processing of personal data, management of databases and access to public information."[23] The current version of the PDPA came into force in 2008.[24] In 2012, the Estonian DPI initiated 595 investigations on both public and private sector practices in implementing PDPA, an increase of 24 percent from the previous year.[25]

Estonia is currently in the process of amending the Penal Code to comply with the European Council Framework Decision 2008/913/JHA[26] of 28 November 2008 on "combating certain forms and expressions of racism and xenophobia by means of criminal law" in order to establish a framework on hate speech criminalization in the country. In July 2012, the Ministry of Justice initiated proceedings to amend sections 151 and 152 of the penal code, which would lead to a new situation regarding hate speech-related legislation in Estonia.[27] This process is still ongoing and has become the topic of significant public debate within the country.

Estonia launched the Electronic Communications Act on January 1, 2005, aligning itself with EU legislation and replacing the Telecommunications Act. Since January 2008, electronic communications companies have been required to preserve traffic and location data for one year, as defined by the EU Data Retention Directive (2006/24/EC). Companies have been required to retain data on internet access, telephony, and e-mail since March 2009, and must only retain such data that becomes known to them in the course of providing communications services. They must also provide the surveillance agency or security authority with the information at their disposal only when presented with a court order.[28] According to the report of the Estonian Parliament Security Authorities Surveillance Select Committee that oversees the practices of surveillance agencies and

[23] Electronic Privacy Information Center (EPIC) and Privacy International, "Republic of Estonia," in *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (Washington: EPIC, 2007), http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-8.html.
[24] Estonian Data Protection Inspectorate, "Inspectorate," March 14, 2013, http://www.aki.ee/en/inspectorate.
[25] DPI Annual Reports to Estonian Parliament, accessed June 15, 2013, http://www.aki.ee/et/inspektsioon/aastaettekanded.
[26] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0913:en:NOT, accessed May 5, 2013
[27] Office of the High Commissioner for Human Rights, "Tenth and Eleventh Periodic Report on the implementation of the International Convention on the Elimination of all forms of Racial Discrimination in Estonia," January 2013, http://www2.ohchr.org/English/bodies/cerd/docs/CERD.C.EST.10-11.docx.
[28] Electronic Communications Act, translation to English, http://www.legaltext.ee/text/en/X90001K2.htm.

security agencies, there were over 7,400 cases of requests for information based on court orders in 2012, an increase of 9 percent from the previous year.[29] The select committee has been established to exercise supervision over the legality of surveillance and the activities of the Security Police.[30] The committee monitors the conformity of the activities of the Security Police Board with the constitution, the Surveillance Act, and other regulations on security agencies.

There have been no physical attacks against bloggers or online journalists in Estonia, though online discussions are sometimes inflammatory. Following instances of online bullying, sexual harassment, and the misuse of social media in 2009-2010, discussions and public awareness campaigns were launched to involved parents in increasing the protection of children on the internet.[31]

Awareness of the importance of ICT security in both private and business use has increased significantly since the cyberattacks that occurred in the spring of 2007. To protect the country from future attacks, the government adopted a five-year Cyber Security Strategy in 2008 that focuses on the development and implementation of new security measures, increasing competence in cyber security, improving the legal framework, bolstering international cooperation, and raising public awareness.[32] Estonia's cybersecurity strategy is built on strong private-public collaboration[33] and a unique voluntary structure through the National Cyber Defense League.[34] With more than 150 experts participating, the league has simulated different security threat scenarios over the past few years as defense exercises that have served to improve the technical resilience of Estonia's telecommunication networks and other critical infrastructure.

Also in 2008, the North Atlantic Treaty Organization (NATO) established a joint cyberdefense center in Estonia to improve cyberdefense interoperability and provide security support for all NATO members. Since its founding, the center has supported awareness campaigns and academic research on the topic and hosted several high-profile conferences, among other activities.[35] From 2009, the NATO Cooperative Cyber Defense Centre of Excellence has organized an annual International Conference on Cyber Conflict, or CyCon, targeting international experts from governments, the private sector, and academia. CyCon has focused on international cooperation and the legal, regulatory, military, and paramilitary aspects of cybersecurity, with the goal of ensuring the development of a free and secure internet.

---

[29] Overview of Parliament Select Committe activities, http://www.riigikogu.ee/public/Riigikogu/Dokumendid/julgeolekuasutuste_jarelevalve_erikomisjon_2012_.pdf.
[30] "Security Authorities Surveillance Select Committee," Riigikogu: The Parliament of Estonia, April 4, 2011, http://www.riigikogu.ee/index.php?id=42701&parent_id=34615.
[31] Targalt internetis [awareness portal], accessed June 12, 2013, http://www.targaltinternetis.ee.
[32] Cyber Security Strategy Committee, *Cyber Security Strategy* (Tallinn: Ministry of Defence, 2008), http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.
[33] Ibid.
[34] "Estonian Defence League's Cyber Unit," Kaitseliit [Defence League], http://www.kaitseliit.ee/en/cyber-unit.
[35] "Conference on Cyber Conflict," Cooperative Cyber Defense Centre of Excellence (CCD COE), accessed July 15, 2013, http://www.ccdcoe.org/conference2010/.

ETHIOPIA

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	22	22
Limits on Content (0-35)	27	28
Violations of User Rights (0-40)	26	29
Total (0-100)	**75**	**79**

* 0=most free, 100=least free

POPULATION: 87 million
INTERNET PENETRATION 2012: 1 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Prior to the announcement of Prime Minister Meles Zenawi's death in August 2012, speculation over the state of his health led to an intensified crackdown against the media and freedom of expression online (see **INTRODUCTION**).
- The Ethiopian government increased its technological capacity to filter, block, and monitor internet and mobile phone communications, with assistance from the Chinese authorities (see **LIMITS ON CONTENT**).
- The Telecom Fraud Offences Law, enacted in July 2012, toughened restrictions on ICTs and extended the anti-terrorism law and criminal code to electronic communications (see **VIOLATIONS OF USER RIGHTS**).
- Two individuals were prosecuted for their ICT activities, while harsh sentences were upheld for two imprisoned opposition journalists (see **VIOLATIONS OF USER RIGHTS**).
- The commercial spyware toolkit FinFisher was discovered in Ethiopia in August 2012 (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Ethiopia has one of the lowest rates of internet and mobile telephone penetration in the world, as meager infrastructure, a government monopoly over the telecom sector, and obstructive telecom policies have notably hindered the growth of information and communication technologies (ICTs) in the country. Despite low access, the government maintains a strict system of controls over digital media, making Ethiopia the only country in Sub-Saharan Africa to implement nationwide internet filtering. Such a system is made possible by the state's monopoly over the country's only telecom company, Ethio Telecom, which returned to government control after a two-year management contract with France Telecom expired in December 2012. In addition, the government's implementation of deep-packet inspection technology for censorship was indicated when the Tor network, which helps people communicate anonymously online, was blocked in mid-2012.

Prime Minister Meles Zenawi, who ruled Ethiopia for over 20 years, died in August 2012 while seeking treatment for an undisclosed illness. Before his death was officially confirmed on August 20th, widespread media speculation about Zenawi's whereabouts and the state of his health prompted the authorities to intensify its censorship of online content. A series of Muslim protests against religious discrimination in July 2012 also sparked increased efforts to control ICTs, with social media pages and news websites disseminating information about the demonstrations targeted for blocking. Moreover, internet and text messaging speeds were reported to be extremely slow, leading to unconfirmed suspicions that the authorities had deliberately obstructed telecom services as part of a wider crackdown on the Ethiopian Muslim press for its coverage of the demonstrations.

In 2012, legal restrictions on the use and provision of ICTs increased with the enactment of the Telecom Fraud Offences law in September,[1] which toughened a ban on certain advanced internet applications and worryingly extended the 2009 Anti-Terrorism Proclamation and 2004 Criminal Code to electronic communications.[2] Furthermore, the government's ability to monitor online activity and intercept digital communications became more sophisticated with assistance from the Chinese government, while the commercial spyware toolkit FinFisher was discovered in Ethiopia in August 2012.

Repression against bloggers, internet users and mobile phone users continued during the coverage period of this report, with at least two prosecutions reported. After a long trial and months of international advocacy on behalf of the prominent dissident blogger, Eskinder Nega, who was charged with supporting a terrorist group, Nega was found guilty in July 2012 and sentenced to 18 years in prison.[3]

---

[1] "A Proclamation on Telecom Fraud Offence," *Federal Negarit Gazeta* No. 61, September 4, 2012, http://www.abyssinialaw.com/uploads/761.pdf.
[2] Article 19, "Ethiopia: Proclamation on Telecom Fraud Offences," legal analysis, August 6, 2012, http://www.article19.org/resources.php/resource/3401/en/ethiopia:-proclamation-on-telecom-fraud-offences.
[3] William Easterly et al., "The Case of Eskinder Nega," *New York Review of Books*, January 12, 2012, http://www.nybooks.com/articles/archives/2012/jan/12/case-eskinder-nega/?pagination=false; Committee to Protect

OBSTACLES TO ACCESS

In 2012, access to ICTs in Ethiopia remained extremely limited and hampered by slow speeds and the state's tight grip on the telecom sector. Government investments in expanding access to remote areas of the country were found to be associated with political motives.

Internet and mobile phone services were introduced in Ethiopia in 1997 and 1999, respectively.[4] In recent years, the government attempted to increase access through investments in fiber-optic cables, satellite links, and mobile broadband services, investing approximately 10 percent of the country's gross domestic product in the telecom sector over the past decade.[5]

Nevertheless, Ethiopia's telecommunications infrastructure is among the least developed in Africa and is almost entirely absent from rural areas, where about 85 percent of the population resides. As of the end of 2012, internet penetration stood at just 1.5 percent, up slightly from 1.1 percent in 2011, according to the International Telecommunications Union (ITU).[6] Nevertheless, the number of fixed broadband subscriptions increased dramatically from 4,600 subscriptions in 2011 to nearly 38,000 subscriptions in 2012, as reported by the Ministry of Communications and Information Technology, though such subscriptions still only represent a penetration rate of just 0.4 percent.[7]

Mobile phone penetration in 2012 was higher at roughly 24 percent with a little over 20.5 million subscriptions, up from a 17 percent penetration rate in 2011.[8] Meanwhile, the use of internet-enabled mobile devices is increasing, particularly in semi-urban areas.[9] While all of the above reflect very slight improvements over 2011, such penetration rates represent extremely limited access to ICTs by global standards, and an ICT sector that remains far behind the rest of the world.[10] Furthermore, an adult literacy rate of 30 percent means that the majority of Ethiopians would be unable to take full advantage of online resources even if they had access to the

---

Journalists, "Ethiopia Sentences Eskinder, 5 Others on Terror Charges," July 13, 2012, http://cpj.org/2012/07/ethiopia-sentences-eskinder-six-others-on-terror-c.php.

[4] The first use of internet-like electronic communication was in 1993, when the United Nations Economic Commission for Africa launched the Pan African Documentation and Information Service Network (PADISNET) project, establishing electronic communication nodes in several countries, including Ethiopia. PADISNET provided the first store-and-forward email and electronic-bulletin board services in Ethiopia. It was used by a few hundred people, primarily academics, and staff of international agencies or nongovernmental organizations.

[5] World Bank, "Chapter 8: Corruption in the Telecommunications Sector in Ethiopia: A Preliminary Overview," in Janelle Plummer (ed.), *Diagnosing Corruption in Ethiopia*, World Bank Publications, 2012, http://issuu.com/world.bank.publications/docs/9780821395318.

[6] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[7] International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2012."

[8] International Telecommunication Union ,"Mobile-cellular Telephone Subscriptions, 2000-2012."

[9] Markos Lemma, "Disconnected Ethiopian Netizens," *Digital Development Debates* (blog), http://www.digital-development-debates.org/issues/09-prejudice/african-innovation/disconnected-ethiopian-netizens/.

[10] Lishan Adam, "Ethiopia ICT Sector Performance Review 2009/2010," Research ICT Africa, 2010, http://www.researchictafrica.net/publications/Policy_Paper_Series_Towards_Evidence-based_ICT_Policy_and_Regulation_-_Volume_2/Vol%202%20Paper%209%20-%20Ethiopia%20ICT%20Sector%20Performance%20Review%202010.pdf.

technology.[11] Radio remains the principal mass medium through which most Ethiopians stay informed.

The combined cost of purchasing a computer, initiating an internet connection, and usage charges makes internet access beyond the reach of most Ethiopians. According to a study by the ITU, Ethiopia's broadband internet connections are among the most expensive in the world when compared with monthly income, second only to the Central African Republic.[12] Prices are set by the state-controlled Ethio Telecom and kept artificially high, though the telecom introduced a new tariff effective on January 1, 2013 that offers a discount for mobile- and fixed-line international calls in a move to generate more revenue.[13] Other price packages dating from 2011 are still current.[14] These reduced subscription charges from $80 to $13 and monthly fees from over $200 for unlimited usage to $17-41 for 1-4 GB of use. For comparison, the annual gross national income per capita at purchasing power parity was $92.50 per month as of the data available during the coverage period.[15] While these tariffs have rendered the service slightly more affordable—though still relatively expensive—for individual users, cybercafe owners have complained that the lack of an unlimited usage option could hurt the financial viability of their business.[16]

The majority of internet users rely on cybercafes to access the web, and the number of cybercafes has grown in recent years, especially in large cities, after a brief period in 2001–02 during which the government declared them illegal and forced some to shut down. Since July 2002, new cybercafes have been required to register for licenses through the Ethiopian Telecommunications Agency (ETA). Nevertheless, connections are often slow and unreliable. A 2010 study commissioned by Manchester University's School of Education found that accessing an online e-mail account and opening one message took six minutes in a typical cybercafé in the capital, Addis Ababa, with a broadband connection, and as of 2013, such slow speeds are still standard.[17] Independent sources have noted that uploading an attachment to an e-mail can take more than 10 minutes. Meanwhile, internet access via mobile phones is also beset by slow connection speeds. According to a 2012 report by the Internet Society, telecom policy issues and poor connectivity are largely to blame for the country's low internet speeds.[18]

---

[11] UNICEF, "Ethiopia: Statistics," accessed July 16, 2012, http://www.unicef.org/infobycountry/ethiopia_statistics.html#67.
[12] Jonathan Fildes, "UN Reveals Global Disparity in Broadband Access," BBC News, September 2, 2010, http://www.bbc.co.uk/news/technology-11162656.
[13] "Ethio Telecom Reduces Tariff for International Calls," *Addis Fortune* via *All Africa*, January 7, 2013, http://allafrica.com/stories/201301081250.html.
[14] "Residential Tariff," Ethio Telecom, accessed July 16, 2012, http://www.ethiotelecom.et/products/residential-tariff.php.
[15] World Bank, "Gross National Income Per Capital 2011, Atlas method and PPP," World Bank Databank, 2011, accessed July 18, 2012, http://data.worldbank.org/data-catalog/GNI-per-capita-Atlas-and-PPP-table.
[16] Elias Gebreselassie, "Ethio-Telecom Limits EVDO Internet Access," *Addis Fortune*, April 3, 2011, http://addisfortune.com/Vol_10_No_570_Archive/Ethio-Telecom%20Limits%20EVDO%20Internet%20Access.htm; "Ethio-Telecom Unveils Wide-ranging Tariff Changes Across All Services," TeleGeography, April 5, 2011, http://bit.ly/16PXRqz.
[17] Andinet Teshome, *Internet Access in the Capital of Africa* (School of Education, University of Manchester, 2009); EthioTube video, posted by "Kebena," accessed August 06, 2010, http://www.ethiotube.net/video/9655/Internet-Access-in-the-Capital-of-Africa-Addis-Ababa.
[18] Dessalegn Mequanint, "Understanding the Factors that Force Down Ethiopia's Rankings in the Digital Economy and their Implications in the ICT Policy and Strategy," Internet Society, 2012, http://www.internetsociety.org/sites/default/files/Final%20Report_UnderstandingTheFactorsEthiopiaDigitalRankings.pdf.

While internet access is mostly concentrated in urban areas, the government has sought to increase access for government offices and schools in rural areas via satellite links. WoredaNet ("network of district administrations"), for instance, connects over 500 *woredas* (local districts) to regional and central government offices, providing services such as video conferencing and internet access. Similarly, SchoolNet connects over 500 high schools around the country to a gateway that provides video- and audio-streamed educational programming.[19] Internet speeds within these networks, however, remain prohibitively slow and outages are common. Moreover, the two projects have increased the ubiquity of the state as both a service provider and political entity across the country. A 2012 study by the Open Society Foundation noted that the projects have been used to broadcast political messages from the central government in Addis Ababa to teachers, students, and district administrators in the remote parts of the country.[20]

Ethiopia is connected to the international internet via satellite, a fiber-optic cable that passes through Sudan and connects to its international gateway, and another cable that connects through Djibouti to an international undersea cable.[21] In an effort to expand connectivity, the government has reportedly installed several thousand kilometers of fiber-optic cable throughout the country in recent years.[22] There are also plans in place to connect Ethiopia to a global undersea cable network through the East African Submarine Cable System (EASSy) project, which was completed and launched in July 2010, but its effects on Ethiopia have yet to be seen as of mid-2013.[23] Connection to the international internet is centralized via Ethio Telecom, from which cybercafes must purchase their bandwidth.

Ethiopia's centralized backbone makes internet access highly vulnerable to widespread service disruptions at the hands of the authorities. In July 2012, internet and mobile phone text messaging speeds were reported to be extremely slow amid a series of weekly uprisings by Ethiopian Muslims in protest against religious discrimination by the government.[24] During this time, some individuals complained that text messages took days, even weeks, to reach their recipients.[25] Given the role that social media tools and text messaging services played in organizing the demonstrations,[26] many blamed Ethio Telecom for deliberately obstructing service and considered the effort as part of a wider crackdown on the Ethiopian Muslim press for its coverage of the demonstrations.[27]

---

[19] Samuel Kinde, "Internet in Ethiopia: Is Ethiopia Off-Line or Wired to the Rim?" MediaETHIOPIA, November 2007, http://www.mediaethiopia.com/Engineering/Internet_in_Ethiopia_November2007.htm.
[20] Iginio Gagliardone and Nicole Stremlau, "Mapping Digital Media: Digital Media, Conflict and Diasporas in the Horn of Africa," Open Society Foundations, December 2011, http://bit.ly/19iyGxZ.
[21] Hailu Teklehaimanot, "Unraveling ZTE's Network," *Addis Fortune*, August 22, 2010, http://www.addisfortune.com/Interview-Unraveling%20ZTEs%20Network.htm.
[22] Kinde, "Internet in Ethiopia."
[23] Brian Adero, "WIOCC-EASSy Cable Ready for Business," *IT News Africa*, July 23, 2010, http://www.itnewsafrica.com/?p=8419.
[24] "Ethiopia's Muslims Protest Against Being 'Treated Like Terrorists,'" France 24, July 25, 2012, http://observers.france24.com/content/20120725-ethiopia-muslims-protest-labeled-terrorists-addis-ababa-muslim-council-awoliya-mosque-al-ahbash-anawar.
[25] "ETC sucks," Facebook group, accessed June 17, 2013, https://www.facebook.com/groups/112900380991/.
[26] Endalk, "Muslims Take Campaign Online for Religious Independence," *Global Voices*, May 12, 2012, http://globalvoicesonline.org/2012/05/12/ethiopia-muslims-take-campaign-online-for-religious-independence/.
[27] "Ethiopian Authorities Crack Down on Muslim Press," Committee to Protect Journalists, August 9, 2012, http://www.cpj.org/2012/08/ethiopian-authorities-crack-down-on-muslim-press.php.

The internet was last cut-off in May 2011 in the lead up to planned demonstrations inspired by the early-2011 anti-government protests in the Middle East,[28] though it remains unclear whether the cause was a deliberate government attempt to restrict communication at a sensitive time, a technical problem, or sabotage of a fiber-optic cable. Separately, when high-profile international events, such as African Union meetings, take place in Addis Ababa or other major cities, the government has been known to redirect much of the country's bandwidth to the host venues, leaving ordinary users with even slower connections than usual.

The Ethiopian Telecommunications Agency (ETA) is the primary regulatory body overseeing the telecommunications sector. Although it was established as an autonomous federal agency, in practice, the ETA is tightly controlled by the government. In addition, the space for independent initiatives, entrepreneurial or otherwise, is extremely limited.[29] In 2011, the government began granting permission to private companies that run internet-dependent operations to acquire and use VSAT links,[30] connections previously reserved for governmental and international organizations per special authorization.[31] Under the new directive, private companies are supposedly permitted to use the technology for their own operations, but bureaucratic redtape significantly hinders the service.[32] Moreover, the directive does not allow companies to provide services to third parties, enabling Ethio Telecom to maintain its monopoly on public internet access.

Despite repeated international pressure to liberalize telecommunications in Ethiopia, the government has been reluctant to ease its grip on the sector.[33] In early 2013, management of the state-owned Ethio Telecom fell back into government hands after a two-year management agreement with France Telecom expired in December 2012.[34] In addition to this state monopoly, increasing corruption in the telecommunications sector has been highlighted as a major reason for poor and unrealizable telecom services in Ethiopia.[35] According to a 2012 World Bank report, the telecommunications sector in Ethiopia has the highest risk of corruption compared to other sectors assessed, such as land, education, and construction, among others.[36]

---

[28] See Freedom on the Net 2012. Also, "Internet is Down Throughout Ethiopia – Update," *Ethiopian Review*, May 26, 2011, http://www.ethiopianreview.com/content/33165.

[29] Al Shiferaw, "Connecting Telecentres: An Ethiopian Perspective," *Telecentre Magazine*, September 2008, http://bit.ly/16DdF6Z.

[30] "Private VSAT Permit Directive Number 2/2003" as noted in: "Ethiopia to Liberalise VSAT Market," Screen Africa, November 16, 2011, http://www.screenafrica.com/page/news/industry/1097820-Ethiopia-to-liberalise-VSAT-market.

[31] Yelibenwork Ayele, "Companies in Ethiopia Permitted to Use VSAT," *2Merkato*, October 3, 2011, http://www.2merkato.com/20111003380/companies-in-ethiopia-permitted-to-use-vsat.

[32] Jon Evans, "The Unconquered Nation, Crippled By Bureaucrats," *TechCrunch*, May 30, 2011, http://techcrunch.com/2011/05/30/unconquered-nation-crippled-ethiopia-internet/.

[33] "US urge Ethiopia to Liberalise Telecom Sector," *Africa News* via *Somali State*, March 10, 2010, http://www.somalistate.com/englishnewspage.php?articleid=4638; Technology Strategies International, "ICT Investment Opportunities in Ethiopia—2010," March 1, 2010, http://bit.ly/1bmsGvq.

[34] "France Telecom's Management Contract with Ethio Telecom Ends," *Telecompaper*, January 4, 2013, http://www.telecompaper.com/news/france-telecoms-management-contract-with-ethio-telecom-ends--917095; Meraf Leykun, "The Management Contract with France Telecom concluded," *2Merkato*, January 4, 2013, http://www.2merkato.com/the-management-contract-with-france-telecom-concluded.

[35] Gabriella Mulligan, "Ethiopian Telecoms Sector Amongst Most Corrupt in Country," *Humanipo*, January 16, 2013, http://www.humanipo.com/news/3331/Ethiopian-telecoms-sector-amongst-most-corrupt-in-country.

[36] Janelle Plummer (ed.), *Diagnosing Corruption in Ethiopia*.

China has emerged as a key investor and contractor in Ethiopia's telecommunications sector,[37] and in October 2012, the government signed new two-year contracts with the Chinese telecom companies, Zhongxing Telecommunication Corporation (ZTE) and Huawei.[38] Given allegations that the Chinese authorities have provided the Ethiopian government with technology that can be used for political repression—such as surveillance cameras and satellite jamming equipment—in the past,[39] the new contracts have led to increasing fears that the Chinese may also be assisting the authorities in developing more robust internet and mobile phone censorship and surveillance capacities (see "Violations of User Rights").

LIMITS ON CONTENT

Ethiopian authorities persistently deny engaging in online censorship,[40] but the results of the most recent independent tests conducted by the OpenNet Initiative (ONI) in 2012, and checked again by Freedom House in January 2013, indicate otherwise. Both sets of tests found that the Ethiopian government imposes nationwide, politically motivated internet filtering.[41] The blocking of websites is somewhat sporadic, tending to tighten ahead of sensitive political events. This on again, off again dynamic continued throughout 2012, especially during the disappearance of Prime Minister Meles Zenawi and the subsequent announcement of his death in June 2012. There were also indications that the technical sophistication of the government's blocking has increased and that periods of openness are shrinking.

The government's approach to internet filtering has generally entailed hindering access to a list of specific internet protocol (IP) addresses or domain names at the level of the international gateway, though it is believed that the government has been introducing more sophisticated equipment capable of blocking a webpage based on a keyword in the URL path.[42] In May 2012, the Tor network—an online tool that enables users to browse anonymously—was blocked,[43] indicating

[37] Isaac Idun-Arkhurst and James Laing, *The Impact of the Chinese Presence in Africa* (London: africapractice, 2007), http://www.davidandassociates.co.uk/davidandblog/newwork/China_in_Africa_5.pdf.
[38] "ZTE, Huawei to Be Awarded Ethiopian Telecommunications Contracts," Bloomberg, October 12, 2012, http://www.bloomberg.com/news/2012-10-11/zte-huawei-to-be-awarded-ethiopian-telecommunications-contracts.html.
[39] Hilina Alemu, "INSA Installing Street Surveillance Cameras," *Addis Fortune*, March 21, 2010, http://www.addisfortune.com/Vol%2010%20No%20516%20Archive/INSA%20Installing%20Street%20Surrviellance%20Cameras.htm; "China Involved in ESAT Jamming," *Addis Neger*, June 22, 2010, http://addisnegeronline.com/2010/06/china-involved-in-esat-jamming/.
[40] "Ethiopia: Authorities Urged to Unblock Websites," Integrated Regional Information Networks, May 25, 2006, http://www.irinnews.org/report.aspx?reportid=59115.
[41] Irene Poetranto, "Update on Information Controls in Ethiopia," OpenNet Initiative, November 1, 2012, http://opennet.net/blog/2012/11/update-information-controls-ethiopia.
[42] Daniel Berhane, "Ethiopia's Web Filtering: Advanced Technology, Hypocritical Criticisms, Bleeding Constitution," *Daniel Berhane's Blog*, January 16, 2011, http://danielberhane.wordpress.com/2011/01/16/ethiopias-web-filtering-advanced-technology-hypocritical-criticisms-bleeding-constitution/.
[43] "Ethiopia Introduces Deep Packet Inspection," *Tor*, May 31, 2012, https://blog.torproject.org/blog/ethiopia-introduces-deep-packet-inspection.

Ethio Telecom had deployed deep packet inspection to enable more sophisticated, selective filtering of internet traffic.[44]

The most recent ONI tests conducted from September 17-19, 2012 found that filtering by Ethio Telecom focuses primarily on independent online news media, political blogs, and Ethiopian human rights groups' websites.[45] Of the 1,375 unique URLs tested, 73 were blocked, including the online portals, Nazret and Cyber Ethiopia, and the websites of opposition movements such as the Solidarity Committee for Ethiopian Political Prisoners. Numerous news websites and forums reporting on the imprisonment of bloggers and journalists, such as *EthioMedia*, *Addis Voice*, *Addis Neger*, and *Ethiopian Review* were also found blocked,[46] in addition to the circumvention and anonymization tools, Ultrasurf and Psiphon.

While ONI found the websites of international nongovernmental organizations such as Human Rights Watch, Amnesty International, and Reporters Without Borders—all of which have criticized the Ethiopian government's human rights record—unblocked during its September 2012 test, independent tests conducted by Freedom House throughout 2012 found that the websites of Freedom House, Electronic Frontier Foundation, Human Rights Watch, and Amnesty International were inaccessible at irregular intervals. Further, another test conducted by Freedom House in early 2013 found that 70 websites related to news and views, 16 websites belonging to different Ethiopian political parties, 40 blogs, 7 audio-video websites, and 40 Facebook pages were not accessible in Ethiopia.[47] As of April 2013, the above-mentioned websites, as well as those of Ethsat (an independent exile television station) and *Dilethiopia* (an opposition website), remained inaccessible.

International news outlets became increasingly targeted for censorship in the past year. Al Arabiya and both of Al Jazeera's Arabic and English websites were both blocked intermittently throughout 2012 and early 2013,[48] while the *Washington Post* became a new target for blocking after the paper reported on the prime minister's whereabouts in August 2012.[49] The article remained blocked as of April 2013. An online *Forbes* article titled, "Requiem for a Reprobate Ethiopian Tyrant Should Not Be Lionized," which was written in response to the local and global praise of the late prime minister's debatable economic growth achievements, was also effectively blocked in August 2012 and remained so at the time of writing.[50]

In addition, the website of a Swedish state broadcaster was blocked in September 2012 for reporting on the release of two Swedish journalists who had been imprisoned for their alleged

---

[44] Warwick Ashford, "Ethiopian Government Blocks Tor Network Online Anonymity," *Computer Weekly*, June 28, 2012, http://www.computerweekly.com/news/2240158237/Ethiopian-government-blocks-Tor-Network-online-anonymity.
[45] Irene Poetranto, "Update on Information Controls in Ethiopia," OpenNet Initiative, November 1, 2012, http://opennet.net/blog/2012/11/update-information-controls-ethiopia.
[46] Poetranto, "Update on Information Controls in Ethiopia,".
[47] Independent test conducted by Freedom House consultant, early 2013.
[48] "Ethiopia 'Blocks' Al Jazeera Websites," Al Jazeera, March 18, 2013, http://www.aljazeera.com/news/africa/2013/03/201331793613725182.html.
[49] Mohammed Ademo, "Media Restrictions Tighten in Ethiopia," *Columbia Journalism Review*, August 13, 2012, http://www.cjr.org/behind_the_news/ethiopia_news_crackdown.php?page=all.
[50] Research conducted by Freedom House consultant.

support of the Ogaden National Liberation Front rebel group.[51] Certain webpages were also restricted in response to the series of weekly Muslims protests against religious discrimination by the government in mid-2012, including the Facebook page and blog of protest organizers titled, *"Dimtsachin Yisema"* ("Let Our Voice Be Heard"). Al Jazeera's main website was blocked after it published a discussion forum about the continuing Muslim protests.[52]

In the past year, the authorities have become more sophisticated in their censorship techniques, electing to block select webpages as opposed to entire websites. There are also worrying suspicions that the authorities may have learned to block websites hosted on foreign servers. In April 2013, one local human rights activist group confirmed that their website was blocked, despite being hosted on both foreign and mirror servers.[53] In addition, some restrictions are placed on mobile phones, such as the requirement for a text message to obtain prior approval from Ethio Telecom if it is to be sent to more than ten recipients.[54] A bulk text message sent without prior approval is automatically blocked.

Meanwhile, social media platforms such as Facebook, YouTube, and Twitter are available, though worries have increased over potential government plans to block social media tools altogether. These concerns were particularly pronounced following news about Prime Minister Meles Zenawi's health in July 2012, which provoked an intensified crackdown against the media.[55] In response to the public debate circulating online over the prime minister's whereabouts, the state-run Ethiopian television station aired a special program to censure the role of social media in society, blaming it for spreading false rumors, being destructive to society's well-being, hampering productivity, and undermining citizens' rights.[56] The social media curation tool Storify was also blocked during this period.[57]

International blog-hosting platforms such as Blogspot have been frequently blocked since the disputed parliamentary elections of 2005, during which the opposition used online communication tools to organize and disseminate information that was critical of the ruling Ethiopian People's Revolutionary Democratic Front .[58] In 2007, the government instituted a blanket block on the domain names of two popular blog-hosting websites, Blogspot and Nazret, though the authorities have since become more sophisticated in their censorship techniques, now blocking select pages such as the *Zone9* independent blog hosted on Blogspot,[59] as opposed to entire blogging platforms. Nazret, however, remained completely blocked at the end of the coverage period. Circumvention

[51] "Swedish State Television Website Blocked in Ethiopia," *Ethiopian Review*, September 22, 2012, http://www.ethiopianreview.com/forum/viewtopic.php?t=42883&p=239162.
[52] Ademo, "Media Restrictions Tighten in Ethiopia.".
[53] Interview conducted by Freedom House consultant. All interviews were conducted in Ethiopia with subjects who requested anonymity.
[54] Interview with individuals working in the telecom sector, as well as a test conducted by a Freedom House consultant who found it was not possible for an ordinary user to send out a bulk text message.
[55] Ademo, "Media Restrictions Tighten in Ethiopia."
[56] Ademo, "Media Restrictions Tighten in Ethiopia.".
[57] Ademo, "Media Restrictions Tighten in Ethiopia.".
[58] Bogdan Popa, "Google Blocked in Ethiopia," *Softpedia*, May 3, 2007, http://news.softpedia.com/news/Google-Blocked-In-Ethiopia-53799.shtml.
[59] Zone9 blog hosted at: http://zone9ethio.blogspot.com/.

strategies have also been targeted, with the term "proxy" yielding no search results on Google, according to an independent source. Some speculate that the search is being filtered through the URL and instantly redirected to a fake Google website. Meanwhile, the terms "sex" or "porn" are still searchable.

Procedures for determining which websites should be blocked and when are extremely opaque. There are no published lists of blocked websites or publicly available criteria for how such decisions are made, and users are met with an error message when trying to access a blocked website. This lack of transparency is exacerbated by the government's continued denial of its censorship efforts, though in September 2012, the director of the Information Network Security Agency (INSA), Brigadier General Tekleberahan Weldearegay, was quoted in an interview for the government-owned Amharic-language magazine, *Zemen*, underscoring the "necessity" of blocking online content that is harmful to Ethiopian society.[60] Meanwhile, the decision-making process does not appear to be centrally controlled, as various governmental entities—including INSA and Ethio Telecom—seem to be implementing their own lists, contributing to the phenomenon of inconsistent blocking.

In addition to increasing online censorship, politically objectionable content has been targeted for removal, often by way of threats from security officials who personally seek out users and bloggers to instruct them to take down certain content. The growing practice suggests that at least some voices within Ethiopia's small online community are being closely watched. In one notable instance, a video of the late Meles Zenawi being heckled by an activist while in Washington D.C. for a G8 meeting in early 2012 was taken down shortly after it was posted on online. Searching for the video on YouTube and elsewhere has yielded no results except for other non-contentious videos of Zenawi.

Lack of adequate funding represents another challenge for independent online media, as fear of government pressure dissuades Ethiopian businesses from advertising with politically critical websites. The authorities also use regime apologists, paid commentators, and pro-government websites to proactively manipulate the online news and information landscape. Acrimonious exchanges between commentators on apologist websites and a wide array of diaspora critics and opposition forces have become common in online political debates. There was a noticeable increase in the number of pro-government commentators in the past year, especially during the period of speculation over Meles Zanawi's disappearance.

Regime critics and opposition forces in the diaspora increasingly use the internet as a platform for political debate and an indirect avenue for providing information to local newspapers. The domestic Ethiopian blogosphere has been expanding, in spite of the blocks on blogging platforms since 2005, though most of the blogging activity on Ethiopian issues still originates in the diaspora. Furthermore, increased repression against journalists working in the traditional media and a number of bloggers throughout 2012 has generated a chilling effect in the online sphere. Few

[60] D. Tizazu, "Whose Hidden Agenda?" [in Amharic], *Zemen*, 2012.

Ethiopian journalists work for both domestic print media and overseas online outlets as this could draw repercussions, and many bloggers publish anonymously to avoid reprisals.[61]

Over the past two years, Facebook has become one of the most popular mediums through which Ethiopians share and consume information, with the country's Facebook penetration exceeding its rate of internet penetration due to increasing access via mobile phones.[62] Social media websites have also become significant platforms for political deliberation and social justice campaigns. For example, in November 2012 a group of young Ethiopian bloggers and activists based in Addis Ababa launched a Facebook and Twitter campaign to demand that the government respect the fundamental freedoms enshrined in the Ethiopian Constitution,[63] though the campaign ultimately fell on deaf ears. Overall, many civil society groups based in the country are wary of mobilizing against the government, and calls for protest come mostly from the Ethiopian diaspora rather than from local activists who fear the government's tendency toward violent crackdowns against protest movements.

VIOLATIONS OF USER RIGHTS

During the coverage period, the Ethiopian government's already limited space for online expression continued to deteriorate alongside its poor treatment of journalists. In 2012, repression against bloggers and ICT users increased, with several arrests and at least one prosecution reported. The Telecom Fraud Offences law enacted in September 2012 toughened the ban on advanced internet applications and established criminal liability for certain types of content communicated electronically. Furthermore, monitoring of online activity and interception of digital communications intensified, with the deployment of FinFisher surveillance technology against users confirmed in early 2013.

Constitutional provisions guarantee freedom of expression and media freedom in Ethiopia.[64] Nevertheless, in recent years the government has adopted problematic laws that restrict free expression.[65] For one, the 2008 Mass Media and Freedom of Information Proclamation includes a clause that permits only Ethiopian nationals to establish mass media outlets. The media law also prescribes crippling fines, licensing restrictions for establishing a media outlet, and powers allowing the government to impound periodical publications.[66]

[61] Lemma, "Disconnected Ethiopian Netizens."
[62] Lemma, "Disconnected Ethiopian Netizens."
[63] Endalk, "Movement to 'Respect the Constitution' in Ethiopia," *Global Voices*, November 11, 2012, http://globalvoicesonline.org/2012/12/11/movement-to-respect-the-constitution-in-ethiopia/.
[64] "Constitution of the Federal Democratic Republic of Ethiopia, Article 29," Parliament of the Federal Democratic Republic of Ethiopia, accessed August 24, 2010, http://www.ethiopar.net/.
[65] Human Rights Watch, *Analysis of Ethiopia's Draft Anti-Terrorism Law* (New York: Human Rights Watch, 2009), http://www.hrw.org/en/news/2009/06/30/analysis-ethiopia-s-draft-anti-terrorism-law.
[66] "Freedom of the Mass Media and Access to Information Proclamation No. 590/2008," *Federal Negarit Gazeta* No. 64, December 4, 2008.

In 2012, specific legal restrictions on ICT use and provision were enacted with the passage of the Telecom Fraud Offences law in September,[67] which revised a 2002 law that had placed bans on certain advanced communication applications, such as Voice over Internet Protocol (VoIP)—including Skype and Google Voice—call back services, and internet-based fax services.[68] Under the new law, the penalties under the preexisting ban were toughened, increasing the fine and maximum prison sentence from five to eight years for offending service providers and penalizing users with three months to two years in prison.[69] The government first instituted the ban on VoIP in 2002 after it gained popularity as a less expensive means of communication and began draining revenue from the traditional telephone business belonging to the state-owned Ethio Telecom.[70] Despite the restriction on paper, many cybercafés still offer the banned service with no reports of repercussions to date.

The new law also added the requirement for all individuals to register their telecommunications equipment—including smart phones—with the government, which security officials enforce by confiscating ICT equipment when a registration permit cannot be furnished at security checkpoints. Most alarmingly, the Telecom Fraud Offences law extended the 2009 Anti-Terrorism Proclamation and 2004 Criminal Code to electronic communications.[71] Under the anti-terrorism legislation, the publication of a statement that is understood as a direct or indirect encouragement of terrorism, broadly defined, is punishable with up to 20 years in prison.[72] Meanwhile, the criminal code holds any "author, originator or publisher" criminally liable for content allegedly linked to offenses such as treason, espionage, or incitement, which carries with it the penalty of up to life imprisonment or death.[73] The criminal code also penalizes the publication of a "false rumor" with up to three years in prison.[74]

In July 2012, the criminal code was applied to digital communication under the Telecom Fraud Offences law for the first time when Ethiopian Muslim Jemal Kedir was found guilty on charges of spreading false rumors and fomenting hatred through text messages. Comprised of various statements protesting against police mistreatment of the Muslim community, the text messages were used as evidence against Kedir in court, leading to a one-year prison sentence.[75]

---

[67] "A Proclamation on Telecom Fraud Offence," *Federal Negarit Gazeta* No. 61, September 4, 2012, http://www.abyssinialaw.com/uploads/761.pdf.

[68] Ethiopian Telecommunication Agency, "Telecommunication Proclamation No. 281/2002, Article 2(11) and 2(12)," July 2, 2002, accessed July 25, 2012, http://www.eta.gov.et/Scan/Telecom%20Proc%20281_2002%20(amendment)%20NG.pdf. As an amendment to article 24 of the Proclamation, the Sub-Article (3) specifically states, "The use or provision of voice communication or fax services through the internet are prohibited" (page 1782).

[69] "A Proclamation on Telecom Fraud Offence."

[70] Groum Abate, "Internet Cafes Start Registering Users," *Capital*, December 25, 2006, http://www.capitalethiopia.com/index.php?option=com_content&view=article&id=259:internet-cafes-start-registering-users-&catid=12:local-news&Itemid=4.

[71] Article 19, "Ethiopia: Proclamation on Telecom Fraud Offences.".

[72] "Anti-Terrorism Proclamation No. 652/2009," *Federal Negarit Gazeta* No. 57, August 28, 2009.

[73] International Labour Organization, "The Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation No. 414/2004, Article 44," http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/70993/75092/F1429731028/ETH70993.pdf.

[74] "The Criminal Code of the Federal Democratic Republic of Ethiopia."

[75] "Ethiopian Man Jailed for One Year for Inciting Public Disorder Using Text Messages," *Sodere*, October 1, 2012, http://sodere.com/profiles/blogs/ethiopian-man-jailed-for-one-year-for-inciting-public-disorder.

Also in July 2012, the well-known dissident blogger Eskinder Nega was found guilty under the anti-terrorism law and sentenced to 18 years in prison for his alleged links to a terrorist group.[76] Such trumped-up charges were based on an online column Nega had published that criticized the government's use of the Anti-Terrorism Proclamation to silence political dissent and called for greater political freedom in Ethiopia, which led to his arrest in September 2011.[77] Nega appealed the verdict at the Federal Supreme Court in early 2013,[78] but his 18-year sentence was upheld on May 2, 2013 amid global observance of World Press Freedom Day.[79]

In another incident in April 2013, a student at the Addis Ababa University's Information Technology Department was arrested and charged with criminal defamation for his Facebook activity. The 21-year-old, Manyazewal Eshetu, was detained from his home in Addis Ababa after he had posted a comment on his Facebook page that criticized the "rampant corruption" of another local university in Arba Minch town, where he was transported after his arrest. At the end of the coverage period, he remained in prison and had not been prosecuted.[80]

Given the high degree of online repression in Ethiopia, some political commentators use proxy servers and anonymizing tools to hide their identities when publishing online and to circumvent filtering, though the ability to communicate anonymously has become more difficult in the past year. As discussed above, the Tor Network anonymizing tool was blocked in May 2012, confirming that the government has deployed deep-packet inspection technology, and Google searches of the term "proxy" mysteriously yield no results (see "Limits on Content").

Anonymity is further compromised by SIM card registration requirements, which involve the need for consumers to provide their full names, addresses, and government-issued identification numbers upon the purchase of a mobile phone. Internet subscribers are also required to register their personal details, including their home address, with the government. In early 2013, an insider leaked worrying details of potential government efforts to draft legislation that seeks to mandate real-name registration for all internet use in Ethiopia.[81]

Government surveillance of online and mobile phone communications is a major concern in Ethiopia, and evidence is emerging regarding the scale of such practices. Increasing Chinese investment in Ethiopia's telecommunications sector over the past few years has led to reports of the government using Chinese technology to monitor phone lines and various types of online

[76] Nega is also the 2011 recipient of the PEN/Barbara Goldsmith Freedom to Write Award. Sarah Hoffman, "That Bravest and Most Admirable of Writers: PEN Salutes Eskinder Nega," PEN American Center (blog), April 13, 2012, http://www.pen.org/blog/?p=11198. See also, Markos Lemma, "Ethiopia: Online Reactions to Prison Sentence for Dissident Blogger," *Global Voices*, July 15, 2012, http://globalvoicesonline.org/2012/07/15/ethiopia-online-reactions-to-prison-sentence-for-dissident-blogger/.

[77] Endalk, "Ethiopia: Freedom of Expression in Jeopardy," *Global Voices*, February 3, 2012, http://advocacy.globalvoicesonline.org/2012/02/03/ethiopia-freedom-of-expression-in-jeopardy/.

[78] "Ethiopia Delays Appeal of Jailed Blogger," *Africa Review*, December 19, 2012, http://www.africareview.com/News/Ethiopia-delays-appeal-of-jailed-blogger/-/979180/1647624/-/mm610r/-/index.html.

[79] "Eskinder Nega's 18-Year Sentence Upheld," PEN America Blog, May 13, 2013, http://worldvoices.pen.org/rapid-action/2013/05/14/eskinder-negas-18-year-sentence-upheld-four-other-journalists-remain

[80] "Student Arrested for Facebook Post," *Addis Journal*, April 3, 2013, http://arefe.wordpress.com/2013/04/03/student-arrested-for-facebook-post/.

[81] Interview conducted by Freedom House consultant..

communication.[82] Fears of direct assistance from China were affirmed in June 2012 when the Ethiopian government openly held an "Internet Management" media workshop with support from the Chinese Communist Party,[83] and spearheaded by a professor from the Chinese Leadership Academy.[84] According to an official government press release, the main purpose of the workshop was to learn about China's experience regarding "mass media capacity building," "mass media institution management," and "internet management."

In August 2012, Ethiopia was reported to be among a group of 10 countries that possesses the commercial spyware toolkit FinFisher,[85] a device that can secretly monitor computers by turning on webcams, record everything a user types with a key logger, and intercept Skype calls. A leaked document confirmed that the UK-based company, Gamma International, had provided Ethio Telecom with the FinFisher surveillance toolkit at some point between April and July 2012.[86] In addition, research conducted by Citizen Lab in March 2013 worryingly found evidence of an Ethio Telecom-initiated FinSpy campaign launched against users that employed pictures of the opposition group, Ginbot 7, as bait.[87] The Information Network Security Agency (INSA)—which is involved in surveillance as well as content blocking[88]—has also reportedly tested tools that can enable its officials to mask their identities to acquire personal information such as usernames and passwords, according to internal sources working in the industry.[89]

In a series of trials of journalists and bloggers throughout 2012 and early 2013, government prosecutors have presented e-mails and phone calls intercepted from journalists as evidence.[90] For example, on January 8, 2013 the Ethiopian Court of Cassation rejected an appeal for acquittal filed by the award-winning journalist Reeyot Alemu, citing the e-mails she had received from opposition discussion groups as justification.[91] Reports and photos she had sent to the U.S.-based opposition news site, Ethiopian Review, were also used against her. Alemu was imprisoned in June 2011 on a slew of charges under the anti-terrorism law and sentenced to 14 years' imprisonment in January

[82] Helen Epstein, "Cruel Ethiopia," *New York Review of Books*, May 13, 2010, http://www.nybooks.com/articles/archives/2010/may/13/cruel-ethiopia/.
[83] Ethiopian Peoples' Revolutionary Democratic Front "Workshop Conducted," , press release, June 3, 2012, http://www.eprdf.org.et/web/guest/news/-/asset_publisher/c0F7/content/3-june-2012-26-2004.
[84] Patrick Roanhouse, "Ethiopian Government Outlaws VOIP, 15-year Prison Sentences Possible," *Betanews*, June 15, 2012, http://betanews.com/2012/06/15/ethiopian-government-outlaws-voip-15-year-prison-sentences-possible/.
[85] Fahmida Y. Rashid, "FinFisher 'Lawful Interception' Spyware Found in Ten Countries, Including the U.S.," *Security Week*, August 8, 2012, http://www.securityweek.com/finfisher-lawful-interception-spyware-found-ten-countries-including-us.
[86] The document was seen by Freedom House consultant. Morgan Marquis-Boire et al., "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab (University of Toronto), March 13, 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.
[87] Marquis-Boire, "You Only Click Twice." .
[88] "Mission Statement," Information Network Security Agency of Ethiopia, accessed June 2, 2010, http://www.insa.gov.et/INSA/faces/welcomeJSF.jsp.
[89] Interview with individuals working in the technology and security sector in Ethiopia, who requested to remain anonymous, January 2012.
[90] Committee to Protect Journalists, "Ethiopian Blogger, Journalists Convicted of Terrorism," January 19, 2012, http://cpj.org/2012/01/three-journalists-convicted-on-terrorism-charges-i.php.
[91] "Cassation Bench Rejects Reeyot's Final Plea," Walta Info, January 8, 2012, http://www.waltainfo.com/index.php?option=com_content&view=article&id=6944:cassation-bench-rejects-reeyots-final-plea&catid=52:national-news&Itemid=291.

2012. An appeal court reduced her sentence to five years in August 2012; however, because the Court of Cassation is the last resort for legal appeals, no further recourse is available for acquittal.[92]

While the government's stronghold over the Ethiopian ICT sector enables it to proactively monitor users, its access to user activity and information is less direct at cybercafes. For a period following the 2005 elections, cybercafe owners were required to keep a register of their clients, but this has not been enforced since mid-2010. Nevertheless, there are strong suspicions that cybercafes are required to install software to monitor user activity, which arose after a few incidents were reported of the authorities arresting users at internet cafes in 2011. The arrests were followed by government warnings that "visiting anti-peace websites using proxy servers is a crime."[93]

To date, cyberattacks and other forms of technical violence have not been a serious problem in Ethiopia, partly due to the limited number of users, though the tide may be turning. In March 2013, the independent activist, Abrah Desta, reported via Twitter that his Facebook page was disabled for an unknown reason, which some observers speculated was the result of criminal hacking.[94] Harassment and intimidation of bloggers and online journalists have also increased over the past couple of years. For example, independent bloggers have reported instances of being summoned by the authorities to receive warnings against discussing certain topics online. Fortunately, there have been no instances of violence against users to date.

[92] Committee to Protect Journalists, "Ethiopian Judge Rejects Reeyot Alemu's Final Appeal," January 8, 2013, http://www.cpj.org/2013/01/ethiopian-judge-rejects-reeyot-alemus-final-appeal.php.
[93] "TPLF Regime Arresting Internet Café Users in Addis Ababa," *Ethiopian Review*, August 12, 2011, http://www.ethiopianreview.com/forum/viewtopic.php?f=2&t=30136.
[94] Abraha Desta, Twitter Post, March 20, 2013, 12:34am, https://twitter.com/AbrahaDesta/status/314278873334419456.

FRANCE

	2012	2013
INTERNET FREEDOM STATUS	N/A	FREE
Obstacles to Access (0-25)	n/a	4
Limits on Content (0-35)	n/a	4
Violations of User Rights (0-40)	n/a	12
Total (0-100)	**n/a**	**20**

* 0=most free, 100=least free

POPULATION: 63.6 million
INTERNET PENETRATION 2012: 83 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Takedown requests received by Google have more than doubled over the past year, mainly over defamatory content (see **LIMITS ON CONTENT**).
- Controversial clauses within the HADOPI, LOPPSI 2, and LCEN laws provoked the ire of internet advocates in the country, mainly over fears of disproportionate punishments for copyright violators, overreaching administrative censorship, and threats to privacy (see **LIMITS ON CONTENT** and **VIOLATIONS OF USER RIGHTS**).
- French intelligence agents attempted to coerce a volunteer Wikipedia editor into deleting an entry on a French military installation, threatening him with arrest and prosecution if he failed to comply (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

This report covers events between May 1, 2012 and April 30, 2013. On May 13, 2013, the government released a report on French cultural policy in the digital era drafted by the former media executive Pierre Lescure. Most significantly, the report has led to the abolishment of internet suspensions for users who are found guilty of violating copyright law.[1] *Additional proposals, including the reduction of user fines from €1,500 to €60 ($2,000 to $80) and the transferring of many competencies away from the High Authority for the Distribution of Works and the Protection of Rights on the Internet (HADOPI), were approved by the Minister for Culture and Communications.*[2]

In addition, in June 2013, French daily newspaper Le Monde released new information concerning the existence of a secret surveillance program operated by the Directorate-General for External Security (DGSE),[3] *a French intelligence agency.*[4] *The DGSE program allegedly collects and stores metadata related to e-mails, phone calls, text messages, and online activity on servers based in central Paris and does not come under a legal framework, unlike the highly-regulated program of the Central Directorate of Interior Intelligence (DCRI). Given that this surveillance has been operational during the period covered by this report, Freedom House has decided to include it in this edition of Freedom on the Net (see Violations of User Rights).*

INTRODUCTION

France has a highly developed telecommunications infrastructure and a history of innovation in information and communications technologies (ICTs).[5] Starting in the 1970s, France began developing Teletex and Videotex technologies, leading to the introduction of the widely popular Videotex service Minitel in 1982, which was accessible through telephone lines. In many ways, Minitel predicted applications of the modern internet, such as travel reservations, online retail, mail, chat, and news. At its peak, Minitel had around nine million users, and hundreds of thousands continued to use the service, even after the World Wide Web was introduced in 1994. It was not until June 2012 that the Minitel service was discontinued, primarily due to the growth of the internet industry.[6] France's current ICT market is open, highly competitive, and has benefitted from the privatization of the state-owned company France Telecom.

---

[1] Liberation, "Aurelie Filippetti announces the end of the Hadopi suspension", May 20, 2013, Accessed July 05, 2013, http://www.liberation.fr/medias/2013/05/20/hadopi-aurelie-filippetti-decrete-la-fin-de-la-coupure_904306.
[2] Guerric Poncet, "Vidéo. Rapport Lescure: la Hadopi est morte, vive la Hadopi! [Lescure Report: Hadopi is dead, long live Hadopi!]," LePoint.fr, May 15, 2013, http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/rapport-lescure-l-hadopi-est-morte-vive-l-hadopi-13-05-2013-1666125_506.php.
[3] Direction Générale de la Sécurité Extérieure, http://www.defense.gouv.fr/english/dgse.
[4] "France 'has vast data surveillance' – Le Monde report," BBC News, July 4, 2013, http://www.bbc.co.uk/news/world-europe-23178284.
[5] Jonathan Gregson, "French infrastructure takes some beating," Wall Street Journal, July 5, 2010, accessed April 23, 2013, http://online.wsj.com/ad/article/france-infrastructure.
[6] John Lichfield, "How France fell out of love with Minitel," The Independent, June 9, 2012, http://www.independent.co.uk/news/world/europe/how-france-fell-out-of-love-with-minitel-7831816.html.

While France has traditionally maintained a relatively open and accessible internet, several actions on the part of successive administrations have raised concerns from internet freedom groups and free speech activists. Hate speech, defamation, copyright, and privacy are highly contentious issues relevant to French cyberspace. On several occasions over the past years, politicians have proposed highly restrictive measures, such as the imprisonment of frequent visitors to extremist websites and the mandatory registration of online news editors. Most recently, a government minister suggested that the state could seek to prosecute Twitter for allowing the hate speech to be posted on the site. A bill was also drafted that would ban the online sale of goods below market prices, thereby hurting e-commerce in a bid to protect brick and mortar shops.[7] At the European Union level, the Anti-Counterfeiting Trade Agreement (ACTA) was rejected by members of the European Parliament in July 2012 in a move that was celebrated by internet freedom groups. While no users were sentenced to prison terms over the past year, French intelligence agents threatened a Wikipedia volunteer to delete a post that allegedly raised national security concerns. Nonetheless, the French government only blocks non-political content such as child pornography and hate speech, and a high percentage of French citizens have taken up online tools to receive their news, engage in social networking, and organize demonstrations.

In a positive development, the most controversial provision of the French anti-piracy law, referred to as the "HADOPI law" after the agency tasked with its implementation, was abolished in July 2013 and replaced with a series of automatic fines for the offenders. The law had been criticized by various civil society organizations and international bodies for its "three strikes" provision that required internet service providers (ISPs) to disconnect users from the internet for a period of two to twelve months when found to repeatedly engage in piracy. Nonetheless, doubts remain over the government's policy to instigate legal proceedings against users for copyright infringement.

OBSTACLES TO ACCESS

Since 2009, the French government has been committed to providing widespread access to high-speed broadband and has promised to achieve universal coverage by 2025.[8] As a part of this plan, in February 2013 Alcatel-Lucent and Orange (France Telecom) announced the deployment of the world's most powerful broadband infrastructure, an optical-link, 400 Gbps line between Paris and Lyon.[9] France had an internet penetration rate of 83 percent at the end of 2012, up from 66 percent in 2007.[10] Fixed broadband use has also increased during this time, from 25.5 percent to 37.8 percent.[11] Regionally, internet use ranges from 84.4 percent in the Paris area to 65 percent in

[7] Guillaume Champeau, "Sell cheaper on the web soon to be forbidden" (translated), April 05 2013, Accessed April 19 2013, http://www.numerama.com/magazine/25593-vendre-ses-produits-moins-cher-sur-internet-bientot-interdit.html.
[8] Jonathan Gregson, "French infrastructure takes some beating," Wall Street Journal, July 5, 2010, accessed April 23, 2013, http://online.wsj.com/ad/article/france-infrastructure.
[9] Bernhard Warner, "Alcatel-Lucent Unveils World's Most Powerful Broadband Infrastructure," Business Week, February 15, 2013, accessed April 23, 2013, http://www.businessweek.com/articles/2013-02-15/alcatel-lucent-unveils-worlds-most-powerful-broadband-infrastructure.
[10] "Percentage of Individuals Using the Internet – 2000-2012," International Telecommunication Union, accessed June 29, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[11] "Fixed (wired) broadband subscriptions," 2000-2012," International Telecommunication Union, accessed June 29, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

the northwest of France.[12] Most at-home users have access to broadband connections, while the remaining households are connected either through dial-up or satellite services, usually due to their rural locations.[13] Nonetheless, some 9.5 million people did not use the internet in 2012, either due to obstacles to access, or simply out of personal choice.[14] As French statisticians do not record information related to race, there is no government data relating to internet use according to ethnicity.[15] On a positive note, there is little or no gender gap when it comes to internet access.[16]

The average monthly cost of broadband internet access in France is approximately €33 ($45), for both ADSL[17] and fiber-optic connections.[18] Considering the average monthly income is €2,410 ($3,257),[19] this makes internet access fairly affordable for a large percentage of the population.[20] Companies such as Free Telecom also offer cheap internet access and mobile contracts through combination deals.

There were 70.9 million mobile contracts in use in France as of March 2013, representing a penetration rate of 108.2 percent.[21] Over 23 million people use their mobile devices to access the internet,[22] mostly in addition to a household connection.[23] The internet backbone consists of several interconnected networks run by ISPs and shared through peering or transit agreements. As such, there is no central internet backbone and internet service providers (ISPs) are not required to lease bandwidth from a monopoly holder.

There are no significant hurdles to prevent diverse business entities from providing access to digital technologies in France. The main ISPs are Orange, Free, SFR, Bouygues Telecom, and Numericable, with around 40 smaller private and non-profit ISPs. Apart from Numericable, these

---

[12] Frantz Grenier, "Internet in the Different Regions of France" (translated), March 21, 2013, accessed April 19 2013, http://www.journaldunet.com/ebusiness/le-net/nombre-d-internautes-en-france-par-region.shtml.
[13] Ariase, "ADSL and Broadband Access in France" (translated), accessed April 19, 2013, http://www.ariase.com/fr/haut-debit/index.html.
[14] Nil Sanyas, "the unplugged" (translated), September 12 2012, Accessed April 14 2013, http://www.pcinpact.com/news/73774-la-france-compte-95-millions-deconnectes-et-17-million-assument.htm.
[15] Patrick Simon, "The Choice of Ignorance: The Debate on Ethnic and Racial Statistics in France," French Politics, Culture & Society, Vol. 26, No. 1, Spring 2008, accessed April 23, 2013, http://www.academia.edu/573214/The_choice_of_ignorance._The_debate_on_ethnic_and_racial_statistics_in_France.
[16] "France," New Media Trend Watch, accessed April 23, 2013, http://www.newmediatrendwatch.com/markets-by-country/10-europe/52-france?start=1.
[17] Ariase, "Comparatifs (Comparatives)", accessed April 23, 2013, http://www.ariase.com/fr/comparatifs/adsl.html.
[18] Ariase, "Comparatifs (Comparatives)", accessed April 23, 2013, http://www.ariase.com/fr/comparatifs/fibre-optique.html.
[19] Le Parisien, "Medium monthly income reaches 2410 euros" (translated), March 13 2013, Accessed April 13 2013, http://www.leparisien.fr/economie/votre-argent/le-salaire-moyen-atteint-2-410-euros-bruts-mensuels-13-03-2013-2637973.php.
[20] Similarly, the median monthly salary is €1,675.
[21] ARCEP, "Mobile contracts in France in 2012," February 7, 2013, http://www.arcep.fr/index.php?id=35, accessed April 19, 2013.
[22] Mediametrie, "Internet everywhere" (translated), February 27 2013, Accessed April 19, http://www.mediametrie.fr/internet/communiques/l-annee-internet-2012-l-internet-sur-tous-les-ecrans-tous-les-reseaux-au-plus-pres-de-l-internaute.php?id=818#.UXvC8MV8NNE, and Alexandra Bellamy, "French people loves their smartphones and tablets" (translated), LesNumeriques.fr, December 11 2012, Accessed April 19 2013, http://www.lesnumeriques.com/france-amoureuse-smartphones-tablettes-n27347.html.
[23] Ipsos MediaCT, "PCs, smartphones, tablets: cumulative and complementary use" (translated), September 22, 2011, accessed April 23, 2013, http://www.ipsos.fr/ipsos-mediact/actualites/2011-09-22-pc-smartphones-tablettes-usages-se-cumulent-et-se-completent.

ISPs are also the four main mobile phone operators and work in conjunction with some 40 mobile virtual network operators (MVNOs). France Telecom is the formerly state-owned company that has since been privatized and renamed "Orange."[24] The government still directly owns 13.5 percent of shares in the company, with a further 13.5 percent owned by a sovereign wealth operated by the state.[25] "Free" is a newcomer in the mobile market—its 3G license was awarded by the French regulatory authority in December 2009—and has quickly picked up market share through an aggressive price war.

The telecommunications industry in France is regulated by the Regulatory Authority for Electronic and Postal Communication (ARCEP),[26] while competition is regulated by France's Competition Authority and, more broadly, by the European Commission (EC).[27] The commissioner of ARCEP is appointed by the government, though as an EU member state, France must ensure the independence of its national telecommunications regulator. Given that the French state is a shareholder in Orange, the country's leading telecommunications company, the EC stated that it would closely monitor the situation in France to ensure that European regulations were being met.[28] The EC has previously stepped in when the independence of national telecommunications regulators seemed under threat, notably in Romania, Latvia, Lithuania, and Slovenia.[29] Despite these warnings, ARCEP remains an independent and impartial body and decisions made by the regulator are usually seen as fair.

ARCEP agreed with the opinion of the Competition Authority when asked by the French government to consider the fairness of the terms governing mobile network sharing and national data roaming. The regulator concluded that "infrastructure-based competition is vital to ensuring a healthy state of competition and strong capital investment" and that these two issues are "not incompatible with this goal of a competitive marketplace."[30] ARCEP also placed Free under investigation after the ISP released a firmware update that included an "ad-blocker" function to remove advertisements from appearing on websites.[31] Executives at Free were reportedly attempting to force Google to compensate the ISP for the high levels of data traffic coming from YouTube and other Google sites, similar to an arrangement the American company had made with

[24] "France Telecom becomes Orange," Orange, July 1, 2013, http://www.orange.com/en/group/France-Telecom-becomes-Orange.

[25] According to Cofisem, as of July 2013, the major shareholders in Orange were Fonds Stratégique d'Investissement (13.5%), French State (13.45%), Employees (4.81%), and company-owned shares (0.58%). 67.66% are owned by "other shareholders." "Orange – European Equities," NYSE Euronext, accessed July 29, 2013, https://europeanequities.nyx.com/en/products/equities/FR0000133308-XPAR/company-information.

[26] "Autorité de Régulation des Communications Électroniques et des Poste," http://www.arcep.fr/index.php?id=1&L=1.

[27] "Autorité de la concurrence," http://www.autoritedelaconcurrence.fr/user/index.php.

[28] "ARCEP must remain independent vis-a-vis government – EC," Telecompaper, January 14, 2011, accessed April 16th 2013, http://www.telecompaper.com/news/arcep-must-remain-independent-vis-a-vis-government-ec--778936.

[29] Arjan Geveke, "Improving Implementation by National Regulatory Authorities," European Institute of Public Administration, 2003, accessed April 24, 2013, http://aei.pitt.edu/2592/1/scop_3_3.pdf.

[30] "ARCEP reviews the Competition Authority's balanced opinion on the terms governing mobile network sharing and roaming," ARCEP, March 11, 2013, accessed April 16th 2013, http://www.arcep.fr/index.php?id=8571&L=1&tx_gsactualite_pi1%5Buid%5D=1592&tx_gsactualite_pi1%5Bannee%5D=&tx_gsactualite_pi1%5Btheme%5D=&tx_gsactualite_pi1%5Bmotscle%5D=&tx_gsactualite_pi1%5BbackID%5D=26&cHash=b419a25d887293a12673299e88aaa3d4.

[31] Cyrus Farivar, "France's second-largest ISP deploys ad blocking via firmware update," Ars Technica, January 3, 2013, http://arstechnica.com/business/2013/01/frances-second-largest-isp-deploys-ad-blocking-via-firmware-update/.

leading ISP Orange. Free backed down under government pressure and criticism that the ISP was harming net neutrality by failing to deliver content to users without any obstructions.[32]

LIMITS ON CONTENT

Although France has a strong record of an open and accessible internet, over the past two years the country has come under criticism from online activists and free speech advocates. Article R645-1 of the French criminal code outlaws the display of the emblems, uniforms, or badges of criminal organizations, under penalty of a fine.[33] Websites that contravene this law have been requested to remove the content or face blocking.[34] Furthermore, child pornography and other illegal websites are blocked.[35] More controversially, French authorities have stepped up efforts to block or remove online content that is found to violate copyright protections or infringe on privacy. The most ardent defenders of free speech have been loath to see any sort of administrative filtering in France, fearing that laws such as LCEN, LOPPSI 2, and the HADOPI law may eventually lead to a spillover whereby controversial yet legal sites are censored by administrative agencies and without a court order.[36] (For more on these laws, please see the following section, "Violations on User Rights")

French law recognizes "the right to be forgotten" (*le droit à l'oubli*), which has its roots in rehabilitated criminals who did not wish to see their past cases publicized, having already "paid their debt to society" through jail time. The issue has recently been taken up by Viviane Reding, European Commissioner for Justice, Fundamental Rights, and Citizenship, in relation to an individual's right to request that their personal data be completely deleted from social networks or other websites, including from any hosting servers. The EU proposals have come under criticism as impossible to enforce,[37] or worse, threatening to free speech.[38] However, the EC has clarified that deletion requests would not pertain to matters of public interest, thereby calming some concerns over possible censorship of the press.[39] In France, individuals can already request that defamatory content related to them can be removed through a court order in line with Article 29 of the 1881

[32] Chiponda Chimbelu, "French ISP revives debate on 'free Internet'," DW, January 9, 2013, http://www.dw.de/french-isp-revives-debate-on-free-internet/a-16508222.
[33] Elissa A. Okoniewski, "Yahoo!, Inc. v. Licra: The French Challenge to Free Expression on the Internet," 2002, accessed April 24, 2013, http://www.auilr.org/pdf/18/18-1-6.pdf
[34] Roger Darlington, "Should the Internet be Regulated?" no publication date, accessed April 17, 2013, http://www.rogerdarlington.me.uk/regulation.html
[35] "French Law Loppsi 2 Adopted by the General Assembly," Digital Civil Rights in Europe, January 12, 2011, accessed April 25, 2013, http://www.edri.org/edrigram/number9.1/loppsi-2-adopted-assembly
[36] Olivier Dumons, "After DADVSI and HADOPI, LOPPSI 2 To Be Released" (translated), May 18 2009, Accessed April 18 2013, http://www.lemonde.fr/technologies/article/2009/05/18/apres-la-dadvsi-et-hadopi-bientot-la-loppsi-2_1187141_651865.html, and La Quadrature du Net, "Administrative Net Censorship adopted in France" (translated), December 15 2010, Accessed April 18 2013, http://www.laquadrature.net/fr/loppsi-censure-administrative-du-net-adoptee-les-pedophiles-sont-tranquilles.
[37] Mike Masnick, "EU Report: The 'Right To Be Forgotten Is Technically Impossible… So Let's Do It Anyway," TechDirt, December 6, 2012, accessed June 19, 2013, http://www.techdirt.com/articles/20121205/08425221239/eu-report-right-to-be-forgotten-is-technically-impossible-so-lets-do-it-anyway.shtml.
[38] Jeffrey Rosen, "The Right to be Forgotten," Stanford Law Review, February 13 2012, http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.
[39] Michael Venables, "The EU's 'Right To Be Forgotten': What Data Protections Are We Missing in the US?" Forbes, March 8, 2013, accessed June 19, 2013, http://www.forbes.com/sites/michaelvenables/2013/03/08/the-ecs-right-to-be-forgotten-proposal-in-the-u-s/.

Law on Press Infractions—related to insult, defamation, or denigration—and the 2004 Law for Trust in the Digital Economy (LCEN), which holds hosting providers liable if they fail to cooperate with a court decision.[40] The passage of LCEN was met with criticism from many in France, including members of parliament (MPs) from the Socialist Party. The MPs submitted a brief to the Constitutional Court to review several clauses of LCEN that failed to define e-mail as private correspondence (and thus subject to greater surveillance), "privatized justice" through administrative notices and extralegal take down procedures, and set a longer statute of limitations for online content versus traditional media. The grounds under which authorities could restrict access to communications were also criticized as overly broad and open to abuse.[41]

Intermediaries are coming under increasing pressure to cooperate with French authorities against defamation, copyright, and hate speech. In 2011, a draft executive order to implement Article 18 of LCEN suggested new means by which various government agencies could force content owners to remove content or instruct ISPs to block webpages. The proposal sought to outline the procedures for blocking or removing online content "in case of violation, or where there is a serious risk of violation, of the maintenance of public order, the protection of minors, the protection of public health, the preservation of interests of the national defense, or the protection of physical persons."[42] However, the order came under fire from internet freedom activists and the e-commerce community who pointed out that intermediaries could face an unfair responsibility to police content.[43] There were also fears that, under the proposal's vague wording, the law would be applicable to most websites rather than only those engaged in e-commerce, as originally intended.[44] This would have opened up the possibility that any website could be blocked arbitrarily and without due process under the proposal's emergency clause. The draft law was eventually rejected at the end of June 2013.[45]

French authorities are highly active in pursuing the removal of content online. As an indication, Google's Transparency Report noted that the total number of content removal requests it received from the French government from January to June 2012 increased by 128 percent, compared to the previous six month period. Google also removed 992 search results which allegedly violated the privacy of an individual, though it did not remove a blog post about a former politician that "allegedly defame[d] him by explaining his connections with the pharmaceutical lobby."[46] In the

[40] Loi pour la Confiance dans l'Économie Numérique
[41] "French E-Commerce Law Tested in Constitutional Court," Digital Civil Rights in Europe (EDRI), June 2, 2004, http://www.edri.org/edrigram/number2.11/lcn.
[42] Simon Columbus, "French Government Plans to Extend Internet Censorship," Open Net, June 2011, https://opennet.net/blog/2011/06/french-government-plans-extend-internet-censorship
[43] French National Digital Council, "Review of the LCEN Decree" (translated), June 17 2011, Accessed April 12 2013, http://static.pcinpact.com/media/2011-06-17_aviscnn_decretart18lcen_vf.pdf
[44] Andréa Fradin, "Administrative filtering" (translated), Owni.fr, June 16 2011, Accessed April 17 2013, http://owni.fr/2011/06/16/filtrage-par-decret/
[45] Olivier Robillart, "Article 18 finally rejected by French Assembly" (translated), June 28, 2013, http://pro.clubic.com/legislation-loi-internet/actualite-568770-lcen-blocage-administratif.html.
[46] "France," Google Transparency Report, accessed April 25, 2013, http://www.google.com/transparencyreport/removals/government/FR/?p=2012-06.

following six month period ending December 2012, takedown requests from court orders and executive bodies remained high, with the vast majority of cases related to defamation.[47]

In January 2013, the French Minister for Woman's Rights and a government spokesperson, Najat Vallaud-Belkacem, called for Twitter to take greater responsibility in preventing the posting of hate speech on the site.[48] However, the proposal was criticized as a danger to free speech, potentially allowing the government to classify unfavorable opinions under the vague term of hate speech.[49] The move would also place an unfair burden on intermediaries, forcing them to use their discretion to prescreen content that could be deemed as offensive.[50] When it comes to the curtailing of illegal content, ISPs and mobile telephone companies who provide internet access currently have no obligation to preemptively review any of the content they transmit or store. Nevertheless, according to LCEN, they must take prompt action to withdraw the relevant content when informed of unlawful information or activity, or face the possibility of civil liability. Similarly, cyber cafes and other public places which provide internet access have no responsibility to review the content which can be viewed by their customers but are liable in cases of illegal activities; as a result, cybercafes must log the activities of their customers (see "Violations of User Rights").

French authorities are fairly transparent about what websites are blocked and why content must be taken down. Incitement of hatred, racism, Holocaust denial, child pornography, copyright infringement, and defamation are illegal. Requests to block or remove content can emanate from individuals, copyright holders, or government bodies. These requests must be reviewed by a court, which then instructs ISPs, content holders, or other intermediaries to implement its decision.

Traditionally, the French state has been criticized as being a "Web 1.0" government.[51] More recently, public figures and politicians have opened up social media accounts and blogs to establish a web presence.[52] Presidential candidates have taken to the web to promote their campaigns, though with mixed results. For example, while all candidates in the 2007 elections created virtual campaign headquarters on the online community known as "Second Life," the headquarters of the far-right candidate Jean-Marie Le Pen was attacked and destroyed when dissenters launched "pig grenades" at the virtual building.[53]

---

[47] "France," Google Transparency Report, accessed July 29, 2013, http://www.google.com/transparencyreport/removals/government/FR/?p=2012-12.
[48] Najat Vallaud-Belkacem, "Twitter must respect the values of the Republic" (translated), Le Monde, December 28 2012, accessed June 20 2013, http://www.lemonde.fr/idees/article/2012/12/28/twitter-doit-respecter-les-valeurs-de-la-republique_1811161_3232.html.
[49] Glenn Greenwald, "France's censorship demands to Twitter are more dangerous than 'hate speech'," The Guardian, January 2, 2013, accessed April 24, 2013, http://www.guardian.co.uk/commentisfree/2013/jan/02/free-speech-twitter-france.
[50] Mike Masnick, "French Politician Wants Twitter To Help Censor Speech," Techdirt, January 04 2013, accessed June 20 2013, http://www.techdirt.com/articles/20130103/03195521559/french-politicians-wants-twitter-to-help-censor-speech.shtml.
[51] Yaron Gamburg, "Web 2.0 is a 'fait accompli' in France. But what about the French version of Gov 2.0?" GovLoop blog, July 23 2011, accessed April 23, 2013, http://www.govloop.com/profiles/blogs/web-2-0-is-a-fait-accompli-in.
[52] Rodolphe Baron, "Twitter changes political marketing", owni.fr, March 29, 2012, accessed July 04, 2013, http://owni.fr/2012/03/29/twitter-change-le-marketing-politique/.
[53] Molly Moore, "French Politics in 3-D on Fantasy Web Site", March 30 2007, Accessed April 16 2013, http://www.washingtonpost.com/wp-dyn/content/article/2007/03/29/AR2007032902540.html.

France is home to a highly diverse online media environment. In recent years, several French protests have been organized online, including demonstrations against cuts in government-supported programs such as education or changes to labor laws proposed in 2006.[54] More recently, from January to April 2013, online campaigns such as those organized by the controversial figure Frigide Barjot and others were able to mobilize large groups of demonstrators using social media networks in an effort to oppose legislation surrounding same-sex marriages.[55] Protests have continued, even after the legislation proposed by the government of François Hollande was passed in April 2013.[56]

French digital rights and online freedom advocacy groups are very active and play a significant role in the country. For example, the group "La Quadrature du Net" successfully lobbied the European Parliament for an amendment to the EU Telecoms Package to ensure that no restrictions on internet access could be imposed without prior judicial approval.[57] After the European Parliament rejected ACTA in July 2012, the group also published a proposal for a new regulatory framework on reforming copyright issues.[58]

VIOLATIONS OF USER RIGHTS

The European Convention on Human Rights, of which France is a signatory, provides for freedom of expression, subject to certain restrictions which are "necessary in a democratic society."[59] France's constitution guarantees freedom of speech[60] in accordance with the 1789 Declaration of the Rights of Man.[61] However, the French government has also enacted several laws which, while seeking to protect the rights of internet users and copyright holders, also threaten the rights of citizens online. For example, in 2012, then-President Nicolas Sarkozy announced his intention to

[54] Le Monde, "CPE protests in France" (translation), March 28 2006, accessed April 16 2013, http://www.lemonde.fr/societe/infographie/2006/03/28/les-manifestations-anti-cpe-du-28-mars-en-france_755523_3224.html, and Flickr, February 2006, Accessed April 16 2013, http://www.flickr.com/groups/71873699@N00/pool/.

[55] Andrew Cusack, "France Marches for Marriage," January 13, 2013, accessed April 17 2013, http://www.andrewcusack.com/2013/01/13/le-manif-pour-tous/, and Stéphane Kovacs, "Protests Over Gay Marriage and Guerilla" (translated), Le Figaro, April 17 2013, Accessed April 19 2013, http://www.lefigaro.fr/actualite-france/2013/04/16/01016-20130416ARTFIG00433-manif-pour-tous-dans-les-coulisses-de-la-guerilla.php.

[56] Laura Smith-Spark, "French lawmakers approve same-sex marriage bill," CNN, April 24, 2013, http://www.cnn.com/2013/04/23/world/europe/france-same-sex-vote.

[57] Danny O'Brien, "Blogging ACTA across the globe: the view from France," Electronic Frontier Foundation, January 2010, accessed April 25, 2013, https://www.eff.org/deeplinks/2010/01/acta-and-france.

[58] Philippe Aigrain, "Elements for the reform of copyright and related cultural policies", Accessed July 04, 2013, http://www.laquadrature.net/files/Elements_for_the_reform_of_copyright_and_related_cultural_policies.pdf.

[59] "European Convention on Human Rights," accessed April 25, 2013, http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/Convention_ENG.pdf.

[60] Guy Carcassonne, "The Principles of the French Constitution," written for the French Embassy in the U.K., May 2002, accessed April 26, 2013, http://www.unc.edu/depts/europe/francophone/principles_en.pdf.

[61] "The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as shall be defined by law," Declaration of the Rights of Man, 17 89, accessed April 26, 2013, http://avalon.law.yale.edu/18th_century/rightsof.asp.

create criminal penalties for habitually visiting websites that advocate terrorism or hate crimes.[62] The proposal raised many concerns and, while it was not pursued,[63] laws such as LOPSSI 2, LCEN, and the HADOPI have been highlighted by online activists and internet companies over concerns that they may overreach in their aims. In mid-2013, reports surfaced that French intelligence agencies may possess secret surveillance capabilities beyond the scope that is currently permitted in French law. In a separate case, intelligence agents were also found to have intimidated a Wikipedia volunteer with no legal basis, threatening to detain him if he did not delete a dated entry that allegedly raised national security concerns.

In a bid to promote the distribution and protection of creative works on the internet, the government introduced the controversial HADOPI laws in 2009.[64] However, the HADOPI law's "three-strikes" rule, which banned users access to the internet for a certain period of time after they have violated copyright laws three times, was largely denounced as a violation of the fundamental right of freedom of access to information on the internet.[65] The "three-strikes" rule was altered in May 2013 to reduce the level of fines and abolish the cutting of internet service. In the past, the website of HADOPI was targeted with distributed denial of service (DDoS) attacks by hacktivists.[66] Independent government agencies, such as the National Commission for Informatics and Liberties (CNIL),[67] also criticized elements of the HADOPI law and highlighted the risks it represents for freedom of speech and privacy.[68] Private companies, like the ISP "Free," refused to send out copyright infringement notices to users, citing the extra costs that it would entail.[69]

Punishments under the HADOPI law were outlined as a "graduated response" in three steps. At first, users downloading illegal content received a warning e-mail or a notice of infringement, of which 1.15 million have been sent in the past three years. If illegal activity persisted, a letter was then sent to the user and his or her ISP, which has occurred some 10,000 times. Finally, the case was then submitted to the Public Prosecutor, which could result in a fine of up to €1,500 ($2,000) and denial of internet access. Fourteen such cases have been launched, with only two resulting in a criminal prosecution. In one case from September 2012, the accused was forced to pay a fine of €150 ($200) for "allowing his Wi-Fi connection to be used to download songs without obtaining prior permission from the copyright owners."[70] In the other case, from June 2013, the defendant

[62] Jean-Loup Richet, "Internet Censorship in France: should we criminalize viewers?", Herdict, April 24, 2012, Accessed April 25, 2013, http://www.herdict.org/blog/2012/04/24/internet-censorship-in-france-should-we-criminalize-viewers/.
[63] National Digital Concil, "Letter to President Sarkozy", March 23, 2012, Accessed April 25, 2013, http://www.cnnumerique.fr/wp-content/uploads/2012/03/2012-03-23_LettreCNN-PR-mesureterrorisme_VF.pdf.
[64] Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet
[65] Frank La Rue, UN Report, May 16 2011, Accessed April 17 2013, http://documents.latimes.com/un-report-internet-rights/.
[66] Eduard Kovacs, "Hacktivists DDOS Hadopi and Others in Anti-ACTA Protest", February 06, 2012, Accessed July 05, 2013, http://news.softpedia.com/news/Hacktivists-DDOS-Hadopi-and-Others-in-Anti-ACTA-Protest-250987.shtml.
[67] Commission Nationale de l'Informatique et des Libertés
[68] Alex Turk, "The Internet Policy in France and the Role of the Independent Administrative Authority CNIL," 2011, accessed April 17, 2013, http://www.kas.de/wf/doc/kas_22806-544-2-30.pdf?110516131251.
[69] Drew Wilson, "French ISPs and French Government Locking Horns Over HADOPI Costs", September 2, 2010, Accessed July 05, 2013, http://www.zeropaid.com/news/90536/french-isps-and-french-government-locking-horns-over-hadopi-costs/.
[70] Rainey Reitman, "French Anti-Piracy Law Claims First Victim, Convicted of Failing to Secure His Internet Connection," Electronic Frontier Foundation, September 2012, accessed April 23, 2013, https://www.eff.org/deeplinks/2012/09/french-anti-piracy-law-claims-first-victim-convicted-failing-secure-his-internet.

was made to pay €600 ($800) and the court ordered the suspension of his internet connection for 15 days.[71]

However, there were doubts as to whether the termination of service can technically be applied by the ISP, since the law maintains that any cut in internet access must not affect the individual's access to private communications services, such as e-mail or even private messages on social networks.[72] Indeed, questions remain surrounding the fate of HADOPI itself, particularly since the publication of the government's Lescure report in May 2013. The former media executive recommended the transfer of many competencies from HADOPI to the Supreme Audiovisual Council (CSA),[73] the reduction of fines from €1,500 to €60 ($2,000 to $80), and the abolishment of internet suspensions.[74] Many of these proposals seem to be underway, particularly after signals from the French Minister for Culture and Communications, Aurélie Filippetti, indicated that suspensions would be halted immediately.[75]

The Law on Guidelines and Programming for the Performance of Internal Security (LOPPSI 2),[76] first presented in May 2009 amid intense debate,[77] was adopted in March 2011 by the National Assembly and the Senate. LOPSSI 2 relates primarily to cybersecurity and the fight against child pornography. There were concerns from online activists, however, that if administrative agencies were allowed to demand ISPs to filter content without first acting on a court order, this may open the door for the administrative filtering of other, more legitimate sites without the need for judicial approval.[78] In July 2012, Fleur Pellerin, Minister for the Digital Economy, announced that Article 4 relating to the administrative filtering of child pornography would not be implemented without a court order.[79] Article 23 grants the police with the authority to install malware—such as keyloggers and Trojan horses—on a suspect's computer in the course of counterterrorism investigations, though authorization must come from a court order.[80]

---

[71] La Tribune, " first internet denial for Hadopi » (translated), June 13, 2013, Accessed July 04, 2013, http://www.latribune.fr/technos-medias/internet/20130613trib000770121/hadopi-la-premiere-et-surement-la-derniere-coupure-internet-a-ete-prononcee.html.

[72] Marc Rees, "Hadopi suspension is impossible to implement" (translated) , June 5, 2013, Accessed July 05, 2013, http://www.pcinpact.com/news/80261-les-petites-hypocrisies-d-aurelie-filippetti-sur-hadopi.htm.

[73] Couseil superior de l'audiovisuel, http://www.csa.fr/.

[74] Guerric Poncet, "Vidéo. Rapport Lescure: la Hadopi est morte, vive la Hadopi! [Lescure Report: Hadopi is dead, long live Hadopi!]," LePoint.fr, May 15, 2013, http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/rapport-lescure-l-hadopi-est-morte-vive-l-hadopi-13-05-2013-1666125_506.php.

[75] Liberation, "Aurelie Filippetti announces the end of the Hadopi suspension", May 20, 2013, Accessed July 05, 2013, http://www.liberation.fr/medias/2013/05/20/hadopi-aurelie-filippetti-decrete-la-fin-de-la-coupure_904306.

[76] Loi d'orientation et de programmation pour la performance de la sécurité intérieure

[77] Corentin Chauvel, "the debate on LOPPSI 2" (translated), 20 Minutes.fr, January 7 2011, Accessed April 17 2013, http://www.20minutes.fr/societe/649278-societe-loppsi-2-retour-points-contestes.

[78] LOPPSI law project, Accessed July 04, 2013, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&fastPos=1&fastReqId=1447818568&categorieLien=id&oldAction=rechTextel.

[79] Numerama, "LOPPSI Article 4 decree finally abandoned", July 25, 2012, Accessed July 05, 2013, http://www.numerama.com/magazine/23260-loppsi-le-decret-sur-le-blocage-des-sites-sans-juge-est-abandonne.html.

[80] Emilien Ercolani, "LOPPSI: Who could install spywares?" (translated), L'informaticien, November 7 2011, Accessed April 17 2013, http://www.linformaticien.com/actualites/id/22101/loppsi-qui-pourra-installer-les-mouchards-informatiques-la-liste-publiee-au-jo.aspx.

The French government does not place hefty restrictions on anonymous communication for online users, although individuals are required to register their real names when purchasing new SIM cards or using cybercafés. In 2010, a law was briefly floated to require anyone who edits "a non-professional communication service online" to register their name, location, and phone number as part of a push to apply existing press regulations on to the blogosphere.[81] However, numerous online advocates condemned the proposal in an online petition and the law was never enacted.

In June 2013, French daily newspaper *Le Monde* revealed the alleged existence of an extralegal surveillance program operated by the Directorate-General for External Security (DGSE),[82] a French foreign intelligence agency.[83] The DGSE maintains the capacity to intercept communications between France and external countries in a plan that was ostensibly designed for counter-terrorism purposes. In early July, additional reports surfaced from *Le Monde* indicating that metadata from telephone and computer activity—even within France—was systematically collected and stored at the DGSE facility in central Paris.[84] This runs counter to existing French law, which only allows for counterterrorism agents within the Central Directorate of Interior Intelligence (DCRI)[85] to make a request to obtain metadata related to a user's telephone and internet activities.[86] These limited requests must also be reviewed by the National Commission of Control for Security Interceptions (CNCIS), an independent administrative authority.[87] In the case of the DGSE program, by contrast, seven different government agencies have access to this large body of user data without any legal basis or judicial oversight. Furthermore, the mandates and scope of operations of some of these agencies are also not strictly limited to counterterrorism.[88] As of August 2013, more details had yet to come out surrounding the allegations.

As previously mentioned, the LCEN maintains that ISPs and hosting providers must retain data on their users and customers for a period of one year.[89] Furthermore, under a decree issued in 2011,

[81] Draft Proposal "facilitate the identification of bloggers" (translated), Senat.fr, May 3, 2010, Accessed April 19 2013, http://www.senat.fr/leg/ppl09-423.html, Xavier Ternisien, Le Monde, "Could we Outlaw Anonymous Bloggers?", May 27 2010, Accessed April 19 2013, http://www.lemonde.fr/technologies/article/2010/05/27/un-blogueur-doit-il-rester-anonyme_1363856_651865.html

[82] Direction Générale de la Sécurité Extérieure, http://www.defense.gouv.fr/english/dgse.

[83] "France 'has vast data surveillance' – Le Monde report," BBC News, July 4, 2013, http://www.bbc.co.uk/news/world-europe-23178284.

[84] Edward Moyer, "Eye on surveillance: France's PRISM, EU's concerns," CNET, July 4, 2013, http://news.cnet.com/8301-13578_3-57592372-38/eye-on-surveillance-frances-prism-eus-concerns/.

[85] Direction centrale du renseignement intérieur, http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-du-Renseignement-Interieur

[86] Laurent Borredon and Jacques Follorou, "En France, la DGSE au Coeur d'un programme de surveillance d'Internet [In France, the DGSE at the heart of a program for internet surveillance]," Le Monde.fr, June 11, 2013, http://www.lemonde.fr/international/article/2013/06/11/en-france-la-dgse-est-au-c-ur-d-un-vaste-programme-de-surveillance-d-internet_3427837_3210.html.

[87] Commission nationale de contrôle des interceptions de sécurité. http://lannuaire.service-public.fr/services_nationaux/autorite-administrative-independante_172128.html.

[88] "Comment la France intercepte les communications [How France intercepts communications]," Le Monde.fr, July 4, 2013, http://www.lemonde.fr/societe/infographie/2013/07/04/comment-la-dgse-collecte-et-stocke-l-ensemble-des-communications-electromagnetiques_3441931_3224.html.

[89] Anne-Laure-Hélène des Ylouses, « Application of article 6 II of the LCEN", Juris Intitiative, March 2011, Accessed April 17 2013, http://www.juris-initiative.net/en/legal-areas/telecom/decree-relating-to-retention-and-communication-of-data.html, and Guillaume Champeau, « LCEN will retain data on user », Numerama, March 01, 2011,

data retention responsibilities were extended in duration and scope in order to bring France in line with the EU Data Retention Directive. Under the decree, a wide array of online companies, websites, and e-commerce outlets must, for a period of two years, store user data such as log-in credentials, phone numbers, data on financial transactions, and web browsing history. An association of online companies representing the likes of eBay, Facebook, Google, Microsoft, Wikipedia, and Yahoo challenged the decision and called for a court review, since under EU law, any new measures related to data retention must be reviewed by the European Commission.[90] As of mid-2013, the decree remains in place.

The EU Data Detention Directive itself has been criticized by European rights groups, such as the European Data Protection Supervisor (EDPS). In a non-binding opinion to the Commission, the EDPS concluded that "the directive has failed to meet its main purpose, namely, to harmonize national legislation concerning data retention" and "does not meet the requirements set out by the rights to privacy and data protection."[91]

While these laws outline under what legal conditions authorities can block a site or fine a user, there were also reports that the government has used more opaque methods to practice censorship. On April 4, 2013, French secret service agents working in the DCRI reportedly threatened a French Wikipedia volunteer, calling upon him to delete an article on a sensitive military installation or face being detained and prosecuted.[92] Representatives from Wikipedia France criticized the incident and called for French authorities to present them with a legal takedown notice. The entry, which relates to a military radio relay station in the region outside of Lyon, has existed since 2009 and remains online.

As is the case with many countries around the world, France's government agencies, websites, and private companies are occasionally subject to cyberattacks and hacking. In January 2013, the French Ministry of Defense's website was hacked and defaced, while information from its database was leaked by a member of the hacker group "XL3gi0n Hackers," supposedly to demonstrate to France that they need to improve their cyber-security measures and to protest against the recent French attack on Mali.[93] In May 2012, after the second round of the presidential election, a piece of malware known as "Flame" was discovered on the computers of the presidential staff.[94] While a French news magazine suggested the US government could be to blame, the US Embassy in Paris

---

http://www.numerama.com/magazine/18191-la-lcen-a-enfin-son-decret-sur-les-donnees-a-conserver-par-les-hebergeurs.html, accessed April 19, 2013.

[90] Matthew J. Schwartz, "Tech Giants Challenge French Data Retention Law," Information Week, April 8, 2011, http://www.informationweek.com/security/privacy/tech-giants-challenge-french-data-retent/229401245.

[91] "Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)," European Data Protection Supervisor, 2011, accessed April 18, 2013, https://www.eff.org/sites/default/files/filenode/dataretention/11-05-30_Evaluation_Report_DRD_EN.pdf.

[92] Kim Willsher, "French secret service accused of censorship over Wikipedia page," The Guardian, April 7, 2013, accessed April 24, 2013, http://www.guardian.co.uk/world/2013/apr/07/french-secret-service-wikipedia-page.

[93] Sabari Selvan, "French Ministry of Defense hacked and database leaked by XtnR3v0LT," E Hacking News, January 16, 2013, accessed April 18, 2013, http://www.ehackingnews.com/2013/01/france-ministry-of-defense-hacked.html.

[94] BBC News Europe, "US 'launched Flame cyber attack on Sarkozy's office'," November 21, 2012, accessed April 18, 2013, http://www.bbc.co.uk/news/world-europe-20429704.

has vehemently denied any part in the attack.[95] Overall, technical violence does not appear to be a serious problem in France. The delicate balance between freedom of speech and protection of information has come to the forefront in the digital age. While France has thus far maintained an openness appreciated by its 48 million internet users, policies will be put to the test as the dark sides of digital capabilities surface.

[95] Sébastian Seibt, "France victim of a cyber attack from the US?" (translated), November 21 2012, Accessed April 13 2013, http://www.france24.com/fr/20121121-cyberattaque-elysee-express-flame-virus-sarkozy-etats-unis-piratage-hacking-revelation.

GEORGIA

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	9	8
Limits on Content (0-35)	10	7
Violations of User Rights (0-40)	11	11
Total (0-100)	30	26

* 0=most free, 100=least free

POPULATION: 4.5 million
INTERNET PENETRATION 2012: 46 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- While internet connections remained somewhat slow and were subject to temporary outages in certain areas, there were no major nation-wide disruptions to internet access as there had been in previous years (see **OBSTACLES TO ACCESS**).
- Incidents of self-censorship and blocking or manipulation of political content online decreased (see **LIMITS ON CONTENT**).
- In the months leading up to the 2012 parliamentary elections, civil society groups created an online crowdsourcing portal to monitor any voting violations or campaign-related incidents (see **LIMITS ON CONTENT**).

INTRODUCTION

Internet access and use continues to grow rapidly in Georgia, particularly as interest in connecting with friends through social-networking sites has increased in recent years. State bodies and several key politicians have also increased their use of the internet and modern social media tools to share information with citizens and attract attention from the potential electorate.[1] Many government agencies are publicizing information on the web, including the Ministry of Justice, which publishes all laws, bills, and decrees of the government on its website.[2]

The internet was first introduced in Georgia at the end of 1990s, and after a boom in new services such as broadband at the beginning of 2004, connections became available for almost everyone with a telephone line in Tbilisi. Internet subscriptions have also proliferated in other large cities. Online news media are still developing slowly, while a growing number of newspapers are launching websites, and major newspapers and news agencies are sharing content through applications such as Facebook, Twitter, and YouTube. Meanwhile, many journalists working in the traditional media sphere are looking for ways to advance their knowledge of internet technology and web tools.

In 2012–2013, there were fewer restrictions on online content in Georgia than there had been in previous years. There are no indications of censorship or content being blocked by the Georgian authorities or internet service providers (ISPs), and there are no recent cases of activists or reporters being questioned or arrested for their online activities.[3]

Despite a moderate internet penetration rate, in 2012, social media tools and Web 2.0 applications were used alongside traditional media outlets to document and respond to significant political and social events. In the months leading up to the parliamentary elections in October 2012, in which the Georgian Dream coalition defeated the ruling United National Movement, the U.S.-based National Democratic Institute partnered with Georgian NGOs to produce an online Elections Portal where citizens could report incidents relating to the election and the preceding campaigns. Additionally, in September 2012, videos revealing prisoner abuse that were shown on television channels were also shared online via YouTube, while images and information about the subsequent protests were shared via Twitter.[4]

OBSTACLES TO ACCESS

The number of internet and mobile telephone users in Georgia is growing, but high prices for services and inadequate infrastructure remain obstacles, particularly for those in rural areas or with

[1] The website of the President of Georgia features links to all of the named social media sites: http://president.gov.ge/.
[2] Ministry of Justice, http://matsne.gov.ge.
[3] Transparency International Georgia, "The State of the Internet: Who Controls Georgia's Telecommunications Sector?" February 2013, http://j.mp/16hJu3p.
[4] Onnik Krikorian, "Georgia: 'Broom Revolution' as Elections Approach," Global Voices, September 23, 2012, http://globalvoicesonline.org/2012/09/23/georgia-broom-revolution-as-parliamentary-elections-approach/.

low incomes. According to statistical data collected by the International Telecommunication Union (ITU), 46 percent of the population had access to the internet in 2012, up from 37 percent in 2011;[5] a survey by the Caucasus Research Resource Centers (CRRC) confirmed that 46 percent of the population accessed the internet on a daily basis.[6] Only four percent of Georgians are unfamiliar with the internet altogether.[7]

The most frequent activity among users was the use of social media tools (75 percent of users), while 45 percent used the internet to search for information, and 20 percent browsed the news.[8] With 1.1 million registered users on Facebook, social networks serve as an important platform for discussion and information exchange among the more liberal segments of Georgian society. State bodies have also stepped up their use of the internet. For example, departments in the Ministry of Justice, the Ministry of Finance's Tax Inspection, and others have developed online services that allow citizens to register and receive services, apply for identification cards, or file tax documentation. Several state services are entering the mobile apps market; for example, the Georgian Police have created an app where users can check important information or pay fines associated with tickets.

ISPs offer dial-up, DSL broadband, fiber-optic, EVDO, and CDMA connections. The average cost for an internet connection is $20 a month, and the lowest price for a 5 Mbps DSL connection is about $12 per month.[9] Many users complain about the quality of connections and suffer from frequent outages. Nevertheless, there were over 430,000 fixed-line broadband internet connections in 2012,[10] resulting in a broadband penetration rate of 7.6 percent, up from 0.6 percent in 2006.[11]

Mobile phone penetration is greater than that of the internet and has continued to grow from 59 percent in 2007 to 109 percent in 2012.[12] Mobile phones significantly outnumber landlines, and reception is available throughout the country, including rural areas. The use of mobile devices to connect to the internet has been limited by high costs, but providers are offering new and somewhat less expensive services, including CDMA and EVDO technologies.

---

[5] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2012, accessed July 1, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[6] "Development of e-communication in Georgia—access to the internet," Institute for Development of Freedom of Information, http://www.idfi.ge/?cat=researches&lang=en&topic=108&header=.

[7] Tinatin Zurabishvili, *Media Survey 2011, Georgia*, Caucasus Research Resource Centers, 2011, http://www.crrc.ge/oda/.

[8] Elza Ketsbaia, "Internet usage in Georgia," Net Prophet, January 30, 2012, http://netprophet.tol.org/2012/01/30/internet-usage-in-georgia/.

[9] Comparative data from two major ISP's prices (SilkNet and Caucasus Online).

[10] Data provided by GNCC – Annual Report 2012 [in Georgian], http://www.gncc.ge/files/3100_2949_681569_ANNUAL%20REPORT%202012.pdf

[11] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions."

[12] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2007 & 2012, accessed July 13, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

The Georgian National Communications Commission (GNCC) introduced mobile number portability in February 2011[13] and fixed-line number portability in December 2011,[14] giving users more freedom to switch between service providers and choose between price plans.[15] According to a new national numbering plan, as of January 2012, all phone numbers have changed to align with international standards.[16]

The web presence and internet usage of large companies and small businesses grew rapidly in 2012–2013, particularly as a result of social media tools. Many established brands and companies such as banks, financial institutions, artists, public figures, and electronics stores have begun to use social media to promote their businesses and build customer support,[17] and more money is being invested in online projects.[18]

Cybercafes provide internet access at reasonable prices, but they are located mainly in large cities, and there are too few to meet the needs of the population. Most cafes have less than a dozen computers, and customers often have to wait as long as an hour for access. Internet cafes have become a popular place for online gamers, where the younger generation spends hours playing online games. Many restaurants, cafes, bars, cinemas, and other gathering places provide Wi-Fi access, allowing customers to use the internet on their personal laptops. As part of the global tourism campaign "Tbilisi – The city that loves you," the municipality has covered most central districts of the city with free Wi-Fi access. The connection speed is relatively slow; it allows users to connect to the internet via mobile devices, but the connection is not strong enough for laptops to offer a full browsing experience.[19]

There are currently 32 entities registered as ISPs in Georgia, 10 of which are large networks of governmental services or corporations, which are closed to the public and serve only their own employees or branches. Most ISPs are privately-owned, and two ISPs serve more than two-thirds of the market: SilkNet, with more than 44.5 percent of the market, and Caucasus Online, with a 32 percent share. Three of the 20 ISPs are also mobile operators.[20] A special report from Transparency International Georgia cites that many of the major telecommunications companies are owned by offshore shell companies.[21]

---

[13] "Ported Subscriber Numbers Statistics," Georgian National Communication Commission, May 25, 2011, http://www.gncc.ge/index.php?lang_id=ENG&sec_id=110&info_id=9071.

[14] "Porting of Subscriber Number of Fixed Network Started From Today," Georgian National Communication Commission, December 1, 2011, http://www.gncc.ge/index.php?lang_id=ENG&sec_id=110&info_id=9812.

[15] Mobile price plan calculator: http://online.gncc.ge/MobileCalc/MobileCalc2.aspx The Calculator gives users the ability to choose best plan and pricing options between mobile operators.

[16] Phone numbers now all begin with *0* and *00* prefixes.

[17] Georgian-language Facebook page statistics service, [in Georgian], http://like.ge/.

[18] According to a leading marketing specialist David Birman: "2011 was the year of discovery of social networks for Georgian Businesses." Commersant.ge, January 25, 2012, [in Georgian], http://www.commersant.ge/?id=6504.

[19] "Mayor Vows to Blanket Tbilisi with Free Wifi," Civil.ge, June 4, 2012, http://www.civil.ge/eng/article.php?id=24848.

[20] Data obtained in August 2013. For current data, see Top.ge at http://top.ge/all_report.php [in Georgian].

[21] A complex and compelling database of the ownerships and relations between companies is provided by TI under following address: http://goo.gl/AgsVL. Transparency International Georgia, "The State of the Internet: Who Controls Georgia's Telecommunications Sector?" February 2013, http://j.mp/16hJu3p.

The telecommunications infrastructure in Georgia is still weak and users may experience disconnections from the international internet up to two or three times per month, allowing them to access only Georgian websites. In general, the connection speed for accessing content hosted in Georgia is greater than for international content. There are many factors influencing the connection to the international backbone, including the major underground fiber-optic cable that is often threatened by landslides, heavy rain, or construction work along the road. However, contrary to instances in recent years when access throughout the entire country was disrupted, no significant outages were reported in 2012-2013.

The Georgian National Communications Commission (GNCC) is the main media and communications regulatory body and is also responsible for regulating online media, although there have yet to be many test cases regarding the latter. The GNCC mostly deals with mobile operators, as well as television and radio broadcasting licenses. However, there is no significant difference between GNCC procedures for handling traditional media and those pertinent to telecommunications and internet issues; thus, criticism surrounding the commission's alleged lack of transparency and flawed licensing procedures for traditional media may reappear in the context of internet regulation. Nevertheless, the GNCC has begun to involve the public in discussions and committee hearings, signaling that it is slowly turning toward openness and transparency. For example, the GNCC has started a project of monitoring the actual speed of the internet connection for customers of three main ISPs; however, the report is not yet available and the project may close before publication due to an alleged corruption case.

LIMITS ON CONTENT

There is no evidence of online content being blocked in Georgia in 2012–2013. In 2011, the government temporarily blocked access to torrent sites and peer-to-peer file sharing services to discourage the illegal download of a Hollywood action film about the 2008 Russian-Georgian war.[22] However, aside from this isolated incident, government censorship is not a major hindrance to internet freedom in Georgia.

YouTube, Facebook, and international blog-hosting services are freely available. Facebook is now the most popular website among internet users in Georgia, with bloggers and journalists increasingly using it to share or promote their content, gain readers, or start discussions on current events. Facebook is also used by civil activists and others as a tool for discussion about ongoing political and social events.

Users can freely visit any website around the world, upload or download any content, and contact other users via forums, social-networking sites, and instant messaging applications. In fact, content is so accessible that numerous sites offer illegal material such as pirated software, music, and movies, and the government has not enacted appropriate legal measures to combat the problem.

[22] "Cracking Down on Pirated August War Movie," Georgian America, 2011, http://georgianamerica.com/eng/news/cracking_down_on_pirated_august_war_movie_3179.

ISPs still host websites with a great deal of pirated material,[23] but visits to such sites have decreased and given way to social-networking, video-sharing, blogging, and news sites.[24] Within some state institutions and private companies, there are instances of website filtering software in place, designed to improve worker productivity by blocking access to sites such as Facebook and YouTube. At the same time, both governmental bodies and private employers are increasingly using social media for recruitment and public relations purposes.

There are no laws that specifically govern the internet, regulate online censorship, or ban inappropriate content such as pornography or violent material. There are also no blacklists or other registers of websites and online resources that should be blocked. Nevertheless, all legal regulations, particularly copyright or criminal law, apply directly to internet activities using legal analogy, and so far this legal ambiguity has not been exploited to impose significant internet content restrictions. However, there are some concerns about the impartiality of blocking decisions made by the GNCC. For example, the political nature of the 2011 decision by the GNCC to crack down on sites illegally hosting the film about the Georgian-Russian war, despite doing very little to combat online piracy in general, implies a lack of evenhanded decision making. To date, however, such decisions regarding online content have been rare.

Self-censorship among Georgian internet users is active to some extent but primarily centers on issues related to Georgian traditions, social norms, taboos, or religion. Instances of self-censorship due to political pressure have decreased over the past year. No cases of governmental manipulation of online content were reported—manipulation is neither systematic nor pervasive.

Inadequate revenues in the online news business, combined with a lack of technological knowledge, have hampered the expansion of traditional media outlets to the internet. The government's apparent interest in blogging and social media could help spur traditional outlets to establish a greater internet presence, but this would also require more private investment in online advertising. Currently, it is estimated that annual spending on online advertising does not exceed $1 million,[25] which is only approximately one percent of the total amount spent in the Georgian advertising market. At present, most online media outlets face difficulty in attracting advertisers; however, the market is rapidly changing and there are signs of improvement.

The Georgian blogosphere grew impressively to over 3,000 blogs in 2011,[26] and online activism continued to increase in the second half of 2012. Much of this online activity was related to the fact that several videos of prisoner torture and abuse were leaked on television broadcasts, which

[23] For example, the websites of Gol.ge (http://gol.ge/) and Adjarnet.com (http://adjaranet.com).
[24] "Top Sites in Georgia," Alexa, accessed August 2013, http://www.alexa.com/topsites/countries/GE.
[25] "The Georgian Advertising Market," Transparency International Georgia, December 2011, http://transparency.ge/sites/default/files/post_attachments/TI%20Georgia%20-%20The%20Georgian%20Advertising%20Market_0.pdf.
[26] Zakaria Babutsidze, et al., "The Structure of Georgian Blogosphere and Implications for Information Diffusion," European Consortium for Political Research, August 5, 2011, http://www.ecprnet.eu/MyECPR/proposals/reykjavik/uploads/papers/1676.pdf.

resulted in mass protests throughout Georgia and caused an unprecedentedly high number of video views, shares, and discussions among almost all Georgian websites, blogs and other services.[27]

Although most Georgians use the internet as a source of entertainment, various social media and communication apps have become important platforms for discussion and information exchange. In the months leading up to the October 2012 parliamentary elections, the National Democratic Institute partnered with three Georgian civil society groups—Transparency International Georgia, the International Society for Elections and Democracy, and the Georgian Young Lawyers' Association—to produce an election monitoring platform where citizens could report not only violations on election day, but also incidents in the months leading up to the election, such as fraudulent voter lists or the illegal use of government resources.[28]

Different political and civil society groups post calls for action on Facebook and use social media marketing tools for communicating with their supporters. However, most forms of online activism to date have remained online and have not had a significant impact offline. Minorities and vulnerable groups in general are not restricted from internet use, and are represented online through a small number of forums and blogs. During the last year, LGBT activists have started to extensively use online tools for coordination, distributing information, and protesting discrimination in the public sphere.

VIOLATIONS OF USER RIGHTS

Civil rights, including the right to access information and freedom of expression, are guaranteed by the Georgian constitution and are generally respected in practice.[29] The Law on Freedom of Speech and Expression makes it clear that other "generally accepted rights" related to freedom of expression are also protected even if they are not specifically mentioned.[30] Furthermore, Article 20 of the constitution and Article 8 of the Law of Georgia on Electronic Communications include privacy guarantees for users and their information, but they simultaneously allow privacy rights to be restricted by the courts or other legislation.[31] Online activities can be prosecuted under these laws—mainly in cases of alleged defamation, which was decriminalized in 2004—or under any applicable criminal law. Furthermore, a huge discussion on the independence of the judiciary has been taking place in Georgian society. International organizations such as Transparency International and Georgian NGOs such as the Georgian Young Lawyers Association have reported that despite recent reforms and changes in the judiciary system, its independence is still tenuous

[27] "Videos of Inmate Abuse, Rape Emerge," Civil.ge, September 19, 2012, http://www.civil.ge/eng/article.php?id=25220.
[28] Chris Doten, "Only Amateurs Steal Elections at the Ballot Box," NDItech DemocracyWorks, February 21, 2012, https://demworks.org/blog/2012/02/only-amateurs-steal-elections-ballot-box.
[29] The constitution is available in English at: http://www.parliament.ge/index.php?lang_id=ENG&sec_id=68.
[30] Article 19, *Guide to the Law of Georgia on Freedom of Speech and Expression* (London: Article 19, April 2005), http://www.article19.org/pdfs/analysis/georgia-foe-guide-april-2005.pdf.
[31] The law is available in English on the GNCC website at: http://www.gncc.ge/index.php?lang_id=ENG&sec_id=7050&info_id=3555.

and "suffers from undue influence exerted by the Prosecutor's Office and the executive authority."[32]

Nevertheless, there were no cases of charges against online users for libel or other internet activities in 2012–2013. There were also no known instances of detention or prosecution, and compared to previous years, there were no reported occurrences of extralegal intimidation or violence against users.

The Georgian Law on Operative-Investigative Activity, passed in 1999, grants the police and security services significant discretion in conducting surveillance. Police can generally begin surveillance without a court's approval, though they must obtain it within 24 hours. There are some official requirements for launching such monitoring, but in reality it is sufficient to label the targeted individual a suspect or assert that he or she may have criminal connections. New amendments to the law promulgated in September 2010 require that websites, mail servers, ISPs, and other relevant companies make private communications data such as e-mail and chats available to law enforcement authorities when court approval is obtained.[33] There were no known cases of this occurring in 2012; however, it was reported from an anonymous executive in the government that the monitoring infrastructure is still in place and allows governmental bodies to monitor and collect data on citizens' telecommunication usage, habits, browsing history, and other details. In the spring of 2013, the Interior Minister and the State Prosecutor declared that all of the data which was collected during previous years under the named law would be destroyed.[34]

Additionally, ISPs and mobile phone companies are obliged to deliver statistical data on user activities concerning site visits, traffic, and other topics when asked by the government. Cybercafes, on the other hand, are not obliged to comply with government monitoring, as they do not register or otherwise gather data about customers. Individuals are required to register when buying a SIM card in order to obtain a phone number.

Cyberattacks against opposition websites have not been a significant issue in Georgia, with the latest major attacks occurring in 2008 and 2009 in relation to political tensions between Georgia and Russia. By the end of 2012, the Data Exchange Agency started monitoring Georgian websites for the presence of malicious codes, hacking attacks, or other suspicious activities, publishing the information regularly on their website[35] as well as on their official Facebook page.[36]

---

[32] Erekle Urushadze, "Judiciary," in *National Integrity System – Georgia*, ed. Caitlin Ryan (Transparency International – Georgia, 2011), http://transparency.ge/nis/2011/judiciary.
[33] Tamar Chkheidze, "Internet Control in Georgia," Humanrights.ge, November 17, 2010, http://www.humanrights.ge/index.php?a=main&pid=12564&lang=eng.
[34] Barbara Frye, Ioana Caloianu, Vladimir Matan, and Molly Jane Zuckerman, "Georgia Offers Amnesty to Collect Illegal Surveillance Tapes, Baku Hits Back at RFE," Transitions Online, July 29, 2013, http://www.tol.org/client/article/23879-georgia-offers-amnesty-to-collect-illegal-surveillance-tapes-baku-hits-back-at-rfe.html.
[35] Data Exchange Agency homepage, http://dea.gov.ge.
[36] CERT Facebook page, https://www.facebook.com/certgovge.

GERMANY

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	4	4
Limits on Content (0-35)	3	4
Violations of User Rights (0-40)	8	9
Total (0-100)	15	17

* 0=most free, 100=least free

POPULATION: 81.8 million
INTERNET PENETRATION 2012: 85 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- A federal regulatory decision made on April 10, 2013 regarding vectoring technology and the prices charged for "last mile" access has the potential to further entrench the market dominance of the leading ISP, Deutsche Telekom (see **OBSTACLES TO ACCESS**).
- A Federal Court of Justice decision in July 2012 placed greater liability on host providers, stipulating that once the provider is made aware of copyright-infringing material, they must take steps to prevent further instances of that material being uploaded to their platform (see **LIMITS ON CONTENT**).
- In May 2012, amendments to the telecommunication act included a provision that would allow the government to define basic requirements for non-discriminatory data transfer and access with a view of safeguarding net neutrality. However, the government has not yet established any requirements (see **LIMITS ON CONTENT**).
- Amendments to the telecommunication act also lowered the threshold for public agencies to access individual user data, including sensitive data such as name, address, date of birth, user passwords and dynamic IP addresses (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Germany has a high level of internet and mobile phone penetration, and only the adoption of high-speed broadband is lagging behind other highly developed countries. However, the fact that regulators are allowing the use of vectoring technology to further the development of superfast broadband internet has encountered criticism, given that this technology allows the largest internet service providers (ISPs) to maintain some of their market dominance.

While media and internet freedom principles are generally well-respected, legally codified, and have been repeatedly affirmed in Germany, certain trends over the past year have challenged these principles. In this respect, changes in online copyright enforcement legislation and practices are starting to limit the liability privilege of ISPs and host providers. Intermediaries are now required to implement specific filter and blocking systems in order to prevent further the infringement of copyright protected materials, which might also lead to undesirable private censorship as companies attempt to avoid this liability.

The struggle for net neutrality continues to be an ongoing issue of public debate in Germany. Amendments to the telecommunication act in May 2012 stipulated that the government could require ISPs to offer internet access in a content-neutral fashion, which would be a significant step toward net neutrality. However, the amendment does not automatically safeguard this principle; rather, it requires the government to take further action by defining the minimum quality standards with which ISPs must comply. Meanwhile, German telecommunications companies introduced revised customer contracts that have revived concerns about their non-transparent traffic management practices.

Against a broad coalition of societal actors, legislators also extended the scope of the "stored data inquiry" (*Bestandsdatenauskunft*) through the amended telecommunication act of 2013. Data protection experts criticize the lower threshold for intrusions of citizens' privacy as disproportionate and are considering another constitutional complaint against the telecommunication act.

OBSTACLES TO ACCESS

Germany's network infrastructure for information and communication technologies is well-developed, with 76 percent of the population in Germany having private internet access. Together with the number of mobile-only internet users, this has resulted in an overall internet penetration rate of 85 percent, which is 10 percentage points above the European Union (EU) average.[1]

[1] Eurostat, "Broadband and Connectivity - Households", April 29, 2013, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15b_h&lang=en. Official International Telecommunication Union (ITU) data places the internet penetration rate for 2012 at 84 percent. See International Telecommunication Union (ITU), "Percentage of individuals using the Internet," 2012, accessed July 8, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx.

However, growth in internet penetration is clearly slowing down, with figures increasing by only 2.5 percentage points in 2012 in contrast to increases of 5–6 points in the years before.[2] Also, few individuals who currently do not use the internet are planning to obtain access in the future.[3]

Internet connections in private homes are almost universal, with 93 percent of households having a broadband connection of at least 1 Mbps and only 5 percent still using slower dial-up connections.[4] The most widely used access technique is still DSL (82 percent), but cable internet connections are becoming more widespread (11 percent).[5] With regard to high-speed broadband connections, there is a remarkable gap between supply and demand. On the supply side, connections with more than 50 Mbps are available for about 55 percent of households.[6] On the demand side, adoption is lagging behind: only 9 percent of households actually subscribe to fast connections between 30 and 100 Mbps.[7] Regarding the take-up of connections of at least 10 Mbps, Germany is also lagging behind internationally with only 33 percent of households having such connections, in comparison to the EU average of 48 percent.[8] For this reason, the federal regulator has been criticized for supporting controversial vectoring technology instead of focusing on the roll-out of fiber-optic broadband.[9]

Mobile phone penetration in Germany is almost universal, with a penetration rate of over 132 percent.[10] The adoption of mobile internet access increased from 28 to 40 percent in early 2013,[11] which is rather slow by international standards.[12] While 72 percent of mobile internet users have additional landline access, mobile internet is the only form of internet access for almost a third of

[2] Birgit van Eimeren/Beate Frees, "76 Prozent der Deutschen online - neue Nutzungssituationen durch mobile Endgeräte. Ergebnisse der ARD/ZDF-Onlinestudie 2012" [76 percent of Germans are online – new usage situations by mobile devices], Media Perspektiven 7-8/2012, p. 362-379, http://www.ard-zdf-onlinestudie.de/fileadmin/Online12/0708-2012_Eimeren_Frees.pdf; Other surveys report up to 79 per cent, cf.: Initiative D21, "(N)Onliner Atlas 2012. Basiszahlen für Deutschland" [Baseline numbers for Germany], 2012. http://www.initiatived21.de/wp-content/uploads/2012/06/NONLINER-Atlas-2012-Basiszahlen-f%C3%BCr-Deutschland.pdf; Forschungsgruppe Wahlen, "Internet-Strukturdaten. Repräsentative Umfrage" [Structural internet data. representative survey], IV quarter of 2012, http://www.forschungsgruppe.de/Aktuelles/Internet-Strukturdaten/web_IV_12_1.pdf.

[3] Initiative D21, 2012, p. 4.

[4] Statistisches Bundesamt [Federal Statistical Office], "28 Millionen Haushalte in Deutschland haben einen Breitbandanschluss" [28 million households in Germany have a broadband connection], press release No. 474, December 19, 2011, https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2011/12/PD11_474_63931.html.

[5] Ibid.

[6] TÜV Rheinland Consulting, "Bericht zum Breitbandatlas Ende 2012 im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi)" [Report of the Broadband Atlas End of 2012 on behalf of the Ministry of Economics and Technology], Part 1, 2012, p. 6, http://www.zukunft-breitband.de/DE/Service/publikationen,did=559116.html.

[7] Kai Lukas/Almuth Marx/Bernd Oliver Schöttler/Christoph Sudhues, "Abschlussbericht 'Dienstequalität von Breitbandzugängen' Studie im Auftrag der Bundesnetzagentur" [Final report 'Service quality of broadband access' Study on behalf of the Federal Network Agency], April 9, 2013, p. 54, http://www.initiative-netzqualitaet.de/fileadmin/user_upload/Abschlussbericht_BNetzA_Studie_Dienstequalitaet_Breitbandzugaenge.pdf.

[8] European Commission, Digital Agenda Scoreboard, http://bit.ly/1h9FS4d.

[9] Die Telekom forciert VDSL-Vectoring statt Glasfaser" [Fiber to the Neverland. DT pushes VDSL-Vectoring instead of Fibre], c't 10/2013, April 29, 2013, pp. 18-21, http://heise.de/-1847272; Volker Briegleb, "Vectoring: Regulierer genehmigt VDSL-Turbo" [Vectoring: Regulator approves VDSL-Turbo]. heise-online, April 09, 2013, http://heise.de/-1837933.

[10] Bundesministerium für Wirtschaft und Technologie [Federal Ministry of Economics and Technology], "Monitoring-Report Digital Economy 2012", November 2012, p. 52 http://bmwi.de/EN/Service/publications,did=542994.html.

[11] Initiative D21/Huawei Technologies Deutschland (Ed.), Mobile Internetnutzung [mobile internet usage], February 2013, p. 8, http://www.initiatived21.de/wp-content/uploads/2013/02/studie_mobilesinternet_d21_huawei_2013.pdf.

[12] Bundesministerium für Wirtschaft und Technologie, 2012, p. 66.

these users. This is reflected in a high share of smartphone users (45.1 percent)[13] and flat rate data contracts (77 percent).[14] While the availability of basic UTMS connections is good (85 percent of all German households), the coverage of fast LTE technology is still growing in Germany, with half of all households being covered.[15]

Apart from the overall number of subscribers, there have also been changes in the socio-demographic composition of internet users. While there are still more men than women accessing the internet in Germany (81 percent compared to 70.5 percent), the increase of female users compared to male users was slightly higher in 2012, resulting in a smaller gender-difference of 10.5 percentage points compared to 11.8 percent in 2011. Internet penetration is particularly high in the age group 40 and younger (94.1 percent) but, in comparison, relatively low in the age group 70 and above (28.2 percent).[16] However, it is worth noting that in the older cohorts there is the highest growth rates of internet usage; for example, the internet penetration of those older than 70 has increased by 3.6 percent since 2011.[17]

Differences in internet usage depending on formal education did not significantly change in the past year; therefore, the mismatch between people with low and high levels of formal education using the internet is still about 20 percent. This phenomenon is confirmed by a comparison of net household incomes. Households with less than €1,000 net income per month have a 54.2 percent penetration rate, whereas those with more than €3,000 net income have a penetration rate of 92.7 percent.[18] Furthermore, differences in internet usage exist between Germany's western region (78 percent) and the eastern region that once constituted the communist German Democratic Republic (70 percent). This difference decreased by one percent from 2011 to 2012.[19] Nevertheless, the gap in internet penetration between urban states like Hamburg, Berlin, and Bremen and rural states such as Lower-Saxony decreased from 16 percent in 2011 to only 13 percent in 2012.[20]

Prices for flat rate broadband internet have been relatively stable over recent years and now range from €20 to €40 ($26 to $53) which is regarded as affordable compared to the average income per household of €3,578, and ranks below average prices in OECD countries.[21] Nevertheless, as the stark differences in internet usage in relation to income indicate, the price level constitutes a barrier for people with low incomes and the unemployed. Although the Federal Court of Justice ruled that access to the internet is fundamental for everyday life, costs for internet access are not adequately

[13] Bundesministerium für Wirtschaft und Technologie, 2012, p. 53.
[14] Bundesministerium für Wirtschaft und Technologie, 2012, p. 66.
[15] TÜV Rheinland Consulting, 2012, p. 4. With the allocation of licenses for the next generation mobile standard LTE, the Bundesnetzagentur has obliged the network providers to build the new infrastructure in rural areas first before installing it cities.
[16] Initiative D21, 2012, p. 5 ; Forschungsgruppe Wahlen, 2012, cf. fn. 1.
[17] Initiative D21, 2012, p. 5.
[18] Initiative D21, 2012, p. 5.
[19] Forschungsgruppe Wahlen, "Internet-Strukturdaten. Repräsentative Umfrage" [Structural internet data. representative survey], IV quarter of 2011, http://www.forschungsgruppe.de/Umfragen/Internet-Strukturdaten/web_IV_11_1.pdf ; And Forschungsgruppe Wahlen, 2012, cf. fn. 1.
[20] Initiative D21, 2012, p. 6.
[21] Statistisches Bundesamt [Federal Statistical Office], "Wirtschaftsrechnungen 2010" [Budget Surveys 2010], Subject-matter series 15 series 1, August 2, 2012, p. 13, http://bit.ly/VfYRV7; OECD Broadband Portal, Broadband Prices, September 2011, http://www.oecd.org/sti/broadband/oecdbroadbandportal.htm.

reflected in basic social benefits.[22] Telecommunication services have become slightly less expensive, decreasing by 2.7 percent, [23] and the costs for mobile internet usage and telephones have decreased by 3.5 percent.[24]

The telecommunications sector was privatized in the 1990s with the aim of fostering competition. Over the past decade, market consolidation has led to a competitive environment dominated by large companies both in fixed-line as well as mobile internet access; consequently, several smaller ISPs have been forced out of business. The incumbent Deutsche Telekom's share of the broadband market is 45 percent. Other relevant ISPs are 1&1-United Internet and Arcor-Vodafone (each with 12 percent of the market), O2-Telefónica (9 percent), and cable companies Unity Media (8 percent) and Kabel Deutschland (6 percent).[25]

There are four general carriers for mobile internet access: T-Mobile, Vodafone, E-Plus, and O2-Telefónica. In 2012, T-Mobile regained its market leadership from Vodafone, gaining a 32 percent market share compared to Vodafone's 30 percent. The smaller providers, E-Plus and O2-Telefónica, have been steadily gaining market shares, with 21 percent and 17 percent of the market, respectively.[26] The mobile market is seen as one of the most competitive in the EU,[27] though competition of mobile services in downstream markets is limited, since most German mobile providers contractually prohibit services such as Voice over Internet Protocol (VoIP) or even instant messaging.[28] The Body of European Regulators for Electronic Communications (BEREC) is investigating this widespread practice of carriers across Europe and discussing possible regulatory interventions.[29]

Internet access, both broadband and mobile, is regulated by the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway (*Bundesnetzagentur* or BNetzA) operating under the supervision of the Federal Ministry of Economics and Technology. The president and vice president of the agency are appointed for five-year terms by the German federal government,

---

[22] Bundesgerichtshof [Federal Court of Justice], "Bundesgerichtshof erkennt Schadensersatz für den Ausfall eines Internetanschlusses zu" [Court awards damages for internet failures], press release 14/13, January 24, 2013, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&pm_nummer=0014/13. Hartz IV standard rate is € 382, of which € 2.28 are for Internet access, Cf. Deutscher Bundestag [German Bundestag], Drucksache 17/3404, p. 60, http://dip21.bundestag.de/dip21/btd/17/034/1703404.pdf.

[23] Statistisches Bundesamt, "Statistisches Jahrbuch. Deutschland und Internationales" [Statistical Yearbook], 2012, p. 402, https://www.destatis.de/DE/Publikationen/StatistischesJahrbuch/StatistischesJahrbuch2012.pdf?__blob=publicationFile.

[24] Bundesministerium für Wirtschaft und Technologie, 2012, p. 42.

[25] Bundesnetzagentur, "Jahresbericht 2012" [Annual Report 2012], May 6, 2013, http://bit.ly/1eNOUXS. DSLWEB ; "Breitband Report Deutschland Q3 2012" [Broadband Report Germany], http://bit.ly/TvtFOy.

[26] Bundesnetzagentur [Federal Network Agency], "Teilnehmerentwicklung im Mobilfunk" [Development of Mobile Subscriptions] , May 13, 2013, http://bit.ly/1h9FtPn; FAZ.net, "T-Mobile ist wieder das beliebteste Handynetz" [T-Mobile is again the most popular mobile phone network], November 13, 2012, http://www.faz.net/-gqi-74br2.

[27] European Commission, Digital Agenda for Europe – Scoreboard 2012, p.68. Cf. also the study by Haucaup et al. documenting a fairly competitive market: Haucap/Heimeshoff/Stühmeier, 2010, "Wettbewerb im Deutschen Mobilfunkmarkt" [Competition in the German mobile market], Ordnungspolitische Perspektiven Nr. 4.

[28] Ekkehard Kern, "Die Tücken der Smartphone-Verträge" [The pitfalls of smartphone contracts], welt.de, April 8, 2013, http://www.welt.de/finanzen/verbraucher/article115087088/Die-Tuecken-der-Smartphone-Vertraege.html.

[29] BEREC, "BEREC publishes net neutrality findings and new guidance for consultation", Press release, May 29, 2012, http://berec.europa.eu/eng/document_register/subject_matter/berec/press_releases/24-berec-publishes-net-neutrality-findings-and-new-guidance-for-consultation. According to this study, at least 20 percent of mobile internet users in Europe experience some form of restriction on their ability to access VoIP services.

following recommendations from an advisory council consisting of 16 members from the German Bundestag and 16 representatives from the Bundesrat. The German Monopolies Commission and the European Commission (EC) have both criticized this highly political setting and the concentration of important regulatory decisions in the presidential chamber of the Federal Network Agency.[30] Similarly, the European Court of Justice (ECJ) and the EC noted that the regulation of data protection and privacy by agencies under state supervision does not comply with the EU Data Protection Directive 95/46/EC.[31]

In addition to such institutional concerns, regulatory decisions by the BNetzA have been criticized for providing a competitive advantage to Deutsche Telekom, the former state-owned monopoly.[32] The most recent examples are the agency's decisions on April 10, 2013 to allow a slight increase in the price that Telekom charges competitors for the "last mile"[33] and to support controversial vectoring technology, which in turn manifests its dominant position regarding the last mile. Vectoring can boost the bandwidth of DSL connections on existing copper lines but requires one operator to manage the whole bundle, in effect limiting the unbundling of the local loop and thus privileging, under specific circumstances, the market leader.[34]

LIMITS ON CONTENT

Blocking of websites or internet content rarely takes place in Germany.[35] In 2012-2013, there were no publicly known incidents of censorship directly carried out by state actors. Since there is also no significant filtering of text messages or e-mail communication, the overall scale and sophistication of censorship has remained stable and on a non-significant level. YouTube, Facebook, Twitter and international blog-hosting services are freely available.

---

[30] Monopolkommission [Monopolies Commission], "Telekommunikation 2009: Klaren Wettbewerbskurs halten" [Telecommunication 2009: stay on target in competition], Sondergutachten 56, 2009, p. 75, http://www.monopolkommission.de/sg_56/s56_volltext.pdf; European Commission, "Progress Report on the Single European Electronic Communications Market (15th Report)", COM(2010) 253, p. 196, http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/annualreports/15threport/15report_part1.pdf.

[31] European Commission, "Data Protection: European Commission requests Germany to ensure independence of data supervisory authority," Press Release, Brussels, April 6, 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/407&format=HTML&aged=0&language=EN&guiLanguage=en.

[32] European Commission, Progress Report, p. 196. Since the Federal Republic still exercises its rights as a shareholder of Deutsche Telekom (circa 38 percent) through another public law entity, commentators see a potential conflict of interest; Christian Schmidt, "Von der RegTP zur Bundesnetzagentur. Der organisationsrechtliche Rahmen der neuen Regulierungsbehörde" [From RegTP to Federal Network Agency. The organizational framework of the new regulator], Die Öffentliche Verwaltung 58 (24), 2005, p. 1028.

[33] ZDNet, "Neuer Vorschlag der Bundesnetzagentur für TAL-Entgelte erntet Kritik" [Network Agency's Plans for Local Loop Unbundling Charges is criticized strongly], March 28, 2013, http://www.zdnet.de/88149343/neuer-vorschlag-der-bundesnetzagentur-fur-tal-entgelte-erntet-kritik/. An international tariff comparison in 2011 showed that the price level in Germany is one of the highest in Europe: Bundesnetzagentur [Federal Network Agency], "International Tariff Comparison", 2011, http://bit.ly/19a3uAJ.

[34] Richard Sietmann, "Fiber to the Neverland. Die Telekom forciert VDSL-Vectoring statt Glasfaser" [Fiber to the Neverland. DT pushes VDSL-Vectoring instead of Fibre]. c't 10/2013, April 29, 2013, pp. 18-21, http://heise.de/-1847272.

[35] Due to substantial criticism by activists and NGOs that provoked an intense political debate, the 2010 law on blocking websites containing child pornography, the Access Impediment law (Zugangserschwerungsgesetz), never came into effect and was finally repealed by the German parliament in December 2011.

Content blocking or filtering practices enforced by corporate actors have been discussed for some time. The ongoing dispute between YouTube and GEMA (German Society for Musical Performance and Mechanical Reproduction)[36] indicates that private entities substantially shape the availability of online content: 61.5 percent of the most popular music videos on YouTube are blocked in Germany.[37] Since 2009, YouTube has refused to pay for a license for copyright-protected music videos disseminated on its platform, and instead shows an error message saying that the video is not available in Germany because GEMA has not granted the publishing rights.[38] YouTube has also been legally required to remove protected content upon request under the breach of duty of care.[39] GEMA holds a de facto monopoly because it exercises rights exclusively and considers it a copyright violation when YouTube uses "the rights administered by GEMA without paying any compensation to the copyright owners,"[40] and consequently sues Google for damages.[41] Google has raised concerns about undesired harms for freedom of expression.[42] The issue is most likely to continue in the courts as both parties filed appeals in May 2012.[43]

In a few cases, private content regulation practices based on the enforcement of corporate terms of service were the subject of controversial public discussions. For example, in March 2013 a German radio host's critical Facebook posts about the Catholic Church and the new pope's attitude toward same-sex marriage were deleted by Facebook without offering any reasons or the possibility to restore the post.[44] The scale and scope of such practices remain non-transparent.

New evidence has confirmed that ISPs across Europe regularly use deep packet inspection (DPI) for the purposes of traffic management, but also to throttle peer-to-peer traffic. Users are especially affected by P2P-related restrictions in the mobile market.[45] In Germany, there is a clear lack of

[36] Collecting societies are private organizations at the national level in Germany authorized by the Copyright Administration Act. Although they act under the supervision of the German Patent and Trademark Office, they belong to the private sector. The foundation requires an exemption from the antitrust laws by the Federal Cartel Office.
[37] Compared to 0.9 per cent in the United States and ca. 1 per cent in Austria and Switzerland. Cf. sueddeutsche.de, "Diese Kultur ist in Deutschland leider nicht verfügbar" [This culture is not available in Germany], January 28, 2013, http://sz.de/1.1584813
[38] GEMA demands 0.375 cents per retrieval.
[39] LG Hamburg [Regional Court Hamburg], judgment of April 20, 2012, Az. 310 O 461/10, http://openjur.de/u/311130.html ; cf. also EDRI, "YouTube loses a case in Germany to collective society Gema", April 25, 2012, http://www.edri.org/edrigram/number10.8/youtube-gema-case.
[40] GEMA, "GEMA and YouTube", accessed May 20, 2013, https://www.gema.de/en/press/popular-subjects/youtube/browse/4.html.
[41] Süddeutsche.de, "Streit mit Youtube: Gema schaltet Schiedsstelle ein" [Dispute with Youtube: Gema calls in arbitration body], January 10, 2013, http://sz.de/1.1570166.
[42] In particular Google argues that because the GEMA doesn't provide a list on the complete repertoire they licensed, most music videos have been blocked in order to avoid financial risks. cf. http://www.djv-bb.de/cms/nachrichten/2013-02-16_GEMA_YouTube_Pressefreiheit.php
[43] Süddeutsche.de, Gema legt Berufung gegen YouTube-Urteil ein [Gema files an appeal against YouTube-jugdement], May 22, 2012, http://sz.de/1.1362833
[44] Tina Kulow, "Was ist mit dem Post von Domian passiert?" [What has happened with Domain's post?], March 19, 2013, https://www.facebook.com/notes/tina-kulow/was-ist-mit-dem-post-von-domian-passiert/625428644149658.
[45] BEREC, "A view of traffic management and other practices resulting in restrictions to the open Internet in Europe. Findings from BEREC's and the European Commission's joint investigation," May 29, 2012, http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf.

transparency regarding the scope of traffic management, particularly surrounding the use of DPI, since ISPs are not required to provide the public with such information.

While there is no systematic blocking and filtering of content by the state, instances of the courts or public authorities ordering the deletion of certain content have become common. In October 2012, the U.S.-based company Twitter complied with a request to close the account of a neo-Nazi group deemed illegal by German authorities.[46] Twitter did not delete the account but started to restrict access to it for German users only.[47] This action was the first application of Twitter's new policy, introduced in January 2012, to block content and accounts on a country-by-country basis in order to balance free speech principles with its compliance of local laws. The specific decision did not arouse much controversy in Germany, and has rather been regarded as a transparent way to minimize censorship.[48]

The autocomplete function of Google's search engine has been repeatedly subject to scrutiny. In September 2012, Germany's former first lady sued Google for defamation over suggested words. The lawsuit demanded that Google delete 85 suggested words, and furthermore, requested the deletion of search results indexing articles that cover the issue. Google partly complied by deleting eight of the 3,000 results from the index due to unlawful and false statements of fact.[49] Following a considerable history of court rulings,[50] in May 2013 the Federal Court of Justice, in a different case, ruled that Google could be held liable, at least under some circumstances, for the infringement of personal rights through its autocomplete function.[51]

There is no censorship prior to the publication of internet content. On the other hand, figures released by ICT corporations concerning the amount of content removal requests received from governments, public authorities, or copyright owners indicate that post-publication content removal is used extensively. Microsoft has started to report the numbers of removal requests on a country-by-country basis. Notably, none of those requests resulted in a disclosure of customer content.[52] According to Google's latest transparency report covering the period from July to December 2012, the company received 231 requests from the German government and public authorities.[53] Based on absolute numbers, Germany ranks third on a list of 65 countries that issued requests for removal of content, following Brazil and the United States. To an unprecedented

[46] The group 'Besseres Hannover' [Better Hanover] has been monitored by the German police for some time and finally banned by the state's interior ministry. Cf. Twitter Inc., "Transparency Report. Removal Requests July 1 – December 31, 2012", 2013, https://transparency.twitter.com/removal-requests-ttr2.

[47] Twitter's general counsel, Alex MacGillivray has announced the issue on Twitter: Alex MacGillivray, October 18, 2012, https://twitter.com/amac/status/258745846584188928.

[48] Twitter reported the case to chillingeffects.org and has made the request by German police authority publicly available: Chilling Effects, "German Police ask Twitter to Close Account", https://www.chillingeffects.org/notice.cgi?sID=625342.

[49] Zeit Online, "Google löscht einige Bettina-Wulff-Einträge" [Google deletes several Bettina-Wulff-entries], November 11, 2012, http://www.zeit.de/digital/datenschutz/2012-11/google-wulf-loeschung.

[50] OLG Köln [Higher Regional Court Cologne], judgment of May 10, 2012, Az. 15 U 199/11, http://openjur.de/u/462365.html.

[51] BGH [Federal Supreme Court], judgment of May 14, 2013, Az. VI ZR 269/12; Jürgen Kuri/Martin Holland, "BGH zu Autocomplete: Google muss in Suchvorschläge eingreifen" [BGH on autocomplete], May 14, 2013 http://heise.de/-1862062.

[52] Microsoft, "2012 Law Enforcement Requests Report", http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/.

[53] Google complied fully or partially with 77 percent of these requests. Google, "Google Transparency Report. Germany. July to December 2012," 2013, http://www.google.com/transparencyreport/removals/government/DE/?p=2012-12.

degree, requests were mandated by court orders (192 requests), most commonly for defamation reasons. The total number of items requested to be removed was 1,105. The most requested items to be removed were for defamation, adult content, and hate speech matters. German youth protection authorities have continuously requested the removal of content deemed to violate German youth protection legislation, especially videos on YouTube.[54]

The protection of minors constitutes an important legal framework for the regulation of online content.[55] Youth protection on the internet is principally addressed by states through the Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting (JMStV), which bans content similar to that outlawed by the criminal code, such as the glorification of violence and sedition.[56] A controversial provision of the JMStV reflecting the regulation of broadcasting media mandates that adult-only content on the internet, including adult pornography, must be made available in a way that verifies the age of the user.[57] Compliance with the interstate agreement is supervised by the Commission for Youth Protection Relating to Media (KJM) and supported by a joint body, *jugendschutz.net*, which operates a hotline for complaints. Notably, the JMStV enables the blocking of content if other actions against offenders fail and if such blocking is expected to be effective. Offending websites hosted outside of Germany are put on blacklists that are made available for privately developed filtering software. Members of the self-regulatory body, Voluntary Self-control for Multimedia Service Providers (FSM), are committed to removing blacklisted websites from their search results. In February 2013, the Federal Minister of Family Affairs, Senior Citizens, Women and Youth, in cooperation with internet industry partners and *jugendschutz.net*, introduced a proxy server meant to ensure safer internet use for children.[58] The software is offered at no charge for individual download and is available for mobile devices as well as computers. Presently, two filtering software solutions for youth protection are officially approved by the KJM.[59]

The liability of platform operators for illegal content is regulated by the telemedia act. The law distinguishes between full liability for owned content and limited "Breach of Duty of Care" (*Stoererhaftung*) of access providers and host providers for third party content.[60] Although access and host providers[61] are not generally responsible for the content they transmit or temporarily auto store, there is a certain tension between the underlying principles of liability privilege and that of

[54] According to the German Report for the first and second half of 2012 (cf. Fn. 51) youth protection authorities requested a total of 451 videos to be removed from YouTube.
[55] The legal framework regulating media protection of minors in particular consists of the Law for the protection of children and youth ("Jugendschutzgesetz", JuSchG) of the federal government and the Interstate Treaty on the Protection of Minors in the Media (short "Jugendmedienschutzstaatsvertrag", JMStV).
[56] Cf. the respective §§ 130, 131 StGB [Crimical Code]. English translation: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.
[57] Cf. the respective § 5, Abs. 3 JMStV.
[58] KinderServer homepage, accessed August 19, 2013, http://www.kinderserver-info.de/
[59] Monika Ermert/Andreas Wilkens, "Neuer Anlauf für den Jugendmedienschutzstaatsvertrag" [New attempt to reform the Interstate Treaty on the Protection of Minors in the Media], February 22, 2013, http://heise.de/-1809147.
[60] In particular: Part 3, §§ 7-10 TMG: liability for own content (§ 7, Abs. 1 TMG); limited liability for access providers (§§ 8, 9 TMG) and host providers (§ 10 TMG).
[61] The BGH in particular has developed the principles of limited liability of host providers: BGH [Federal Court of Justice], judgment of October 25, 2011, Az. VI ZR 93/10.

secondary liability.[62] Principally, ISPs are not required to proactively control or review the information of third parties on their servers; they become legally responsible as soon as they gain knowledge of violations or violate reasonable audit requirements.[63]

In 2012, court rulings limited the liability privilege of ISPs by further specifying requirements, responsibilities, and obligations. Notably, these have commonly occurred in relation to copyright enforcement online. In this respect, additional blocking and filter obligations of host providers have been put in more concrete terms by the Federal Court of Justice (*Bundesgerichtshof*, BGH) in the "Alone in the Dark" case.[64] In the specific instance, the game publisher Atari sued the file hosting service Rapidshare for copyright violations concerning the video game "Alone in the Dark." Although the judges did not hold Rapidshare liable for a direct infringement, they saw a violation of the service's monitoring obligation under the breach of duty of care. Once the file hosting service was notified of one infringing copy, the court said, it should have proactively controlled its service for other copies of the same material.[65] Hosting services are now supposed to implement technically and economically reasonable mechanisms in order to prevent any further violations of the respective copyright.

In addition to the mere deletion of relevant data, the court also deemed manual post-filtering by words and the control of external link collections technically reasonable. Depending on the current technical standard, automated control mechanisms can also be considered.[66] Furthermore, ISPs are obliged to disclose customer information for prosecutions of copyright infringement, even though the person may not have infringed copyrights for commercial purposes.[67] A special requirement to review the content on any violations of rights was also ruled in a case where a blogger integrated a YouTube video onto his website.[68] Whereas linking to other websites is regarded as unproblematic, embedding content, primarily videos from other sources, could cause liability risks for the provider.[69]

An important exception to the liability privilege concerns wireless networks.[70] Because of a highly disputable ruling against the existing liability privilege by the Federal High Court in 2010,

---

[62] Liability privilege means that information intermediaries on the internet such as ISPs are not responsible for the content their customers transmit. Secondary or indirect liability applies when intermediaries contribute to or facilitate wrongdoings of their customers.
[63] BGH [Federal Court of Justice], judgment of March 27, 2012, Az. VI ZR 144/11, http://openjur.de/u/405723.html.
[64] BGH [Federal Court of Justice], judgment of July 12, 2012, Az. I ZR 18/11, http://openjur.de/u/555292.html.
[65] Timothy B. Lee: Top German court says RapidShare must monitor link sites for piracy, July 16, 2012, http://arstechnica.com/tech-policy/2012/07/top-german-court-says-rapidshare-must-monitor-link-sites-for-piracy/.
[66] Thomas Stadler, "BGH: Rapidshare muss Wortfilter einsetzen und externe Linksammlungen überprüfen" [Federal Court of Justice: Rapidshare is required to deploy filters by words and to screen external link collections], February 2, 2013, http://www.internet-law.de/2013/02/bgh-rapidshare-muss-wortfilter-einsetzen-und-externe-linksammlungen-uberprufen.html.
[67] Bundesgerichtshof [Federal Court of Justice], judgement of April 19, 2012, Az. I ZB 80/11, http://openjur.de/u/438903.html.
[68] LG Hamburg [Regional Court Hamburg], judgement of May 18, 2012, Az. 324 O 596/11, http://openjur.de/u/404386.html.
[69] Leonhard Dobusch, "Risikofaktor Einbettung: YouTube, Twitter und das Urheberrecht" [Risk factor embedding: YouTube, Twitter and copyright legislation], January 23, 2013, http://netzpolitik.org/2013/risikofaktor-einbettung-youtube-twitter-und-das-urheberrecht/.
[70] In 2010, the German Federal High Court sentenced the private owner of a wireless router on the grounds that his or her open network allowed illegal activities. cf. Christopher Burgess, "Three Good Reasons to Lock Down Your Wireless Network," The

legislative initiatives from states and political parties now seek to modify the secondary liability of local Wi-Fi operators.[71]

Content hosts have also been pursued for further investigations for opinions expressed by third parties on their platforms, as single cases indicate. In these cases, authorities have required platform owners to provide the real names of users who were prosecuted for defamation reasons. They even went so far as to search the editorial office of a newspaper, which was later ruled as being unlawful,[72] and to order a coercive detention for an online editor because he refused to provide the user's name.[73] In the latter case, the editor invoked his right to refuse testimony and has appealed to the Federal Constitutional Court (*Bundesverfassungsgericht*, BVerfG).

The principle of proportionality has constitutional status in Germany to which public authorities must comply. All means taken by the state against its citizens must remain proportional to the ends pursued. The interplay between the Ministry of Justice, the national data protection officer, the association of internet service providers (Eco), and the internet community effectively hold the bodies involved accountable.

Court proceedings are generally public. While a comprehensive list of all content blocking or deletion orders is not available, the media generally covers such measures. One important exception in reporting concerns the indexes of internet services of the KJM and the Federal Review Board for Media Harmful to Young People (BpJM), which are kept secret.[74]

There is no systematic self-censorship in the German press; however, certain incidents signal that press companies are becoming more risk-averse when making decisions on the content they intend to publish through private app stores.[75] Furthermore, there are more or less unspoken rules reflected in the publishing principles of the German press.[76] The penalty code and the JMStV prohibit content in a well-defined manner (such as child pornography, racial hatred, and the

---

Huffington Post (blog), June 8, 2010, http://www.huffingtonpost.com/christopher-burgess/three-good-reasons-to-loc_b_599945.html.

[71] Cf. Resolution of Bundesrat of October 12, 2012, TOP 12,
[71]http://www.bundesrat.de/cln_236/nn_6898/DE/parlamentsmaterial/to-plenum/901-sitzung/to-node.html?__nnn=true) and the debate in the German Bundestag, "Plenarprotokoll 17/201. Stenografischer Bericht. 201. Sitzung Berlin", [Minutes of the pleneray meeting] October 25, 2012, http://dip21.bundestag.de/dip21/btp/17/17201.pdf.

[72] beck-aktuell, "LG Augsburg: Durchsuchung einer Redaktion rechtswidrig" [Regional Court Augsburg: Permission to search the editorial office illegal], May 20, 2013, http://beck-aktuell.beck.de/news/lg-augsburg-durchsuchung-einer-redaktion-rechtswidrig.

[73] Deutsche Wirtschafts Nachrichten, "Drohung mit Beugehaft wirkt: Online-Portal gibt Nutzer-Daten preis" [Threat of coercive detention works: online portal discloses user data], May 6, 2013, http://deutsche-wirtschafts-nachrichten.de/2013/05/06/drohung-mit-beugehaft-wirkt-online-portal-gibt-nutzer-daten-preis/.

[74] The so called parts C and D of the index are not public. BpJM, „Liste der Bundesprüfstelle" [Index of the Federal Review Board for Media Harmful to Young People], http://www.bundespruefstelle.de/bpjm/Jugendmedienschutz/Indizierungsverfahren/verfahrensarten,did=32964.html; See also for in overview in English http://www.bundespruefstelle.de/bpjm/information-in-english.html.

[75] In order to avoid later complaints a news magazine was prompted to change the issue cover in the way it deemed to be in line with Apple's terms concerning nudity ; Cf. heise.de, "E-Kiosk-Betreiber Zinio verlangt Zensur auf Android- und iOS-Geräten" [E-kiosk operator Zinio demands censorship on Android and iOS-devices], May 6, 2012, http://www.heise.de/mobil/meldung/E-Kiosk-Betreiber-Zinio-verlangt-Zensur-auf-Android-und-iOS-Geraeten-1568938.html

[76] Presserat [Press Council], "Pressekodex" [press code], version dated March 13, 2013, http://www.presserat.info/inhalt/der-pressekodex/pressekodex.html.

glorification of violence). The JMStV also regulates adult content that is potentially harmful to minors, stipulating that content inappropriate for certain age groups must be regulated to prevent access by children or young persons.

While the degree to which political actors can successfully pressure online news outlets to exclude certain information from their reporting is still insignificant, there have at least been attempts to delete critical information on the internet. The German Bundestag asked a blog to delete an expert report on corruption among parliamentarians because of an alleged copyright infringement. The platform owner refused to do so without further consequences.[77] Additionally, the Federal Ministry of Defense has taken legal steps against a newspaper,[78] demanding that it delete a set of leaked mission reports covering Afghanistan operations of the federal armed forces *(Bundeswehr)*, based on alleged copyright infringement.[79]

With the latest amendment of the telecommunications act (*Telekommunikationsgesetz*, TKG) enacted in May 2012, the principle of net neutrality has been legally codified (§ 41a TKG), but is still not entirely safeguarded.[80] The law authorizes the government to define basic requirements for non-discriminatory data transfer and content access, but it does not require the government to take any further action. The German Federal Network Agency (Bundesnetzagentur, BNetzA) principally supports net neutrality, but instead of safeguarding it legally, the national regulator favors new business models based on price discrimination and differentiated classes of service as long as ISPs are transparent about their policies and give customers a choice.[81] The lack of concrete action on the part of the German government has also encountered criticism, especially when two of the market-leading telecommunications companies, Vodafone and Deutsche Telekom, announced new terms for customer contracts. Telekom, for example, announced that it would place limits on customers' high-speed data transfer per month, but that its own services, such as television and movie-streaming services, would not count toward customers' data transfer limits.[82] Treating in-house services differently in particular has raised concerns in terms of competition and consumer protection by governmental representatives who also declared that these practices should be scrutinized more closely.[83]

---

[77] Markus Beckedahl, "Der Deutsche Bundestag fordert uns auf, das bisher geheim gehaltene Gutachten zur Abgeordnetenkorruption zu depublizieren" [The German Bundestag calls on us to take down a yet secret report on MPs corruption], October 17, 2012, https://netzpolitik.org/2012/der-deutsche-bundestag-fordert-uns-auf-das-bisher-geheim-gehaltene-gutachten-zur-abgeordnetenkorruption-zu-depublizieren/

[78] David Schraven, "Verteidigungsministerium geht juristisch gegen die WAZ vor" [Ministry of Defense taking legal steps against the WAZ], DerWesten Rechercheblog, April 8, 2013, http://www.derwesten-recherche.org/2013/04/verteidigungsministerium-geht-juristisch-gegen-waz-vor/.

[79] David Schraven/WAZ, Die Afghanistan Papiere [The Afghanistan wires], accessed April 10, 2013, http://afghanistan.derwesten-recherche.org/.

[80] In particular: § 41a TKG, http://dejure.org/gesetze/TKG/41a.html. The clause simply authorizes the government to define basic requirements for non-discriminatory data transfer and content access, and leaves it to the Bundesnetzagentur to determine minimum quality of service standards -- a path the regulator is not likely to go.

[81] Cf. minutes of the Expert Meeting on net neutrality of the Parliamentary Inquiry Commission, October 8, 2010, http://bit.ly/1dOvaQl.

[82] Rolf Wenkel, "Telekom's planned data limit meets with protest," Deutsche Welle, April 25, 2013, http://www.dw.de/telekoms-planned-data-limit-meets-with-protest/a-16773016.

[83] Annett Meiritz/Severin Weiland, "Flat-Rate Fiasco: Telekom Plan to Limit DSL Worries Berlin", http://www.spiegel.de/international/business/government-wary-of-telekom-limits-on-flat-rate-dsl-access-a-896435.html.

Germany is home to a vibrant internet community and blogosphere. Local and international media outlets and news sources are generally accessible and represent a diverse range of opinions.[84] Policies affecting internet regulation, data protection, or surveillance enjoy increasing public attention and media coverage. Internet-related topics are growing increasingly popular, also due to increased attention among political institutions. All political parties now have internet experts. Whereas in early 2012 the German Pirate Party could continue its remarkable success in state elections,[85] their popularity has recently been decreasing.[86] After three years of work, the multi-stakeholder Commission of Inquiry (Enquete-Kommission) on Internet and Digital Society[87] released its final report in April 2013.[88] Among other things, the commission calls for the establishment of a permanent internet commissioner at the federal level.[89]

In 2012, an example of the growing discursive power of the internet community revolved around a discussion which started on Twitter. Under the hashtag #aufschrei ("outcry"), people started to tweet about everyday sexism against women. The discussion soon left the Twitter-sphere and became a nation-wide societal debate.[90] Additionally, activists are waging online campaigns in the fight for net neutrality[91] against the telecoms Vodafone[92] and Deutsche Telekom, and have already been partly successful.[93] At the same time, multiple laws that restrict internet freedom, such as some of the amendments to the telecommunication act, were passed despite strong criticisms by a broad coalition of societal actors.

VIOLATIONS OF USER RIGHTS

Germany is considered to be one of the most privacy-conscious countries; however, the 2012 amendments to the telecommunication act included a provision which allows more public agencies access to user data, and lowers the threshold for this access from investigations into serious crimes to misdemeanors and administrative offences, raising concerns about the trajectory for privacy protections in the country.

[84] Bundesinnenministerium [Federal Ministry of the Interior], "Die nationalen Minderheiten in Deutschland" [National minorities in Germany], January 30, 2013, http://bit.ly/13cNnE7.
[85] Voter turnout of the Pirate Party in Berlin: 8.9 percent, Saarland: 7.4 percent, Schleswig-Holstein: 8.2 percent, Nordrhein-Westfalen: 7.8 percent
[86] Daniel Leisegang, "Piraten auf Schlingerkurs" [Pirates are on slalom course], Blätter 11/2012, p. 11-14, http://www.blaetter.de/archiv/jahrgaenge/2012/november/piraten-auf-schlingerkurs.
[87] Cf. the website of the Enquete-Kommission [Parliamentary Inquiry Commission]: http://www.bundestag.de/internetenquete/.
[88] Final report of the Parliamentary Inquiry Commission "Internet und digitale Gesellschaft" [The Internet and digital society]: Deutscher Bundestag, Drucksache17/ 12550, April 5, 2013, http://dipbt.bundestag.de/dip21/btd/17/125/1712550.pdf.
[89] Der Spiegel, "Net Politics: Report Calls for German Internet Commissioner", April 19, 2013, http://ml.spiegel.de/article.do?id=895412.
[90] Silke Wünsch, "Anti-sexism Twitter campaign gains momentum", January 26, 2013, http://dw.de/p/17S9K.
[91] Cf. campaign website: http://echtesnetz.de/.
[92] Cf. campaign website: http://halbesnetz.de/.
[93] The Federation of German Consumer Organizations (vzbv), a non-governmental organization for consumer protection, admonished both companies for disseminating misleading information in their terms and inadmissible contracts. Cf. http://www.vzbv.de/10432.htm ; http://bit.ly/16LO8Xh

The German Basic Law guarantees freedom of expression and freedom of the media (Article 5) as well as the privacy of letters, posts, and telecommunications (Article 10). These articles generally safeguard offline as well as online communication. In addition, a groundbreaking 2008 ruling by the Federal Constitutional Court established a new fundamental right warranting the "confidentiality and integrity of information technology systems" grounded in the general right of personality guaranteed by Article 2 of the Basic Law.[94]

These rights were contested in the political aftermath of the September 2001 terrorist attacks in the United States (cf. the 2001 Act for Limiting the Secrecy of Letters, the Post, and Telecommunications).[95] However, after several cases concerning the infringement of the rights of journalists, a Federal Constitutional Court ruling in February 2007 set a strong precedent for the protection of journalists' sources.[96] On March 29, 2012, in response to this ruling, the Federal Parliament issued the Act on Strengthening Press Freedom (*Gesetzes zur Stärkung der Pressefreiheit im Straf- und Strafprozessrecht*, PrStG), which protects journalistic sources and establishes high barriers for searching and seizing journalists' property.[97] In addition to the aforementioned rulings on the liability privilege of providers, these developments constitute a trend of strengthening media freedom in Germany. In particular, the rulings of the Federal Constitutional Court continue to promote freedom of expression.

Online journalists are generally granted the same rights and protections as journalists in the print or broadcast media. Although the functional boundary between journalists and bloggers is starting to blur, the German Federation of Journalists maintains professional boundaries by issuing press cards only to full-time journalists. Similarly, the German Code of Criminal Procedure grants the right to refuse testimony solely to individuals who have "professionally" participated in the production or dissemination of journalistic materials.[98]

The German Criminal Code (StGB) includes a paragraph on "incitement to hatred" (§ 130 StGB), which penalizes calls for violent measures against minority groups and assaults on human dignity.[99]

---

[94] BVerfG [Federal Constitutional Court], Provisions in the North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) on online searches and on the reconnaissance of the internet null and void, judgment of February 27, 2008, 1 BvR 370/07 Absatz-Nr. (1 - 267), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html; See also, Press release no. 22/2008, http://www.bundesverfassungsgericht.de/en/press/bvg08-022en.html. For more background cf. Wiebke Abel/Burkhard Schaferr, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG", NJW 2008, 822", 2009, 6:1 SCRIPTed 106, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp.

[95] This Act enables secret services to intercept, monitor, and record private communications, including the surveillance of journalists under specific conditions. It also restricts journalistic privileges such as the right to refuse to give evidence. "Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses" [Law on the restriction of correspondence, posts and telecommunications secrecy], http://www.gesetze-im-internet.de/g10_2001/index.html.

[96] BVerfG [Federal Constitutional Court], "Cicero-Urteil," judgment of February 27, 2007, 1 BvR 538/06, Absatz-Nr. (1 - 82), http://www.bverfg.de/entscheidungen/rs20070227_1bvr053806.html ; For the European context, see David Banisar, "Speaking of Terror: A Survey of the Effects of Counter-terrorism Legislation on Freedom of the Media in Europe", Council of Europe, 2008, http://www.coe.int/t/dghl/standardsetting/media/Doc/SpeakingOfTerror_en.pdf.

[97] Cf. the press release of the Federal Ministry of Justice, March 30, 2012: http://bit.ly/1bhKUOP.

[98] Code of Criminal Procedure (StPO), § 53 (1) 5, http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0198.

[99] Cf. fn. 54.

The German people mostly regard this provision as legitimate, particularly because it is generally applied in the context of holocaust denials.[100]

Website owners or bloggers are not required to register with the government. However, due to clauses in both the Telemedia Act (*Telemediengesetz*, TMG) and the Interstate Treaty on Broadcasting (*Rundfunkstaatsvertrag*, RFStV), most websites and blogs need to have an imprint naming the person in charge and contact address. The anonymous use of e-mail services, online platforms, wireless internet access points, and public telephone booths are legal. Although the Federal Minister of the Interior and some other members of the conservative parties have repeatedly expressed their disapproval of anonymity on the internet,[101] this situation is not likely to change. With explicit references to the constitution, several courts have repeatedly affirmed the right to anonymity and its necessity for the exercise of the constitutional right to freedom of expression.[102]

The right of anonymity notwithstanding, the telecommunication act of 2004 stipulates that the purchase of SIM cards requires registration, including the purchaser's full name, address, international mobile subscriber identity (IMSI), and international mobile station equipment identity (IMEI) numbers if applicable.[103] In this way, the growing penetration of mobile internet threatens to further erode the possibility of anonymous communication.

The use of proxy servers is common in Germany, but more for the purpose of circumventing copyright restrictions than to avoid censorship. There are no figures available for the extent of their use.

Excessive interceptions by secret services formed the basis of a 2008 Federal Constitutional Court ruling, which established a new fundamental right warranting the "confidentiality and integrity of information technology systems." The court held that preventive covert online searches are only permitted "if factual indications exist of a concrete danger" that threatens "the life, limb, and freedom of the individual" or "the basis or continued existence of the state or the basis of human existence." The court also established that any covert infiltration of information technology systems requires a court order and that statutes permitting such infiltrations must "contain precautions in order to protect the core area of private life."[104] Based on this Constitutional Court ruling, the

[100] BVerfG, [Federal Constitutional Court] 1 BvR 2150/08 from November 4, 2009, Absatz-Nr. (1 - 110), http://www.bverfg.de/entscheidungen/rs20091104_1bvr215008.html ; See also the Press release no. 129/2009 of 17 November 2009, Order of 4 November 2009 – 1 BvR 2150/08 – § 130.4 of the Criminal Code is compatible with Article 5.1 and 5.2 of the Basic Law, http://www.bverfg.de/pressemitteilungen/bvg09-129en.html .

[101] Cf. Anna Sauerbrey, "Innenminister Friedrich will Blogger-Anonymität aufheben" [Federal Minister of Interior wants to abolish anonymity of bloggers], Tagesspiel online, August 7, 2011, http://www.tagesspiegel.de/politik/internet-innenminister-friedrich-will-blogger-anonymitaet-aufheben/4473060.html.

[102] E.g. Oberlandesgericht (OLG) Hamm [German Federal Court of Appeals Hamm], File I-3 U 196/10, August 3, 2011, http://www.justiz.nrw.de/nrwe/olgs/hamm/j2011/I_3_U_196_10beschluss20110803.html.

[103] Telecommunications Act (TKG), § 111, http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/TelecommunicationsAct-TKG.pdf?__blob=publicationFile.

[104] Bundesverfassungsgericht [Federal Constitutional Court], Provisions in the North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) on online searches and on the reconnaissance of the Internet null and void, judgment of February 27, 2008, 1 BvR 370/07; For more background cf. W Abel and B Schafer, "The German Constitutional

Federal Parliament passed an act in 2009 authorizing the Federal Bureau of Criminal Investigation (BKA) to conduct covert online searches to prevent terrorist attacks on the basis of a warrant.[105] In addition to online searches, the act authorizes the BKA to employ methods of covert data collection, including dragnet investigations, surveillance of private residences, and the installation of a program on a suspect's computer that intercepts communications at their source.

The amended telecommunication act of 2013 reregulates the "stored data inquiry" requirements (*Bestandsdatenauskunft*).[106] Under the new provision, approximately 250 registered public agencies, among them the police and customs authorities, are authorized to request from ISPs both contractual user data and sensitive data, such as PINs, passwords, and dynamic IP addresses. While the 2004 law restricted the disclosure of sensitive user data to criminal offenses, the amended act extends it to cases of misdemeanors or administrative offenses. Additionally, whereas the disclosure of sensitive data and dynamic IP addresses normally requires an order by the competent court, contractual user data (such as the user's name, address, telephone number, and date of birth) can be obtained through automated processes. The requirement of judicial review (*Richtervorbehalt*) has been subject to two empirical studies, both of which found that in the majority of cases a review by a judge does not take place.[107] Data protection experts criticize the lower threshold for intrusions of citizens' privacy as disproportionate. Two members of the Pirate Party and a lawyer who had already filed the complaint against the data retention law in 2007 have filed a new constitutional complaint against the telecommunication act.[108]

Telecommunications interception by state authorities for reasons of criminal prosecution is regulated by the code of criminal procedure (StPO) and is understood as a serious interference with basic rights. It may only be employed for the prosecution of serious crimes for which specific evidence exists and when other, less-intrusive investigative methods are likely to fail. According to recent statistics published by the Federal Office of Justice, there were a total of 21,118 orders for telecommunications interceptions in 2011, of which 1,345 concerned internet communications.[109] This is an increase of about 35 percent compared to 2010. There were also a

---

Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG", NJW 2008, 822, (2009) 6:1 SCRIPTed 106, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp.

[105] Dirk Heckmann, "Anmerkungen zur Novellierung des BKA-Gesetzes: Sicherheit braucht (valide) Informationen" [Comments on the amendment of the BKA act: Security needs valid information], Internationales Magazin für Sicherheit nr. 1, 2009, www.ims-magazin.de/index.php?p=artikel&id=1255446180,1,gastautor.

[106] Bundesrat, "Mehr Rechtssicherheit bei Bestandsdatenauskunft" [More legal certainty for stored data inquiry], Press release no. 251/2013, May 3, 2013, http://www.bundesrat.de/DE/presse/pm/2013/094-2013.html.

[107] Two independent studies from by the Universität of Bielefeld (2003: Wer kontrolliert die Telefonüberwachung? Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung" [Who controls telecommunication surveillance? An empirical investigation on judicial overview of telecommunication surveillance], edited by Otto Backes and Christoph Gusy, 2003) and Max-Planck-Institut Institute for Foreign and International Criminal Law (Hans-Jörg Albrecht, Claudia Dorsch, Christiane Krüpe 2003: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen [Legal reality and efficiency of wiretapping, surveillance and other covert investigation measures], http://bit.ly/wDVLS5) evaluated the implementation of judicial oversight of telecommunication surveillance. Both studies found that neither the mandatory judicial oversight nor the duty of notification of affected citizens are carried out. According to the study by the Max Planck Institute, only 0,4 % of the requests for court orders were denied.

[108] Breyer, Patrick, "Verfassungsbeschwerde gegen Bestandsdatenauskunft eingereicht" [Constitutional complaint against stored data inquiry submitted], July 1, 2013, http://bestandsdatenauskunft.de/?p=357.

[109] Bundesamt für Justiz [Federal Office of Justice], "Übersicht Telekommunikationsüberwachung (Maßnahmen nach §100a StPO) für 2011," July 23, 2012 [Summary of telecommunication surveillance for 2011] http://bit.ly/18aJxwx.

total of 14,153 orders requesting internet traffic data in 2011.[110] Surveillance measures conducted by the secret services under the Act for Limiting the Secrecy of Letters, the Post, and Telecommunications exceed these figures. For 2011, the competent Parliamentary Control Panel reported that a total of 2.8 million telecommunications – most of them e-mail – were scanned, of which only 290 were considered relevant. [111] The e-mail contents were scanned for keywords relating to certain "areas of risk," namely international terrorism, proliferation of arms and other military technology, and human smuggling.[112]

For purposes of criminal prosecution, since 2009, the German police have used Trojan-like pieces of software to spy on criminal suspects. The Trojan, programmed by the commercial manufacturer DigiTask, not only enables the police to legally eavesdrop on encrypted conversations but also has the potential for a wider range of actions, some of which are illegal. Among these illegal encroachments are the searching of digital devices, logging of keystrokes, and planting of "backdoors" that allow for the remote installation of additional software or insertion of false evidence. Five German states admitted to the use of the "Federal Trojan" (*Bundestrojaner*) but denied the use of any illegal functions.[113] Due to the considerable public criticism following the "Bundestrojaner affair," the Federal Police decided to develop in-house capacity to produce its own lawful intrusion software. More controversially, the Federal Police have purchased FinFisher/FinSpy IT, another commercial spyware, for the "transition period" until its own solution is operational.[114]

Recent evidence shows that German police authorities regularly make use of radio cell queries for criminal investigation.[115] In the states of Berlin and Saxony, for example, radio cell queries were used in 2012 in the context of criminal investigations for which millions of data records were

[110] Bundesamt für Justiz, "Übersicht Verkehrsdatenerhebung (Maßnahmen nach § 100g StPO) für 2011" [Summary of traffic data collection], July 23, 2012, http://bit.ly/179zDvJ.

[111] These are aggregated figures related to the three areas of risk in which scannings took place according to the report of the Parliamentary Control Panel. Cf. Deutscher Bundestag, Drucksache 17/12773, March 14, 2013, p.7, http://dip21.bundestag.de/dip21/btd/17/127/1712773.pdf. Please note that the annually presented numbers do not refer to the last year but to the year before, i.e. 2011. The Parliamentary Control Panel periodically reports to the parliament and nominates the members of the G10 Commission. The G10 Commission controls surveillance measures and is also responsible for overseeing telecommunications measures undertaken on the basis of the Counterterrorism Act of 2002 and the Amendment Act of 2007. See also: http://www.bundestag.de/htdocs_e/bundestag/committees/bodies/scrutiny/index.html.

[112] Cf. the report of the Parliamentary Control Panel: Deutscher Bundestag, Drucksache 17/12773, March 14, 2013, p. 6, http://dip21.bundestag.de/dip21/btd/17/127/1712773.pdf.

[113] Deutsche Welle, "Several German states admit to use of controversial spy software," October 11, 2011, http://www.dw.de/dw/article/0,,15449054,00.html.

[114] Meister, Andre, "Secret Government Document Reveals: German Federal Police Plans To Use Gamma FinFisher Spyware", netzpolitik.org, January 16, 2013, http://bit.ly/10zhgPA; For the classified document see: "Bericht zur Nr. 10 des Beschlusses des Haushaltsausschusses des Deutschen Bundestages zu TOP 20 der 74. Sitzung am 10. November 2011" [Report of Article 10 of the decision of the Parliament's Budget Committee], https://netzpolitik.org/wp-upload/BMI-Bericht-Sachstand-CC-TK%C3%9C.pdf; EDRI, "Details on German State Trojan programme", October 24, 2012, http://www.edri.org/edrigram/number10.20/details-german--state-spyware-Staatstrojaner.

[115] Berlin Commissioner for Data Protection and Freedom of Information, Alexander Dix: "Abschlussbericht zur rechtlichen Überprüfung von Funkzellenabfragen [Report on the legal examination of radio cell queries], p. 16, http://www.datenschutz-berlin.de/attachments/896/Pr__fbericht.pdf?1346753690 . Data are currently available for the states of Berlin and Saxony. In both states radio cell queries were used in 2012 for hundreds of lawsuits for which millions of data records were collected.

collected without informing the individuals affected, as required by law.[116] The extensive use of radio cell queries has raised questions of proportionality.[117]

A constitutional complaint filed by ISPs in 2012 successfully challenged the existing provisions that mandated ISPs to retain customer data and provide information on users' contractual data, PIN numbers, keys, and passwords to law enforcement agencies and secret services upon request.[118] The Federal Constitutional Court held that these provisions breach the individual right of self-determination over personal information of the Basic Law. The Federal Constitutional Court particularly criticized as partly unconstitutional the duty of telecommunications providers to provide information about passwords and other access protection measures.[119]

Following the EU Data Retention Directive, the 2007 Law on the Revision of Telecommunications Monitoring and other Covert Investigation Measures and on the Implementation of Directive 2006/24/EC mandated that ISPs and mobile phone companies have to retain traffic data for six to seven months to facilitate criminal investigations. A constitutional complaint led to the repeal of the national data retention provisions in 2010.[120] The German government has not transposed the EU Data Retention Directive within the stipulated timeframe into German law and does not intend to do so.[121] On May 31, 2012, the European Commission filed a complaint against the German government due to non-compliance, proposing that the court impose a daily penalty payment of € 315,036.54.[122]

A 2012 survey by the German Federal Network Agency shows that, in the absence of a legal obligation for data retention, the four major mobile communications providers in Germany continue to store user data for a period of between 7 and 210 days.[123]

---

[116] E.g. in Berlin, in the first half of 2012, 128 lawsuits with radio cell queries and 200 realized queries. In 302 analysed cases (2009-04/2012) more than 6,619,155 data sets have been recorded, shown in this handout of the Berlin Chamber of Deputies, "Ergebnisse der polizeilichen Auswertung -Funkzellenabfragen-" [Results of the police investigation on radio cell queries], https://www.piratenfraktion-berlin.de/wp-content/uploads/2012/08/0480_001.pdf. Cf. also Andre Meister, "Funkzellenabfrage geht weiter: Jeder Berliner ist jedes Jahr zwei Mal verdächtig" [Radio cell queries continue: Each citizen of Berlin is suspected twice a year], August 28, 2012, https://netzpolitik.org/2012/funkzellenabfrage-geht-weiter-jeder-berliner-ist-jedes-jahr-zwei-mal-verdachtig/ ; In Saxony 60 cases have been reported from January to September 2012: Saxon Parliament, Drs 5/10379, http://ws.landtag.sachsen.de/images/5_Drs_10379_-1_1_4_.pdf.

[117] Berlin Commissioner for Data Protection and Freedom of Information, 2012, see footnote 35, p. 17 ; Landgericht Dresden [District Court of Dresden] Az. 15 Qs 34/12, http://bit.ly/15RxTaL.

[118] Dokumentations- und Informationssystem für Parlamentarische Vorgänge, "Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft" [Act to amend the Telecommunications Act and the revision of the existing stored data inquiry], ID: 17-48610, http://dipbt.bundestag.de/extrakt/ba/WP17/486/48610.html.

[119] Bundesverfassungsgericht [Federal Constitutional Court], judgment of January 24, 2012, 1 BvR 1299/05, Absatz-Nr. (1 - 192), http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html

[120] BVerfG, judgment of March 2, 2010, 1 BvR 256/08, Absatz-Nr. (1 - 345), http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

[121] Nikolas Busse, "Jeden Tag 315.036,54 Euro Strafe" [For each day a fine of Euro 315,036.54], FAZ.net, May 31, 2012, http://www.faz.net/-gpg-709kp.

[122] European Commission, "Data retention: Commission takes Germany to Court requesting that fines be imposed", Press release IP/12/530, May 31, 2012, http://europa.eu/rapid/press-release_IP-12-530_en.htm.

[123] Speicherdauer" [duration of storage], http://wiki.vorratsdatenspeicherung.de/images/BNetzA_Speicherdauer.pdf

German authorities also request user data from internet content providers. From July–December 2012, Google reported an increasing number of requests (1,550 compared to 1,426 requests for the same period in 2011), putting Germany at number four on the list of the countries that request the most user data, behind the United States, India, and France.[124] Microsoft reported 8,419 requests, affecting 13,226 accounts. In 7,088 of these cases (84.2 percent), at least "some customer data" was disclosed. Skype data has been listed separately: in 2012, there were 686 requests, affecting 2,646 accounts.[125]

There are no legal obligations to report security breaches. However, according to the Federal Ministry of Interior, approximately 1,100 cyberattacks took place in 2012. As a response to these estimates, the ministry has developed a "Cyber Security Strategy for Germany," thereby following the global trend to improve the security of information networks in a proactive manner.[126] On June 16, 2011, Germany´s Interior Minister Hans-Peter Friedrich introduced the new National Cyber Response Centre tasked to optimize the cooperation between several federal authorities and agencies such as the Federal Office for Information Security (BSI) and the Federal Office for the Protection of the Constitution (BfV). The Cyber Response Centre is a sub-unit of the Ministry of Interior with 10 permanent employees.[127] In addition, a National Cyber Security Council was founded in 2011. It consists of government officials and associated business representatives who meet at least three times a year. Academic experts can be invited if required.[128] In March 2013, the Federal Ministry of the Interior proposed a law to improve the security of information networks which would have made it a mandatory obligation for telecommunication firms and critical infrastructure operators to report security breaches to the Federal Office for Information Security (BSI).[129] The Federal Ministry of Economics and Technology blocked the legislative draft in the early consultation phase. Digital rights advocates criticized the legislative proposal because it did not include a notification of users in case of security breaches. Industry associations, on the other hand, feared potential costs and bureaucratic burdens of notifying the Federal Office for Information Security.[130]

---

[124] Google, "Google Transparency Report. User Data Requests. Germany. July to December 2012", 2013, http://www.google.com/transparencyreport/userdatarequests/DE/?hl=en_US.

[125] Microsoft, "2012 Law Enforcement Requests Report", http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/.

[126] *"German firms see rising Chinese cyberattacks," February 24, 2013, http://www.thelocal.de/sci-tech/20130224-48165.html. Cf. also Federal Ministry of the Interior, "Cyber Security Strategy for Germany," Edition February 2011, p.8, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile.*

[127] Federal Ministry of the Interior, "Bundesinnenminister Dr. Hans-Peter Friedrich eröffnet das Nationale Cyber-Abwehrzentrum" [Germany´s Interior Minister Hans-Peter Friedrich introduced the new national National Cyber Response Centre], Press Release, June 16, 2013. Cf. also Federal Ministry of the Interior, "Cyber Security Strategy for Germany", Edition February 2011, p.9, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile.

[128] Christian Tretbar, "Friedrich: Speichern von Daten dient einem 'edlen Zweck'" [Friedrich: Data storage provides for a good cause], July 14, 2013, http://bit.ly/143AqhH.

[129] Cf. Federal Ministry of the Interior, "Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme" [Draft legislative proposal for improving the security of information networks], March 5, 2013, http://bit.ly/XsVWs1.

[130] Cf. Andre Meister, " IT-Sicherheitsgesetz vor dem Aus: Wirtschaft verhindert Meldepflicht über Sicherheitsvorfälle" [Cyber security law on the brink: Industry blocks reporting obligation for security breaches], June 5, 2013, https://netzpolitik.org/2013/it-sicherheitsgesetz-vor-dem-aus-wirtschaft-verhindert-meldepflicht-uber-sicherheitsvorfalle/.

In June 2012, the media reported the establishment of a new cyberwarfare unit within the German military forces (*Bundeswehr*). However, the unit is said to be poorly staffed compared to its international allies.[131]

[131] The Economic Times, "Germany prepares special unit to tackle cyberattack," June 6, 2012, http://articles.economictimes.indiatimes.com/2012-06-06/news/32079025_1_cyber-warfare-cyber-attack-special-cyber. Cf. also Kuhn Johannes, "Deutschlands Hackertruppe übt noch" [Germany´s hacking unit still practices], June 5, 2012, http://www.sueddeutsche.de/digital/bundeswehr-im-cyberwar-deutschlands-hackertruppe-uebt-noch-1.1374819.

HUNGARY

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	5	5
Limits on Content (0-35)	6	8
Violations of User Rights (0-40)	8	10
Total (0-100)	19	23

* 0=most free, 100=least free

POPULATION: 9.9 million
INTERNET PENETRATION 2012: 72 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Revisions to the criminal code, passed on June 25, 2012 and scheduled to take effect in July 2013, could allow the government to block websites if host providers fail to respond to takedown notices (see **LIMITS ON CONTENT**).
- The Supreme Court fined two blog owners for defamation based on readers' comments, even though the comments were deleted (see **VIOLATIONS OF USER RIGHTS**).
- The fourth modification of the constitution annulled previous decisions of the Constitutional Court, causing uncertainty as to how previous legal protections, particularly regarding free speech, will be interpreted (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

When Hungary transitioned from a one-party state to a parliamentary democracy in 1989–1990, very few people were using the internet in the country. In the following years, dial-up connections spread and the number of users expanded, particularly in the 2000s when the price of internet started to decrease while the availability of broadband connections increased. Today, a majority of the population is online. Information and communication technologies (ICTs) are being used not only for social activities and newsgathering, but also increasingly for political activism.

In the 2010 parliamentary elections, the conservative Hungarian Civic Union (Fidesz) and its ally, the Christian Democratic People's Party (KDNP), won a 53 percent majority,[1] granting them more than two-thirds of the seats in parliament and enabling them to draft and accept a series of laws without meaningful political or public consultation.[2] The new laws regulating the media, including online media outlets and news portals, are of particular concern.[3] A new regulatory authority, the National Media and Infocommunications Authority (NMHH) and its decision-making body, the Media Council, were also established to oversee the mass communications industry, with the power to penalize or suspend outlets that violate stipulations of the media regulations. In April 2011, the national assembly adopted a new constitution, the Fundamental Law of Hungary, which includes a provision concerning the supervision of the mass communications industry and the media as a whole. The parliament also created the National Agency for Data Protection, whose independence has been called into question due to the political appointment process of the agency's leadership.

Immediately after the 2010 media laws were passed, Hungary came under fierce criticism from the international community, as the laws were deemed incompatible with the values of the European Union. Despite the modifications to the media laws in May 2012 based on the ruling of the Hungarian Constitutional Court in December 2011, members of the Organization for Security and Co-operation in Europe (OSCE) and the Council of Europe have argued that the laws remain unsatisfactory, and that unclear provisions and the significant power given to the NMHH continue to threaten media freedom.[4] In particular, high fines can be imposed on all types of media outlets by the one-party Media Council based on an obscure content provision. In January 2013, the Council of Europe welcomed the results of the dialogue with the Hungarian government about media regulation,[5] while domestic nongovernmental organizations (NGOs) expressed their continued concerns to the Secretary General of the Council of Europe.[6]

---

[1] Toplist, Parliamentary Election of 2010, April 25, 2010, National Election Office, http://bit.ly/1bhDO9u.
[2] For more details about the overhaul of the legislature, see "Democracy and Human Rights at Stake in Hungary. The Viktor Orbán Government's drive for centralisation of power," Norwegian Helsinki Committee, 2013, http://bit.ly/WrcX3T, and in general, what has been happening in Hungary since the 2010 parliamentary elections see Kim Lane Scheppele's Testimony at the Helsinki Commission Hearing on Hungary, March 19, 2013, http://bit.ly/Y1Cu8c.
[3] Act CIV of 2010 on the freedom of the press and the fundamental rules on media content, http://bit.ly/1hbKJBW; Act CLXXXV of 2010 on media services and on the mass media, http://bit.ly/197GmZJ.
[4] "Revised Hungarian media legislation continues to severely limit media pluralism, says OSCE media freedom representative," Organization for Security and Cooperation in Europe, May 25, 2012, http://www.osce.org/fom/90823.
[5] "Secretary General welcomes changes to Hungarian laws on media and judiciary," Council of Europe, January 29, 2013, http://bit.ly/WuGSZY.
[6] "Letter of Hungarian NGOs on Media Legislation to Mr. Thorbjørn Jagland, Secretary General, Council of Europe," Standards Media Monitor, February 4, 2013, http://bit.ly/197GoRm.

OBSTACLES TO ACCESS

According to the International Telecommunication Union (ITU), internet penetration in Hungary stood at 72 percent in 2012, up from 53 percent in 2007,[7] while the National Media and Infocommunications Authority of Hungary (NMHH) reported in late 2012 that there were over two million broadband internet subscriptions in a country of ten million inhabitants.[8] NRC, a company specializing in internet market research in Hungary, puts the internet penetration at 63 percent in 2012.[9] In 2011, 50 percent of households had an internet subscription, the overwhelming majority using a broadband connection.[10] Dial-up internet service is not widely used. The ITU and NMHH also recorded a mobile phone penetration rate of 117 percent and 2.94 million mobile internet subscriptions,[11] while over 78 percent of residential areas had 3G coverage by mid-2012.[12] In 2012, only 26 percent of the population had never used the internet, a decrease from 52 percent in 2006.[13] A 2011 Eurobarometer survey found that the main reasons why Hungarian households do not have internet subscriptions were that the monthly subscription was too expensive, the cost of buying a computer and modem was too high, or that no one in the household had an interest in using the internet.[14]

There are geographical, socioeconomic, and ethnic differences in Hungary's internet penetration levels, with lower access rates found in rural areas[15] and among the Roma community, the country's largest ethnic minority.[16] An industrial expert noted that internet use is largely determined by age and education, resulting in a higher concentration of internet users in cities, since most young people leave rural areas to attend universities or get jobs in urban centers. He added that in 2012, among users between 15–24 years of age, the internet penetration was over 90 percent; similar rates were found among users having a degree.[17]

---

[7] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2007 & 2012, accessed July 25, 2013, http://bit.ly/6bZQ1.
[8] "Flash report on wireline service," National Media and Infocommunications Authority (NMHH), October 2012, http://nmhh.hu/dokumentum/154927/vezetekes_gyj_2012_okt_eng.pdf.
[9] "Internet penetrációs adatok" [Internet penetration data], 2012/II, http://nrc.hu/kutatas/internet_penetracio.
[10] Special Eurobarometer 362, "E-communications household survey"(Eurobarometer, July 2011): 49-65, http://bit.ly/nMMupu.
[11] "Flash report on mobile internet," NMHH, October 2012, http://bit.ly/1azZkFJ; Hungary's population was 9,958,000 in early 2012. See, "Population, vital statistics," Hungarian Central Statistical Office (KSH), http://bit.ly/1bj3WEr.
[12] "Flash report on mobile internet," NMHH, June 2012, http://bit.ly/1azZkFJ.
[13] "Individuals who have never used the internet. Percentage of individuals aged 16 to 74," Eurostat, accessed December 27, 2012, http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00093.
[14] Special Eurobarometer 362, "E-communications household survey" (Eurobarometer, July 2011): 56.
[15] Anna Galácz, Ithaka Kht, eds., "A digitális jövő térképe. A magyar társadalom és az internet. Jelentés a World Internet projekt 2007. évi magyarországi kutatásának eredményeiről" [The map of the digital future. The Hungarian society and the internet. Report on the results of the 2007 World Internet Project's Hungarian research], (Budapest: 2007): 20.
[16] Statistically speaking, someone who is younger, studying, working or has a degree, and living in the capital or in a city is more likely to use internet than the elderly, unemployed or pensioner, with lower educational background, living in a village. See, World Internet Project (WIP), Report on the Hungarian Research for the World Internet Project 2007 (Budapest: Ithaka, 2008): 26, http://worldinternetproject.com/_files/_Published/_oldis/Hungary_Report_2007.pdf; "Internet-riport 2011/Q3" [Internet-report 2011/Q3], Nrc.hu, 2011, http://nrc.hu/index.php?name=OE-eLibrary&file=download&keret=N&showheader=N&id=215.
[17] Imre Kurucz, "Hogyan tovább, internetpenetráció?" [What's next internet penetration?], In: *Marketingkutató* [Marketing Researcher] Nr. 3, Winter 2012, p. 24.

The National Core Curriculum for 2013 drastically decreased the number of IT classes in primary and high schools,[18] possibly maintaining and further increasing the digital divide between social groups, as children coming from poor families may not have access to computers and other digital devices in their homes. Most internet users access the internet from home, work, and school, while access at internet cafes and "telecottages" (local community centers) is less common.[19] The use of gadgets like smartphones, tablets, netbooks, and e-books to access the internet is increasing.[20] In 2012, approximately 28 percent of phones used in Hungary were smartphones.[21] Additionally, an increasing number of widely-used software and websites are available in Hungarian, and there are several Hungarian blog-hosting sites. By mid-2013, there were more than 634,000 registered ".hu" domains[22] recorded at some 150 companies.[23]

The government does not restrict bandwidth, routers, or switches,[24] and backbone connections are owned by telecommunications companies.[25] Legally, however, internet and other telecommunications services can be paused or limited in instances of unexpected attacks, for preemptive defense, or in states of emergency or national crisis.[26] The Budapest Internet eXchange (BIX) is a network system that maintains the Hungarian internet traffic between domestic internet service providers (ISPs), and is overseen by the Council of Hungarian Internet Service Providers (ISZT)[27] without any governmental interference.[28]

Nine ISPs share 88 percent of the total fixed broadband market,[29] and there are three mobile phone service providers, all privately owned by foreign companies.[30] The existence of only three mobile phone service providers (in addition to the resellers that use the networks of the three major mobile phone service providers) has created a relatively stagnant market in terms of mobile internet network expansion. In January 2012, a consortium of state-owned companies won a mobile

[18] "Digitális analfabétákat képeznek az iskolák," [Schools educate digitally illiterates], Miklós Hargitai, Nol.hu, October 22, 2012, http://nol.hu/belfold/20121022-digitalis_analfabetakat_kepeznek.
[19] World Internet Project, "Map of the Digital Future: Hungarian Society and the Internet," 2007, http://bit.ly/18eRcu0.
[20] "Már minden harmadik netezőnek van okostelefonja," [Every third netizen have a smartphone], Nrc.hu, February 2012, http://nrc.hu/hirek?page=details&oldal=1&news_id=625&parentID=644.
[21] "Christmas presents getting smarter – Smartphones are all the rage," Enet.hu, November 27, 2012, http://www.enet.hu/en/news/christmas-presents-getting-smarter-smartphones-are-all-the-rage/.
[22] "The number of domains under the .hu public domains," Council of Hungarian Internet Providers, May 1, 2013, http://www.nic.hu/English/statisztika/.
[23] "List of registrars," Official .hu domain registry, accessed April 27, 2013, http://www.domain.hu/domain/English/.
[24] Zoltán Kalmár, Council of Hungarian Internet Service Providers, email communication, January 24, 2012.
[25] "Magyarország internetes infrastruktúrája" [Hungary's internet infrastructure], Rentit.hu, January 29, 2010, http://www.rentit.hu/hu-HU/Cikk/erdekessegek/magyarorszag-internetes-infrastrukturaja.rentit.
[26] Act CXIII of 2011 on home defense, Military of Hungary, and the implementable measures under special legal order, Art. 68, par. 5.
[27] "BIX Charter," Budapest Internet Exchange (BIX), April 21, 2009, http://bix.hu/?lang=en&page=charter.
[28] Zoltán Kalmár, Council of Hungarian Internet Service Providers, email communication, January 24, 2012.
[29] Major internet service providers are: T-Home with a 34.7 percent market share, UPC 21.8 percent, and DIGI 13.6 percent. In 2012 UPC acquired RubiCom, bringing the number of major service providers from ten to nine. See "Flash report on wireline service," National Media and Infocommunications Authority (NMHH), October 2012, http://nmhh.hu/dokumentum/154927/vezetekes_gyj_2012_okt_eng.pdf.
[30] The three mobile phone companies are: T-Mobile with a 46 percent market share, Telenor 31 percent, and Vodafone 23 percent. See "Flash report on mobile phone," NMHH, http://english.nmhh.hu/dokumentum/155178/mobil_hang_jelentes_2012_november_eng.pdf, November 2012.

frequency tender;[31] however, in September 2012, the Budapest Metropolitan Court annulled the decision by the NMHH to award these frequencies to the state-owned consortium, as well as cancelling the award of additional frequencies to the other three companies in the same auction, thus delaying the spread of 3G networks.[32]

In 2012, despite earlier promises, the government decided to keep the special tax that had been levied on the telecommunication industry since 2010 in an effort to meet the nation's budget requirements.[33] The European Commission asked the government to amend these taxes, which it viewed as discriminatory toward foreign companies, and referred the case to the European Court of Justice when Hungary failed to change the taxes. The case is still pending,[34] however, the government decided to withdraw the tax regardless.[35] In mid-2012, the government introduced a tax on mobile phone calls and text messages (a maximum of $3 monthly for individual subscribers),[36] to counterbalance the withdrawal of the special tax, which also induced an infringement proceeding from the European Commission against Hungary.[37] Almost all mobile service providers have since raised their prices.[38]

The National Media and Infocommunications Authority of Hungary (NMHH) and the Media Council, established under the 2010 media laws, are responsible for overseeing and regulating the mass communications industry. The Media Council is the NMHH's decision-making body related to media outlets, and its responsibilities include allocating television and radio frequencies and penalizing violators of media regulations. The members of the Media Council are nominated and elected by the governing two-thirds parliamentary majority.[39] Previously, the president of the NMHH was also the president of the Media Council, and was appointed directly by the prime minister for a nine-year term, indicating the council's lack of independence.[40] However, after consultations with industry leaders and the Council of Europe in January 2013, the government decided to amend the media regulation so that the president of the Media Council will now be appointed by the president of the republic, based on the proposal of the prime minister, for a non-renewable nine-year term.[41]

---

[31] "State-run consortium bags biggest frequency block at auction," Bbj.hu, January 31, 2012, http://www.bbj.hu/business/update---state-run-consortium-bags-biggest-frequency-block-at-auction--_62585.
[32] "Hungarian court annuls mobile frequency tender results," September 17, 2012, Edith Balazs, Bloomberg.com, http://www.bloomberg.com/news/2012-09-17/hungarian-court-annuls-mobile-frequency-tender-results-1-.html.
[33] "EU asks Hungary for change in 'discriminatory' special taxes," Aoife White and Edith Balazs, Bloomberg.com, November 21, 2012, http://www.bloomberg.com/news/2012-11-21/eu-asks-hungary-for-change-in-discriminatory-special-taxes-1-.html.
[34] European Commission vs. Hungary, Case C-462/12, November 23, 2012.
[35] "Giró-Szász: okafogyott Brüsszel hozzánk intézett felhívása," [Giró-Szász: Brussels is appealing in vain], Hvg.hu, November 23, 2012, http://hvg.hu/gazdasag/20121123_GiroSzasz_EU.
[36] "Hungary phone tax burden may affect Magyar Telekom dividend," Andras Gergely, Bloomberg.com, May 10, 2012, http://www.bloomberg.com/news/2012-05-10/hungary-tax-may-hit-magyar-telekom-dividend-mattheisen-says-1-.html.
[37] "EU says Hungary's revamped telecom tax is illegal," Reuters.com, January 24, 2013, http://www.reuters.com/article/2013/01/24/eu-hungary-telecom-idUSL6N0ATA8J20130124.
[38] "Hol és mennyivel drágább a telefonálás a telefonadó miatt?", [Where and how more expensive phone calls are due to the phone tax?], Csaba Balogh, Hvg.hu, July 7, 2012, http://hvg.hu/Tudomany/20120707_telefonado_aremelkedesek.
[39] Act CLXXXV of 2010, Art. 124.
[40] Act CLXXXV of 2010, Art. 111, par. 3.
[41] "Elkészült a médiatörvény módosítása," [The amendment of the media regulation is ready], Imre Bednárik, Nol.hu, February 16, 2013, http://nol.hu/belfold/elkeszult_a_mediatorveny_modositasa.

Despite these modifications, some of the decisions of the Media Council have been regarded as politicized. For instance, an analysis by the Standards Media Monitor showed that during the 2011 radio frequency allocation process, preference was given to a few applicants, who received nearly half of the available frequencies.[42] Organizations such as Human Rights Watch criticized this process and highlighted it as an example of the declines in media freedom.[43] In January 2012, the NMHH accepted only one new registration application for a mobile phone frequency tender from a consortium of state-run companies, rejecting all other applicants based on "formal deficiencies,"[44] although this award was later annulled by the Budapest Metropolitan Court.

With the newly adopted Fundamental Law of Hungary, in operation since January 2012, the governing parties prematurely ended the six-year term of the well-functioning Data Protection Commissioner, replacing the former office with the National Agency for Data Protection. The head of the new agency is appointed by the prime minister for a nine-year term and can be dismissed by the president or prime minister on arbitrary grounds,[45] calling into question the independence of the agency.

LIMITS ON CONTENT

The government does not currently mandate any type of technical filtering of websites, blogs, or text messages,[46] though online content is somewhat limited as a result of self-censorship, lack of revenue for independent media outlets online, and the dominance of the state-run media outlet. The government does not place any restrictions on access to Web 2.0 applications: YouTube, Facebook, Twitter, international blog-hosting services, instant messaging, person-to-person communication, and other Web 2.0 applications are freely available. However, while there are currently no mechanisms in place for blocking online content, the revisions to the criminal code, which were passed on June 25, 2012 and are scheduled to take effect on July 1, 2013, include provisions that could force ISPs to block unlawful content.

The revisions to the criminal code stipulate that unlawful content on the internet can be made inaccessible,[47] or that ISPs can be obliged to block content in order to fight child pornography, crimes against the state, and terror attacks.[48] For example, if a host provider fails to respond to

[42] "The Media Council's tender procedures for broadcasting frequencies," Standards Media Monitor, http://www.mertek.eu/en/reports/the-media-councils-tender-procedures-for-broadcasting-frequencies-executive-summary.
[43] "Memorandum to the European Union on Media Freedom in Hungary," Human Rights Watch, February 16, 2012, http://www.hrw.org/news/2012/02/16/memorandum-european-union-media-freedom-hungary.
[44] "State-run consortium bags biggest frequency block at auction," Bbj.hu, January 31, 2012, http://www.bbj.hu/business/update---state-run-consortium-bags-biggest-frequency-block-at-auction--_62585.
[45] Act CXII of 2011 on data protection and freedom of information, Section 40, par. 1, 3; Section 45, par. 4–5, http://www.naih.hu/files/ActCXIIof2011_mod_2012_05_09.pdf.
[46] The failed Anti-Counterfeiting Trade Agreement (ACTA) would have not imposed any stricter rules related to intellectual property than the operating Hungarian laws, according to the National Board Against Counterfeiting. See, "Kérdések és válaszok a Hamisítás Elleni Kereskedelmi Megállapodásról (ACTA)" [Questions and Answers on the Anti-counterfeiting Trade Agreement (ACTA)], February 3, 2012, http://bit.ly/14Tt2EX.
[47] Act C of 2012 on the Criminal Code, Art. 77.
[48] "Abandoning safe harbours: Hungarian online freedoms at risk," European Digital Rights, November 21, 2012, http://www.edri.org/edrigram/number10.22/hungarian-online-freedoms-abandon.

take-down notices regarding illegal content, ISPs would then be required to block users' access to the site. The new code also includes plans for a non-transparent blacklist handled by the NMHH, under which ISPs could be obligated to temporarily block content even before a court ruling.[49] As the blacklist would not be public and the process by which websites are placed on the list is not transparent, there are concerns that it might trigger self-censorship among bloggers.

Anyone can launch a blog or a website to freely express his or her opinion. Nevertheless, the 2010 media laws contain several general content regulation provisions concerning online media outlets, particularly if these outlets provide services for a profit. For example, the media regulation states that print and online media outlets bear editorial responsibility if their aim is to distribute content to the public for "information, entertainment or training purposes," but that editorial responsibility "does not necessarily imply legal liability in relation to printed press materials."[50] The law fails to clarify what editorial responsibility entails and whether it would imply legal liability for online publications. A member of the Media Council claimed that this provision could apply to a blog if the blog were produced for a living.[51]

Intermediaries are not legally responsible for transmitted content if they did not initiate or select the receiver of the transmission, or select or modify the transmitted information.[52] Intermediaries are also not obliged to verify the content they transmit, store, or make available, nor do they need to search for unlawful activity.[53]

The 2010 media laws stipulate that media content—both online and offline—may not offend, discriminate or "incite hatred against persons, nations, communities, national, ethnic, linguistic and other minorities or any majority as well as any church or religious groups."[54] Further, the law states that constitutional order and human rights must be respected, and public morals cannot be violated.[55] However, the law does not define the meaning of "any majority" or "public morals." If a media outlet does not comply with the law, the Media Council may oblige it to "discontinue its unlawful conduct," publish a notice of the resolution on its front page, and/or pay a fine of up to HUF 25 million (approximately $111,000).[56] If a site repeatedly violates the stipulations of the media regulation, ISPs can be obliged to suspend the site's given domain, and as a last resort, the media authority can delete the site from the administrative registry.[57] Any such action can be appealed in court, although the overhaul of the judiciary calls into question the independence of the court system.

[49] "Internetcenzúrává alakulhat a pedofilok elleni harc," [Fight against pedophiles can turn into internet censorship], Áron Kovács, Hvg.hu, October 27, 2012, http://hvg.hu/itthon/20121027_internetcenzura_tartalmak_letiltasa.
[50] Act CIV of 2010, Art. 1, par. 6.
[51] "Tanácsnokok és bloggerek" [Members and bloggers], Mediatanacs.blog.hu, January 11, 2011, http://mediatanacs.blog.hu/2011/01/11/tanacsnokok_es_bloggerek.
[52] Act CVIII of 2001 on Electronic Commerce, Art. 8, par. 1.
[53] Act CVIII of 2001, Art. 7. par. 3.
[54] Act CIV of 2010, Art. 17.
[55] Act CIV of 2010, Art. 16, and 4, par. 3.
[56] Act CLXXXV of 2010, Art. 186, par. 1, 187, par. 3. bf.
[57] Act CLXXXV of 2010, Art. 187, par. 3. e, 189, par. 4.

Critics of the 2010 media laws contend that the Media Council operates with unclear provisions and imposes high fines and sanctions on media outlets,[58] which might give rise to uncertainty and fear, lead to self-censorship, and have a chilling effect on journalism as a whole. Nonetheless, as of April 2013, no online media outlet had been penalized for violating the new stipulations introduced by the 2010 media laws, and in December 2011, the Constitutional Court struck down several provisions applicable to print and online outlets.[59] In May 2012, the parliament modified the media regulation in order to comply with the ruling of the Constitutional Court,[60] but left the above listed provisions valid in the case of printed press outlets and online media outlets. OSCE Representative on Freedom of the Media Dunja Mijatovic warned that the amendments "only add to the existing concerns over the curbing of critical or differing views in the country."[61]

Cases of copyright infringement are usually considered under civil law and can result in the "destruction of the device or material."[62] However, copyright infringement cases that cause financial injury can be punishable by imprisonment under both the current and the new criminal codes.[63]

A series of interviews conducted with journalists in 2012 provide a picture of the extent of self-censorship in Hungary, which is due to political and economic pressure on both traditional and online media outlets. According to most of the interviewees, the media laws had not made any difference when it came to self-censorship; instead, as one respondent noted, "the two-third majority push of executive power, the unprecedented leverage of that power, and the rise of the Fidesz party" have had a greater effect on self-censorship. Another journalist added that "party finance is entangled with media financing. Political and economic influence is exerted through public and private advertising." A respondent explained that "there was always some other interest at play, political or from the side of business and advertising—or both simultaneously, because these two often go hand in hand."[64] A journalist on hunger strike with colleagues against the alleged manipulation of news items in the public service media[65] held that "if your boss is telling you to falsify reports, it is your professional consciousness that decides whether you will fulfill these orders or not."[66]

---

[58] "Hungarian media laws Q&A," Article 19, August 2011, http://www.article19.org/data/files/medialibrary/2714/11-09-01-REPORT-hungary.pdf.
[59] Judit Bayer, "Hungarian Constitutional Court repeals parts of Media Constitution and Media Law," Media Laws, December 29, 2011, http://www.medialaws.eu/hungarian-constitutional-court-repeals-parts-of-media-constitution-and-media-law/. See also "Ruling No. 165/2011. (XII. 20.) AB of the Constitutional Court—Summary," Mertek. http://bit.ly/15BXMg1.
[60] "New laws curb media freedom," Human Rights Watch, May 29, 2012, http://bit.ly/MC3Oji.
[61] "Revised Hungarian media legislation continues to severely limit media pluralism, says OSCE media freedom representative," Organization for Security and Cooperation in Europe, May 25, 2012, http://www.osce.org/fom/90823.
[62] Act LXXVI of 1999 on Copyright, Art. 94, http://www.oapi.wipo.net/wipolex/en/text.jsp?file_id=127828#P530_98754.
[63] Act IV of 1978 on the Criminal Code, Art. 329/A, http://www.wipo.int/wipolex/en/details.jsp?id=2199 and Act C of 2012, Art. 359.
[64] "The Reins on Freedom: Self-Censorship in the Hungarian Press," Attila Mong, http://www.mertek.eu/en/reports/self-censorship-in-the-hungarian-press. The article was originally published in Hungarian in Élet és Irodalom, LVI, Nr. 15, April 20, 2012.
[65] "How the news get edited on Hungarian state television," Thecontrarianhungarian.wordpress.com (blog), December 14, 2011, http://thecontrarianhungarian.wordpress.com/2011/12/14/how-the-news-gets-edited-on-hungarian-state-television/.
[66] "Hunger strike speaks of downward spiral in Budapest," Rosie Scammel, January 24, 2012, http://www.huffingtonpost.co.uk/rosie-scammell/hunger-strike-budapest-hungary-downward-spiral_b_1228566.html.

Soon after the 2010 parliamentary elections, state advertising funds were partially or completely withdrawn from some quality newspapers, allegedly for political reasons, while others multiplied their revenues from such state sources.[67] Additionally, private advertisers tend to advertise where state companies do, meaning that some media outlets (those generally critical of the government) are "bleeding out."[68] The same phenomenon can be witnessed in the case of other platforms such as radio stations and outdoor advertisements; companies with close ties to the governing party received a large share of state funding for advertisements in 2012.[69] However, there is currently no data to determine the level of political influence over advertisements in cases of online media.

Despite the reported self-censorship and lack of financial resources, online media outlets have also become a tool to scrutinize public officials. For instance, starting in January 2012, Hvg.hu, an online news portal whose content is mostly different from the printed business weekly *HVG*, published a series of articles on how the then-president of the republic plagiarized his doctoral dissertation. Although he denied any wrongdoing, Pál Schmitt resigned in April 2012.[70]

Since 2011, the state-owned Hungarian News Agency (MTI) has had a virtual monopoly on the news market, as most of its news items are available to other news outlets free of charge. Consequently, media outlets that have been impacted by the economic crisis tend to republish MTI news items. During its overhaul, MTI became integrated into the system of public service broadcasting, led by the media authority. The media laws oblige MTI to produce news bulletins for public service broadcasters and edit their joint news portal.[71]

Although MTI has a major effect on traditional and online content, the online content landscape is relatively diverse. The two main news portals are Origo.hu (with an average of 862,000 daily visitors as of April 2013) and Index.hu (with an average of 685,000 daily visitors as of April 2013).[72] Most civil society organizations have websites, and an increasing number of them have a presence on Facebook. There are some media outlets, including online portals, for the minority Roma community;[73] the LGBT community and religious groups have online sources and forums as well. Nevertheless, many news sources, although independent, often reflect the politically divided nature of Hungarian society, and partisan journalism is widespread.[74]

---

[67] Annamária Ferenczi, "Kormányzati intézmények és állami cégek médiaköltései Magyarországon, 2003-2011. Leíró statisztikák és megfigyelések" [Government Advertising Incomes in the Hungarian Media, 2003-2011. Descriptive statistics and observations.], BCE Corruption Research Center, 2012, http://www.crc.uni-corvinus.hu/download/media_ah_2012_riport1_130430.pdf.
[68] Kim Lane Scheppele, "Hungary's free media," March 14, 2012, http://nyti.ms/zdrDTE.
[69] Ildikó D Kovács and Attila Bátorfy, "Az állam a médiapiacon 2012-ben," [The state on the media market in 2012], Kreativ.hu, December 19, 2012, http://www.kreativ.hu/media/cikk/az_allam_teljesen_ratelepedett_a_mediapiacra.
[70] Palko Karasz, "Hungarian president resigns amid plagiarism scandal," NYTimes.com, April 2, 2012, http://www.nytimes.com/2012/04/03/world/europe/hungarian-president-pal-schmitt-resigns-amid-plagiarism-scandal.html.
[71] Act CLXXXV of 2010, Art. 101, par. 4.
[72] "Total daily average for April 2013," Medián webaudit, accessed May 25, 2013, http://webaudit.hu/.
[73] Borbala Toth, "Minorities in the Hungarian media. Campaigns, projects and programmes for integration" (Center for Independent Journalism: Budapest, 2011): 19.
[74] If a media outlet does not have a leaning to a political/ideological side, then it is apolitical, dedicated to human interest stories, crimes, and catastrophes.

Blogs are generally considered an opinion genre and do not typically express independent or balanced news. There are also blogs analyzing governmental policies, the activities of public figures, and corruption.[75] Trolling is usually moderated where it is possible to comment on articles, typically to prevent negative discussions. It was reported that even politicians participated in online forum discussions using a pseudonym, and parties and ministries operated a monitoring system to be able to participate in discussions related to their work.[76] A survey conducted in 2011 among those netizens who knew what "commenting" meant indicated that 87 percent of the respondents encountered trolling on websites, but an overwhelming majority of the respondents considered commenting as a form of freedom of expression.[77]

Facebook, which had almost 4.3 million users in Hungary as of April 2013,[78] has grown increasingly popular as a tool for advocacy, especially after the 2010 parliamentary elections.[79] Since then many Facebook groups have formed, and several large demonstrations were organized through Facebook and disseminated on other social-networking sites, mobilizing tens of thousands of people both for[80] and against the government.[81] In 2012, the number of protests organized online for various social and political issues had mushroomed.[82] Protests are frequently broadcast online using Ustream, and pictures and videos are distributed instantly via Facebook.[83] In late 2012, students protesting against the overhaul of the higher education system started to produce their own videos to announce protests and to communicate their demands.[84] In October 2012, a coalition of civil society organizations formed "Together 2014," a campaign to defeat the Orbán administration during the next election cycle.[85] One of these organizations, Milla (One Million for Press Freedom), is a grassroots movement founded on Facebook in response to the 2010 media laws and which has since grown to be one of the largest opposition movements, organizing numerous demonstrations.[86] The extent of mobile phone use in organizing protests is unknown.

---

[75] To name a few: Atlatszo.hu, K-monitor.hu, Mandiner.hu, Szuveren.hu, Velemenyvezer.blog.hu, and the sites of Human Civil Liberties Union (Tasz.hu) and Eötvös Károly Institute (Ekint.org).
[76] László Bodolai, "Olvasói levelezés," [Readers' correspondence], in *Élet és Irodalom*, LV, Nr. 29, July 22, 2011.
[77] "Kommentek megítélése. Elemzés" [Judgement of comments. Analysis], MTE, Origo, Ipsos, 2012, p. 3 and 81, http://www.mte.hu/dokumentumok/mte_komment_kutatas.pdf.
[78] "Facebook Statisztika" [Facebook Statistics], Socialtimes.hu, accessed April 25, 2013, http://socialtimes.hu/stat/HU.
[79] Walter Mayr, "Facebook generation fights Hungarian media law," Spiegel.de, January 4, 2011, http://www.spiegel.de/international/europe/0,1518,737455,00.html.
[80] "Pro-government rally in Hungary, Jan. 21, 2012, Thecontrarianhungarian.wordpress.com, January 23, 2012, http://thecontrarianhungarian.wordpress.com/2012/01/23/pro-government-rally-in-hungary-jan-21-2012/
[81] "Hungarians protest against new Fidesz constitution," BBC, January 3, 2012, http://bbc.in/tyltNa.
[82] "Civil sphere and grassroots protest in Hungary: December, 2011," Thecontrarianhungarian.wordpress.com (blog), January 2, 2012, http://thecontrarianhungarian.wordpress.com/2012/01/02/civil-sphere-and-grassroots-protests-in-hungary-december-2011/. The group The City is for All regularly organizes protests related to homelessness and other social issues, see http://avarosmindenkie.blog.hu/tags/english. A trade union called Solidarity also frequently organizes demonstrations related to labour and social issues.
[83] Hajnalka Fülöp, "Így harcolnak a diákok a hálón," [This is how students fight on the web], Nol.hu, December 27, 2012, http://nol.hu/tud-tech/20121227-igy_harcolnak_a_diakok_a_halon.
[84] Mariette Le, "Students rally all over Hungary to save tuition-free education," Global Voices, December 13, 2012, http://globalvoicesonline.org/2012/12/13/students-rally-all-over-hungary-to-save-tuition-free-education/.
[85] Agnes Lovasz, "Hungary's Together 2014 to Struggle to Oust Orban, Eurasia Says," *Bloomberg*, December 11, 2012, http://www.bloomberg.com/news/2012-12-11/hungary-s-together-2014-to-struggle-to-oust-orban-eurasia-says.html.
[86] Erin Marie Saltman, "'Together 2014' movement emerges in Hungary," Policy-network.net, November 23, 2012, http://bit.ly/1bj3o1g.

VIOLATIONS OF USER RIGHTS

In June 2012, the Supreme Court fined two blog owners who were found guilty of defamation for comments that were posted by users on their websites, even though the comments were subsequently deleted. Additionally, cyberattacks against government websites continued to take place, and there was one case of physical assault against an online journalist covering a rally in October 2012.

The Fundamental Law of Hungary acknowledges the right to freedom of expression and defends "freedom and diversity of the press,"[87] though there are no laws that specifically protect online modes of expression. In 2012, the European Commission launched several infringement proceedings against Hungary, partly regarding the independence of the National Agency for Data Protection and the judiciary.[88] The European Commission expressed concerns over Hungary's decision to lower the mandatory retirement age from 70 years to 62 years for judges and prosecutors, effectively sending 274 judges, including some on the Supreme Court, into early retirement.[89] In November 2012, the Court of Justice of the European Union ruled that the early retirement of judges, prosecutors, and notaries was discriminatory.[90] Prior to that, in July 2012, the Hungarian Constitutional Court ruled that the early retirement was unconstitutional.[91] In March 2013, the parliament accepted a law that gradually decreases the retirement age of judges, prosecutors, and pensioners from 70 to 65 in the next 10 years.[92]

Additionally, there are concerns over the independence of the judiciary, as control over budgetary and management decisions has been handed over to the president of the National Judicial Office. The parliamentary majority amended the constitution for a fourth time in early 2013,[93] triggering further criticisms.[94]

Hungarian law does not distinguish between traditional and online media outlets in libel or defamation cases. The criminal code bans defamation, slander, the humiliation of national symbols (the anthem, flag, and coat of arms), the dissemination of totalitarian symbols (the swastika and red pentagram), the denial of the sins of national socialism or communism, and public scare-mongering through the media.[95] However, in February 2013, the Constitutional Court ruled that the ban on

[87] The Fundamental Law of Hungary (25 April 2011) Art. VIII., 1–2.
[88] "European Commission launches accelerated infringement proceedings against Hungary over the independence of its central bank and data protection authorities as well as over measures affecting the judiciary" European Commission, January 17, 2012, http://europa.eu/rapid/press-release_IP-12-24_en.htm.
[89] "European Commission launches accelerated infringement proceedings against Hungary over the independence of its central bank and data protection authorities as well as over measures affecting the judiciary" European Commission.
[90] Judgment of the Court (First Chamber), Case C-286/12, November 6, 2012, http://bit.ly/14TuyXJ.
[91] "Elkaszálták a bírói nyugdíjszabályt" [The retirement rule for judges was annulled], Index.hu, July 16, 2013, http://index.hu/belfold/2012/07/16/elkaszaltak_a_biroi_nyugdijszabalyt/.
[92] "Megszavazták a bírák lassú nyugdíjba küldését" [The law on the slow retirement of judges was accepted], Hvg.hu, March 11, 2013, http://hvg.hu/itthon/20130311_Megszavaztak_a_birak_lassu_nyugdijba_kuld.
[93] Kim Lane Scheppele, "Constitutional Revenge", Nytimes.com, March 1, 2013, http://nyti.ms/12hhYly.
[94] "Hungary defies critics over change to constitution,", Bbc.co.uk, March 11, 2013, http://bbc.in/10uVZmd.
[95] Act IV of 1978, Art. 179, 180, 269/A, 269/B, 269/C, Art. 270, 270/A. Act C of 2012, Art. 226–227, 332–335.

using totalitarian symbols is unconstitutional,[96] but the parliamentary majority decided to include it again in the penal code in April 2013.

Both the current civil code and the new draft of the civil code, which is scheduled to take effect in 2014, recognize civil rights (including protection against defamation) and ban the insulting of an individual's honor.[97] The draft civil code introduces the "damnification fee" for the non-pecuniary damages caused by violating civil rights.[98] Libel cases demonstrate that the courts generally protect freedom of expression, except when there is a conflict with another basic right. Defamation cases have decreased since a 1994 Constitutional Court decision, which asserted that a public figure's tolerance of criticism should be higher than an ordinary citizen's.[99] Some fear that the amended Fundamental Law and the new civil code—if accepted—will open up a "Pandora's box" of slander and libel cases initiated by anyone, including public figures, who can claim that their dignity has been harmed.

The fourth amendment to the Fundamental Law of Hungary, adopted by parliament on March 11, 2013, includes a provision that annuls all decisions of the Constitutional Court made prior to January 1, 2012. This provision calls into question the status of a number of decisions that the Constitutional Court had previously ruled on and which are not specifically outlined in the new Fundamental Law. For example, the court had previously ruled that the right to criticize public officials was protected speech; however, this right is not explicitly stated in the new constitution, which means it is unclear whether or not this right will be protected in the future.[100]

Prior to 2008, the criminal code was rarely used in cases of defamation or slander.[101] In 2008, the Hungarian Supreme Court found a journalist guilty of libel for describing the famous Hungarian Tokaj wine as "shit" in an article published in both the print and online versions of a daily newspaper. This decision was reversed at the European Court of Human Rights in 2011.[102] Launching criminal investigations for online activities is a recent phenomenon. In November 2012, the police launched an investigation based on comments that appeared on Nepszava.hu[103] and the news site Hir24.hu[104] that criticized Ferenc Papcsák, a Fidesz member of parliament and mayor of a district in Budapest. The police ordered the release of the personal data connected to these comments, including the users' internet protocol (IP) and e-mail addresses, although in the case of the latter site, commenters log-in via Facebook rather than providing a username or e-mail address.

[96] "Constitutional Court voids ban on «symbols of tyranny»; red star, swastika to become legal on April 30", Politics.hu, February 21, 2013, http://bit.ly/18eRl0o.
[97] Act IV of 1959 on the Civil Code, Art. 75–85; Bill Nr. T/7971 on the Civil Code, Art. 2:45.
[98] Bill Nr. T/7971, Art. 2:52–53.
[99] Péter Bajomi-Lázár and Krisztina Kertész, "Media Self-Regulation Practices and Decriminalization of Defamation in Hungary," in *Freedom of Speech in South East Europe: Media Independence and Self-Regulation*, ed. Kashumov, Alexander (Sofia: Media Development Center, 2007): 177-183.
[100] Scheppele 2013.
[101] Bajomi-Lázár and Kertész 2007: 179.
[102] See ruling of European Court of Human Rights, Case of Uj vs. Hungary, 2011.
[103] "Latest Papcsák case may infringe on freedom of the press", Civilmedia.net, November 13, 2012, http://bit.ly/16AgLbS.
[104] "Feljelentették a Népszava és a Hír24 kommentelőit", [Comments of Nepszava and Hir24 denounced] Gepnarancs.hu, November 10, 2012, http://gepnarancs.hu/2012/11/feljelentettek-a-nepszava-kommenteloit/.

In January 2013, a blogger named Tamás Polgár, alias "Tomcat," was condemned for incitement, and received a prison sentence of one year and two months based on the penal code.[105] The sentence was suspended for five years, and the ruling is not final as the defendant has appealed. In a blog post in 2009, during a period in which six Roma people were killed in a case of serial murders, Polgár called upon readers to beat up Gypsies.[106] This is the first case since the democratic transition in which someone has been prosecuted under the penal code for material they posted online. As is the case with decisions of the Supreme Court, one needs to demonstrate that there was clear and imminent danger, which is hard to prove.[107]

Generally, users who wish to comment on a web article need to register with the website by providing an e-mail address and username, or they need to use a Facebook login. The operator of a website may be asked to provide the commenter's IP address, e-mail address, or other data in case of an investigation.[108] According to some analysts, the 2010 media laws "blurred the responsibility of the media outlet and the commenter."[109] In an article published on Index.hu in July 2011, however, a member of the Media Council stated that comments are not subject to the media laws.[110]

The legal implications of comments posted online remains unclear. As the chair of the self-regulatory Association of Hungarian Content Providers (MTE) noted, court decisions are diverse in cases of libel committed in a comment online.[111] His analysis of case studies concludes that Act CVIII of 2001 on Electronic Commerce—based on which providing a commenting option could be considered as a web-hosting service—is not applied frequently. Nonetheless, a comment that has been posted could technically be brought to court even if it were deleted minutes later, rendering website moderating a less useful method for avoiding legal liability. Requiring prior approval from the website administrator before comments are posted may also prove problematic, as a court might consider it editing, which would exclude the use of the Act on Electronic Commerce. Websites operated from abroad can be brought to court as well. This legal uncertainty may prompt some outlets to disable the commenting feature altogether, as at least one popular website did in 2011.

In June 2012, the Supreme Court condemned the publishers of two blogs for defamation committed in comments posted on their sites based on the right of good reputation as described in the civil code, regardless of the fact that the comments had been deleted. The Supreme Court ruled

[105] Act IV of 1978, Articule 269 says: "A person who incites to hatred before the general public against a) the Hungarian nation, b) any national, ethnic, racial group or certain groups of the population, shall be punishable for a felony offense with imprisonment up to three years."
[106] "Court slaps far-right activist Tomcat with suspended jail term", Politics.hu, January 11, 2013, http://bit.ly/17dkzxc.
[107] Zsolt Zádori, "Bűntethető-e Bayer véres szájalása?" [Can they condemn Bayer's bloody words?], Helsinkifigyelo.hvg.hu, January 8, 2013, http://helsinkifigyelo.hvg.hu/2013/01/08/buntetheto-e-bayer-veres-szajalasa/.
[108] Act XIX of 1998 on criminal proceedings, Art. 178/A, par. 1.
[109] Anonymous internet expert, email communication, February 7, 2012.
[110] "A kommentekre nem vonatkozik a médiatörvény" [The media law does not concern comments], Index.hu, July 3, 2011, http://index.hu/belfold/2011/07/03/a_kommentekre_nem_vonatkozik_a_mediatorveny/.
[111] Péter Nádori, "Kommentek a magyar interneten: a polgári jogi gyakorlat," [Comments on Hungarian internet: civil code practice], In Medias res, I, Nr. 2, 2012, Pp. 319–333.

that the plaintiff was harmed in his right to good reputation, and that the defendants needed to pay for the legal expenses incurred.[112]

There are no restrictions on anonymous communication, and encryption software is freely available without government interference. Pretty Good Privacy (PGP), a data encryption program, is often used by investigative journalists.[113] Nevertheless, to sign a contract with the mobile phone company, users must provide personal data upon purchase of a SIM card.[114]

According to the Electronic Communications Act, electronic communications service providers[115] are obligated to "cooperate with organizations authorized to perform intelligence information gathering and covert acquisition of data."[116] Additionally, the act states that "the service provider shall, upon the written request from the National Security Special Service, agree with the National Security Special Service about the conditions of the use of tools and methods for the covert acquisition of information and covert acquisition of data."[117]

National security services can "gather information from telecommunications systems and other data storage devices" without a warrant.[118] The authorities have allegedly installed black boxes on ISP networks.[119] Secret services can access and record communication transmitted via ICTs, though a warrant is required.[120] There is no data on the extent to which, or how regularly, the authorities monitor ICTs. In June 2012, colleagues of the Eötvös Károly Institute issued a complaint to the Constitutional Court requesting the annulment of the provision that allows the minister overseeing the work of the Counter Terrorism Center to approve the secret surveillance of individuals.[121] They argued that this provision is unconstitutional and that such surveillance should be tied to the approval of a judge rather than a minister.[122]

In accordance with the EU Directive 2006/24/EC on data retention, ISPs and mobile phone companies in Hungary must retain user data for up to one year, including personal data, location, caller phone numbers, the duration of phone conversations, IP addresses, and user IDs for investigative authorities and security services.[123] There is no data on the extent of these activities,

---

[112] Pfv.IV.20.217/2012/5, June 13, 2012.
[113] Borbala Toth, "Mapping Digital Media: Hungary," Open Society Foundations, February 2012, p. 50, http://www.opensocietyfoundations.org/reports/mapping-digital-media-hungary.
[114] Act C of 2003 on Electronic Communications, Art. 129, http://www.ictregulationtoolkit.org/en/Publication.2347.html.
[115] Electronic service providers provide electronic communications service, which means a "service normally provided against remuneration, which consists wholly or mainly in the conveyance, and if applicable routing of signals on electronic communications networks, but exclude services providing or exercising editorial control over the content transmitted using electronic communications network; it does not include information society services, defined under separate legislation, which do not consist primarily in the conveyance of signals on electronic communications networks," Act C of 2003, Art. 188, par. 13.
[116] Act C of 2003, Art. 92, par. 1.
[117] Act C of 2003, Art. 92, par. 2.
[118] Act CXXV of 1995 on the National Security Services, Art. 54, http://bit.ly/1bhE9cm.
[119] "Hungary – Privacy Profile," Privacy International, January 22, 2011, https://www.privacyinternational.org/reports/hungary.
[120] Act CXXV of 1995, Art. 56.
[121] Act CXXV of 1995, Art. 58, par. 2. states that in some instances – basically including the tasks of the Counter Terrorism Center – the minister for justice can grant the warrant.
[122] László Majtényi et al, "Mit keres a Terrorelhárítási Központ a paplan alatt?", [What is the Counter Terrorism Center is doing under the duvet?], in: Élet és Irodalom, LVI, Nr. 26, June 29, 2012.
[123] Act C of 2003, Art. 159/A; "Hungary – Privacy Profile," Privacy International, January 22, 2011.

even though there is a legal obligation to provide the European Commission with statistics of the queries for data made by the investigating authorities.[124] Cybercafes, on the other hand, are not required to collect user information, and anyone can access the internet at a cybercafe without registration.

Bloggers, ordinary ICT users, websites, or users' property are not generally subject to extralegal intimidation or physical violence by state authorities or any other actors. However, in September 2011, photographers of the online news portals Index.hu and Origo.hu were banned from parliament because they had allegedly taken pictures of the prime minister's notes.[125] In a separate incident in December 2011, journalists from Index.hu were banned from parliament for being disrespectful after they posted a video of two reporters singing and dancing in the building.[126] The journalists were permitted to enter parliament again roughly one month later. In January 2012, a photographer from Vagy.hu was not admitted to the public ball of Debrecen city because the organizers claimed that the local news site was not registered with the NMHH.[127] These types of incidents impede the ability of journalists to cover the news, compromising the Hungarian news and information landscape. In October 2012, there was one physical attack against a journalist of Index.hu, whose nose was broken by an extreme-right protester at an anti-government rally.[128]

In response to Hungary's 2010 media laws, the international hacker group Anonymous posted a video on YouTube threatening the Hungarian government with a cyberattack in August 2011.[129] Since then, the group rewrote the new Hungarian constitution on the website of the Constitutional Court,[130] and several government sites, including that of the National Board Against Counterfeiting and the personal website of the Minister of State for Education, were disrupted via distributed denial-of-service (DDoS) attacks in early 2012.[131] Additionally, the website of Közgép, a construction company that frequently wins public procurements, was attacked on September 5, 2012.[132] Three days later, several Hungarian members of Anonymous were arrested,[133] although the accused were discharged to prepare for the defense. In January 2013, the websites of Prime Minister Viktor Orbán (Miniszterelnok.hu, Orbanviktor.hu) were also hacked by Anonymous.[134]

---

[124] Act C of 2003, Art. 159/A, par. 7.
[125] "Photographers banned from Hungarian Parliament," Thecontrarianhungarian.worldpress.com (blog), September 20, 2011, http://thecontrarianhungarian.wordpress.com/2011/09/20/photographers-banned-from-hungarian-parliament/.
[126] "Hungary's leading online news portal banned from parliament," Politics.hu, December 22, 2011, http://bit.ly/sWPWb4.
[127] Zsolt Kácsor, "Debrecen nem kért a TV2 és az RTL kameráiból" [Debrecen did not want the cameras of TV2 and RTL Klub], Nol.hu, January 16, 2012, http://nol.hu/lap/mo/20120116-csak_a_helyi_teve_tudosithatott_a_rekordkiserletrol.
[128] "Halál rátok, zsidók!" ["Death on you, Jews!"], Index.hu video, 23 October 2012, http://bit.ly/X95KpO.
[129] "The Anonymous message to Hungarian government," YouTube, accessed January 30, 2012, http://www.youtube.com/watch?v=SStDZ5De1Og.
[130] "Anonymous geek-topia: Hackers change Hungarian constitution," Rt.com, March 5, 2012, http://rt.com/news/anonymous-hungary-court-constitution-881/.
[131] Máté Nyusztay, "'A rendszert támadjuk' – Magyarország is az Anonymous célkeresztjében" ['We attack the system' – Hungary is among the targets of Anonymous], Nol.hu, February 15, 2012, http://nol.hu/belfold/a_rendszert_tamadjuk__-_magyarorszag_is_az_anonymus_celkeresztjeben.
[132] "Közgép 'oligarchy' hit by hackers," Budapesttimes.hu, September 5, 2012, http://www.budapesttimes.hu/2012/09/05/kozgep-oligarchy-hit-by-hackers/.
[133] "Elfogták a magyar Anonymous tagjait" [Hungarian members of Anonymous were captured], Index.hu, September 8, 2012, http://index.hu/belfold/2012/09/08/elfogtak_a_magyar_anonymus_tagjait/.
[134] "Feltörték Orbán honlapját" [Orbán's site got hacked], Index.hu, January 23, 2013, http://index.hu/tech/2013/01/23/feltortek_orban_honlapjat/.

ICELAND

	2012	2013
INTERNET FREEDOM STATUS	N/A	FREE
Obstacles to Access (0-25)	n/a	1
Limits on Content (0-35)	n/a	1
Violations of User Rights (0-40)	n/a	4
Total (0-100)	n/a	6

* 0=most free, 100=least free

POPULATION: 320,000
INTERNET PENETRATION 2012: 96 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- In 2013, the previous minister of the interior proposed a new law to ban online pornography, though the ban has not been implemented and is currently stalled (see **LIMITS ON CONTENT**).
- The internet continues to play a significant role in online mobilization: on October 20, 2012, a majority of the population participated in a crowdsourced, non-binding constitutional referendum (see **LIMITS ON CONTENT**).
- The Icelandic Modern Media Initiative from 2010, which aims to transform Iceland into a global free-speech safe haven, continued to make progress (see **VIOLATIONS OF USER RIGHTS**).
- The new media law from 2011 helped reduce the number of libel cases against journalists (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Iceland has one of the highest rates of internet and social media use in the world, according to the World Economic Forum.[1] In the wake of the country's financial collapse in 2008, when the three major banks went bankrupt, social media platforms like Facebook were integrated into the process of creating a new crowdsourced constitution.[2] Internet and digital media play a vital role in Icelandic society, and Iceland is an international leader when it comes to focusing on free speech and online media. In June 2010, the Icelandic parliament launched a new media initiative protecting free speech, aiming to make Iceland a safe haven for journalists and whistleblowers.[3] At the same time, a recent political proposal from the former minister of the interior, Ögmundur Jónasson, to ban online pornography has received immense international media attention. Since there has been a change in government after the parliamentary election in late April 2013, this bill will most likely remain stalled until later in 2013.[4]

OBSTACLES TO ACCESS

Iceland is one of the most connected countries in the world, with the highest percentage of households with access to the internet in Europe.[5] Iceland has been connected to the internet since 1989 via the NORDUnet in Denmark. The following year, a leased line to NORDUnet in Sweden was established, and the link was gradually upgraded. The Nordic connection was supplemented in 1997, when ISnet established a direct connection to Teleglobe in Canada, which was upgraded when the line was moved to New York in 1999.[6] In 1998, broadband connections were put into operation, and already in 2006 just under 90 percent of Icelandic households had internet access. The percentage of households with high speed internet connections, such as ADSL or SDSL, has increased greatly in recent years.[7] In 2007, the Icelandic city of Seltjarnes became the first municipality in the world where every citizen has access to fiber-optic internet service.[8]

According to the official website Iceland Statistics, Iceland had an internet penetration rate of 96 percent in 2012, with only a minimal difference in usage between the capital region and the other regions of the country. [9] The price of accessing the internet via computers and mobile phones is very affordable: a basic internet subscription with 12 Mbps costs around ISK 3,700 per month

[1] World Economic Forum, "The Global Information Technology Report 2013," http://bit.ly/10UMw8u.
[2] Robert Robertson, "Voters in Iceland Back New Constitution, More Resource Control," *Reuters*, October 21, 2012, http://www.reuters.com/article/2012/10/21/us-iceland-referendum-idUSBRE89K09C20121021.
[3] International Modern Media Institute, https://immi.is/.
[4] Interview with employee at the Icelandic Media Commission, May 17, 2013.
[5] As of 2012, 95 percent of households in Iceland had internet access, followed by Norway and Luxembourg with 93 percent and Denmark with 92 percent. International Telecommunication Union, "Core indicators on access to and use of ICT by households and individuals," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[6] Cathy Newman, "Iceland Internet Diffusion," http://www1.american.edu/carmel/cn9463a/iceland.htm.
[7] Birgir Gudmondsson, "Media Landscapes – Iceland", European Journalism Centre, 2010, http://ejc.net/media_landscapes/iceland.
[8] Idega-website, "Seltjarnes," http://www.idega.is/pages/vidskiptavinir/seltjarnarnes/?iw_language=en.
[9] Statistics Iceland, http://www.statice.is.

(approximately $31), and a basic mobile phone connection with 500 Mb data costs around ISK 590 per month (approximately $5),[10] while the average monthly salary is approximately ISK 560,000 ($4,700).[11] Icelanders are frequent internet users, with 91 percent connecting to the internet daily or almost daily. A vast majority of the population (88 percent) is connected via broadband, and a growing number (21 percent) are connected via fiber-optics.[12] In addition, mobile phones are widely used to access the internet, and 44 percent of Icelanders have a mobile connection of 3G or faster. Only five percent has a mobile connection slower than 3G service.[13]

Iceland has multiple channels connecting the country to the international internet, including connections to the international backbone through three submarine cables: FARICE-1, DANICE, and Greenland Connect. The Reykjavik Internet Exchange point, which exchanges internet traffic among internet service providers (ISPs) located in Iceland, is operated independently of the government by the top-level domain registry ISNIC.

Síminn is the main internet and telecommunications operator in Iceland and runs fixed-line and mobile voice call services, as well as internet services and broadband television.[14] Síminn is based on a merger between Landssími Íslands, which was privatized in 2005, and the company Skipti ehf. Of the ISPs, Síminn holds the largest market share (50.7 percent), followed by Vodafone (32.1 percent), Tal (9.1 percent), Hringdu (3.4 percent) and other companies comprising the remaining 4.7 percent. Regarding market share in mobile broadband, Síminn is the leading provider with 37.7 percent of the market, followed by Nova (33.2 percent), Vodafone (25 percent), and Tal (3.8 percent).[15]

The main regulatory body governing information and communication technologies (ICTs) in Iceland is the Post and Telecom Affairs (PTA), which is an independent center under the direction of the Ministry of the Interior. The PTA supervises development, logistics, and fair competition in the field of telecommunications networks. Decisions of the PTA may be referred to the Rulings Committee for Electronic Communications and Postal Affairs. The minister of the interior appoints the three members of the Appellate Committee, following the nomination by the Supreme Court. The chairman and vice chairman must comply with the competence qualifications applying to Supreme Court judges. The members of the committee are appointed for a period of four years.[16] In addition to the PTA, the Ministry of the Interior is responsible for the legal matters relating to online content.

A new media law was established on September 1, 2011, and continued to stir debate in 2012 and 2013. While the intention of the law was to create greater press freedom through a comprehensive

[10] Siminn Iceland: http://www.siminn.is/english/mobile/mobile-internet/.
[11] Statistics Iceland, "Wages," http://bit.ly/19JQxja.
[12] Post and Telecom Administration, "Statistics on the Icelandic Electronic Communications Market for the First Half of 2012," http://www.pfs.is/upload/files/T%C3%B6lfr%C3%A6%C3%B0isk%C3%BDrsla%20PFS%20fyrri%20hluti%202012.pdf
[13] Statistics Iceland: http://www.statice.is
[14] The Post and Telecom Administration, "Statistics on the Icelandic Electronic Communications Market for the First Half of 2012," http://www.pfs.is/upload/files/T%C3%B6lfr%C3%A6%C3%B0isk%C3%BDrsla%20PFS%20fyrri%20hluti%202012.pdf.
[15] The Post and Telecom Administration, 2012: Tölfræðiskýrsla PFS um fjarskiptamarkaðinn_f.hl. 2012.xls
[16] The Post and Telecom Administration, "Rulings Committee," http://www.pfs.is/Default.aspx?cat_id=146.

framework governing broadcast, press, and online media, the creation of an oversight State Media Commission has been criticized. According to the law, the minister of education, science and culture appoints five persons to the Media Commission for terms of four years at a time. Two representatives are appointed in accordance with a nomination by the Supreme Court, one in accordance with a nomination by the standing Committee of Rectors of Icelandic Higher Education Institutions, and one in accordance with a nomination by the National Union of Icelandic Journalists. The fifth is appointed by the minister without an outside nomination.[17]

The Media Commission has no authority to deal with media concentration (a major concern of public debate in Iceland), but new legislation was put forth in 2013 that would give the Competition Authority oversight responsibility in consultation with the Media Commission. The bill was passed as an amendment to the new media law in March 2013. The amendment gives the Competition Authority other means and measures to deal with competition cases when media companies are concerned. Thus, the Competition Authority can look at issues such as plurality and whether there will be a decrease in newsrooms resulting from mergers and acquisitions, for example. According to the bill, the Media Commission shall in such cases give its opinion from a media authority's perspective. The commission has extensive powers to impose fines on media outlets, as well as requiring media outlets to register with a detailed "editorial strategy," meaning that all media companies must set their own rules for editorial independence in cooperation with the Association of Journalists or a similar entity. In 2012, all media companies had to set such rules as part of the process of self-regulation, and no decisions have yet been made regarding online media by the Icelandic Media Commission.[18]

LIMITS ON CONTENT

Access to information and online communication is free from government interference. Iceland is not a member of the European Union; however, since the country is part of the European Economic Area, it has agreed to follow legislation regarding consumer protection and business law similar to the other member states, meaning that the legal status of file-sharing websites such as Pirate Bay is up for debate.[19] In April 2013, the Pirate Bay website relocated to Iceland, giving it a ".is" domain name.[20] According to Icelandic law, the registrant is responsible for ensuring that the use of the domain is within the limits of the law.[21] In April 2013, the Icelandic Supreme Court confirmed the Reykjavík District Court's ruling ordering Valitor (the Icelandic partner of Visa and MasterCard) to remove the unlawful block on donations to the website for the organization WikiLeaks.[22]

Similar to other Nordic countries, ISPs in Iceland filter websites containing child pornography. The

[17] Fjolmidlanefnd, "The Media Commission," http://fjolmidlanefnd.is/english/.
[18] Fjolmidlanefnd, "The Media Commission."
[19] OpenNet Initiative, "Nordic Countries," https://opennet.net/research/regions/nordic-countries.
[20] The URL www.thepiratebay.is is automatically transferred to www.thepiratebay.xs.
[21] News of Iceland, "The Pirate Bay Moves to Iceland," April 25, 2013, http://bit.ly/ZuRY4c. .
[22] Ian Steadman, "Icelandic Court Declares WikiLeaks Donation Ban 'Unlawful,'" *Wired*, April 27, 2013: http://bit.ly/12NeQvx.

ISPs collaborate with the Icelandic Save the Children *Barnaheill* and participate in the International Association of Internet Hotlines (INHOPE) project.[23] In addition, pornography in general is illegal in Iceland, although the ban is not strongly enforced. During the past few years, political attempts have been made to eliminate the sex industry, including banning strip clubs and imposing fines and jail terms for customers taking advantage of prostitutes. In 2013, the previous minister of the interior, Ögmundur Jónasson, proposed two new bills to the parliament in order to uphold and reinvigorate an existing law banning pornography and gambling online that is rarely enforced and vaguely worded. The ban focuses on pornography that is defined as violent and degrading material, and a committee of experts was to explore how a ban on pornography could be enforced—for example, by making it illegal to pay for pornographic material with Icelandic credit cards, or by creating a national internet filter and a blacklist of websites that contain pornographic content.[24] Opponents led by Icelandic Member of Parliament and free speech activist Birgitta Jónsdóttir deemed that the ban would limit free speech online, a position that was supported by academics and free speech advocates from outside Iceland in an open letter to the Icelandic minister of the interior.[25] The plan for banning pornographic content online has most likely lost its momentum since the change in government during the parliamentary election on April 27, 2013.

Social media platforms such as YouTube, Facebook, Twitter, and international blog hosting services are freely available and are used by a large part of the population. Iceland ranks in the top of countries with a high percentage of Facebook usage, and 72.6 percent of the population has an account.[26] A poll among politicians running in the May 2010 municipal elections showed that many considered Facebook to be the second most important medium during the election for reaching the general public in their municipalities, second only to local newspapers.[27]

ISPs and content hosts are not held responsible for the content that they host or transmit. Claims regarding intellectual property rights are handled by the Icelandic Patent Office, which is substantially dependent on international cooperation, and Iceland is party to a number of international agreements in this field. Moreover, Iceland, as a member of the World Trade Organization (WTO), has adapted Icelandic legislation to the provisions of TRIPS (Trade-Related Aspects of Intellectual Property Rights). Furthermore, the Agreement on the European Economic Area has led to several legislative amendments in Iceland in accordance with the directives and regulations of the European Union.

Icelandic law number 30/2002 establishes a system of takedown notices for IP addresses or other online content that violates the law, in accordance with the Directive 2000/31/EC of the European Parliament. During the last session of parliament, a bill was presented to ban online gambling by prohibiting Icelandic credit card companies from processing payments to gambling websites;

[23] INHOPE website, http://www.inhope.org.
[24] "Banning the Sex Industry - Naked Ambition," *The Economist,* April 20, 2013, http://econ.st/12q1wwM.
[25] IceNews, "Iceland's Porn Ban Effort Draw Fire from Abroad," March 17, 2013, http://www.icenews.is/2013/03/07/icelands-porn-ban-effort-draws-fire-from-abroad/.
[26] Socialbakers, Facebook Statistics by Country, http://www.socialbakers.com/facebook-statistics/.
[27] Birgir Gudmondsson, "Media Landscapes – Iceland", European Journalism Centre, 2010, http://ejc.net/media_landscapes/iceland.

however, the bill was not passed.[28] The Ministry of the Interior is responsible for handling matters related to online content, and the appeals process for disputing the removal of content is linked to the independent courts in Iceland.

Self-censorship is not a widespread problem in Icelandic online media, and there are very few instances of government or partisan manipulation of online content. However, during the Wikileaks controversy in 2010, a number of banks and credit card companies, including the Icelandic credit card company Valitor, blocked donations to the Wikileaks website. In April 2013, the Icelandic Supreme Court confirmed the Reykjavík District Court's ruling ordering Valitor (the Icelandic partner of Visa and MasterCard) to remove the unlawful block on donations to the website.[29]

Iceland has a vibrant digital sphere and almost all traditional media, such as print, radio, and television, offer versions of their content online. The websites of some newspapers, like the daily *Morgunbladid*, are among the most popular Icelandic-language sites.[30] Internet banking is widely used, and a large majority of Icelanders (90 percent) are online bank users. E-governance is successful in Iceland, and Iceland Statistics states that in 2012 approximately 75 percent of the population obtained information from public authorities' websites.[31] In recent years, public institutions have started a migration process from proprietary software to free and open software.[32] The government promotes the use of digital signatures and electronic filing, and the use of digital signatures is supported through legislation such as the Public Administration Act. Digital signatures are in the process of being integrated further into the public administration.[33]

The popularity of social media sites like Facebook was used to engage the population during the process of redrafting the Icelandic constitution over the past few years. The original and existing constitution is an almost exact copy of the Danish constitutional text, which was adopted when Iceland gained independence from Denmark in 1944. In the wake of the Icelandic financial crisis in 2008, the population demanded an extensive review of the country's constitution.[34] A 25-member council consisting of ordinary residents helped draft a new constitution and worked through sixteen versions in four months based on 16,000 comments from Icelandic citizens using social media platforms such as Facebook, Twitter, and YouTube.[35] A majority of the population voted for the draft constitution in a national referendum on October 20, 2012.[36] The draft constitution is not

[28] Information from the Icelandic Patent Office, www.els.is.
[29] Ian Steadman, "Icelandic Court Declares WikiLeaks Donation Ban 'Unlawful,'" *Wired*, April 27, 2013, http://www.wired.co.uk/news/archive/2013-04/26/wikileaks-wins-visa-case.
[30] Birgir Gudmondsson, "Media Landscapes – Iceland", European Journalism Centre, 2010, http://ejc.net/media_landscapes/iceland.
[31] Iceland Statistics, http://www.statice.is/.
[32] ePractice EU, "Public administration in Iceland is moving to open source," April 5, 2012, http://www.epractice.eu/en/news/5351796.
[33] IDABC – European eGovernment Services, "Study on Mutual Recognition of eSignatures," July 2009, http://ec.europa.eu/idabc/servlets/Docae09.pdf?id=32328.
[34] Robert Robertson, "Voters in Iceland Back New Constitution, More Resource Control," *Reuters*, October 21, 2012, http://www.reuters.com/article/2012/10/21/us-iceland-referendum-idUSBRE89K09C20121021.
[35] "A Proposal for a New Constitution for the Republic of Iceland", Drafted by *Stjórnlagaráð*, a Constitutional Council, appointed by an *Althingi* resolution, March 24, 2011, http://stjornlagarad.is/other_files/stjornlagarad/Frumvarp-enska.pdf
[36] Julia Mahncke, "Iceland's Grassroots Constitution on Thin Ice," *Deutsche Welle*, March 13, 2013, http://bit.ly/XmC9Hj.

likely to become an actual constitution, since the results of the referendum were non-binding and the previous parliament put the draft constitution on hold until after the election in 2013. The political parties forming the newly elected government, together with many interest groups and independent academics, were opposed to many of the proposed changes in the draft document.[37]

Social and online media were widely used in the recent parliamentary elections, and a historically large number of parties ran for parliament. In particular, small parties with limited resources see digital media as an inexpensive way to inform voters about their political agenda. The newly elected Icelandic Pirate Party, led by Birgitta Jónsdóttir, exclusively used online media to disseminate their platform supporting media freedom with a focus on the internet. [38]

VIOLATIONS OF USER RIGHTS

Iceland has a strong tradition of protecting freedom of expression that extends to the use of the internet. Freedom of expression is protected under Article 73 of the Icelandic constitution.[39] In June 2010, in the wake of the financial crisis and inspired by the whistleblower website WikiLeaks, the Icelandic parliament approved a resolution on the Icelandic Modern Media Initiative, aiming to create a global safe haven with legal protection for the press, bloggers, and whistleblowers.[40] The reform process of the ambitious Icelandic Modern Media Initiative is still in progress, although source protection has been implemented into law.[41] The minister of education, science and culture has appointed a committee of experts with the task of reporting on online and offline challenges and proposing changes regarding freedom of expression and information. The task of this committee is to come up with a whistleblower protection law, review the articles on defamation in the penal code, and look into source protection and communications protection. This committee was appointed in 2012 and its mandate will be renewed for another year. [42]

The Icelandic media law, which came into effect in September 2011, established several legal protections for journalists that extend to the online sphere, including editorial independence from media service providers' owners and the protection of anonymous sources.[43]

There has been great concern about libel laws in recent years, in regard to both online and offline media. Journalists consider the court's practice to be too rigid, leading to lawsuits that aim to silence critical press. In 2012, two libel cases went to the European Court of Human Rights, which ordered the Icelandic state to pay considerable damages to the journalists Erla Hlynsdóttir[44] and

[37] Interview with employee at the Icelandic Media Commission, May 17, 2013.
[38] Ibid.
[39] Constitution of the Republic of Iceland, http://www.government.is/constitution/.
[40] IFEX, "Authorities Create a Safe Haven for Press", June 23, 2010: http://www.ifex.org/iceland/2010/06/23/safe_haven/
[41] International Modern Media Institute, https://immi.is.
[42] Interview with employee at the Icelandic Media Commission, May 17, 2013.
[43] Article 24 and Article 25, The Icelandic Media Law, April 20, 2011, http://bit.ly/15C05KS.
[44] European Court of Human Rights, "Case of Erla Hlynsdóttir vs. Iceland," October 10, 2012, http://bit.ly/MfiatW.

Björk Eiðsdóttir of the print and online daily newspaper *DV*.[45] The two journalists had been found guilty of defamation by an Icelandic court under the old media law because they had quoted sources who made what could be considered as defamatory statements. That same year, a blogger at *DV*, Teitur Atlason, suggested that prominent businessman and former Member of Parliament Gunnlaugur Sigmundsson had been involved in corruption. Sigmundsson sued the blogger for libel, although Atlason was acquitted, as the allegations were not new and had been published previously in Icelandic media.[46] In 2011, DV.is journalist Jón Bjarki Magnússon was convicted of defamation for quoting from open court documents from 1989 in an article on a family with a history of violence. The court found the documents too old to be relevant for the public.[47]

As a direct result of the aforementioned cases and the subsequent public debate within Iceland, the new media law attempts to solve some of these problems. According to Article 51, journalists can no longer be held responsible for potentially libelous quotes from sources.[48] Article 51 specifies that journalists can only be held responsible for their own content and not for content quoted from other sources. This article does nothing to change the libel laws in Iceland, but only who can be held responsible for potentially libelous quotes.

The government does not place any restrictions on anonymous communication. No registration is required when purchasing a SIM card in Iceland.

Currently, the Electronic Communications Act of 2003 implements data retention requirements mandated by Iceland's inclusion in the European Economic Area.[49] The law applies to telecommunication providers, and its current implementation mandates the retention of records of all connection data for six months. It also states that companies may only deliver information on telecommunications in criminal cases or on matters of public safety, and that such information may not be given to anyone other than the police or the public prosecution.[50]

There have been no physical attacks against bloggers or online journalists in Iceland, and there were no significant incidences of cyberattacks in Iceland during 2012–2013.

[45] The ECHR found that quoting a source making possibly defamatory comments could not in itself be seen as defamatory and that the right journalistic ethical practices were in place. European Court of Human Rights, "Case of Björk Eidsdóttir vs. Iceland," October 10, 2012, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-112091
[46] Sigrun Davidsdóttir, "Elections in Iceland: Looking for the Past in the Present," April 17, 2013, http://bit.ly/15GjM82.
[47] Anna Andersen, "An Icelandic Modern Media Inferno," *The Reykjavik Grapevine*, November, 7, 2011, http://bit.ly/vDZmgA.
[48] The Icelandic Media Law, April 20, 2011, http://bit.ly/15C05KS.
[49] Electronic Communications Act, March 26, 2003, http://bit.ly/MfiatW.
[50] Icelandic Media Initiative, https://immi.is/index.php/projects/immi.

INDIA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	13	15
Limits on Content (0-35)	9	12
Violations of User Rights (0-40)	17	20
Total (0-100)	**39**	**47**

* 0=most free, 100=least free

POPULATION: 1.3 billion
INTERNET PENETRATION 2012: 13 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Hundreds of blocks, supposedly targeting inflammatory content, affected a wide range of pages, including some in the public interest (see **VIOLATIONS OF USER RIGHTS**).
- At least eleven people were charged under Section 66 of the 2008 IT Act amendment for posts on social media (see **VIOLATIONS OF USER RIGHTS**).
- Cartoonist Aseem Trivedi was arrested for anti-corruption cartoons, initially on charge of sedition, which carries a life sentence (see **VIOLATIONS OF USER RIGHTS**).
- The Central Monitoring System, partly in place since April 2013, seeks to equip a range of agencies to monitor any electronic communication in real time, without informing the target or a judge (see **VIOLATIONS OF USER RIGHTS**).
- Online campaigning for women's rights in the wake of a brutal sexual assault promoted street protests and some legislative reforms (see **LIMITS ON CONTENT**).

INTRODUCTION

The internet has become a powerful tool for sharing information and articulating dissent in India, despite low overall penetration and power shortages limiting access for many. While still concentrated in urban areas, access is gradually spreading to rural India, providing a forum for voices not always represented in the traditional media.

There are no systematic restrictions on political content on the Indian web. Since the November 2008 terrorist attacks in Mumbai, however, a confusing and frequently contradictory series of legal amendments, rules, and guidelines have strengthened official powers to censor online content and monitor communications. A 2008 Information Technology Act amendment allowed officials to issue blocking orders to internet service providers (ISPs), outlining a procedure and protecting compliant companies from legal proceedings. But 2011 intermediary guidelines under the same Act introduced a different process, making companies liable to criminal penalties if they fail to delete or take down content which any individual flags as "offensive." Courts can also order blocks, and their efforts to contain copyright violations sometimes render entire platforms inaccessible. All told, hundreds of pages were reported blocked by multiple actors during the coverage period, most by the government grappling with religious unrest, though no formal count was made public. While some blocks targeted legitimate hate speech, the opaque process undermined public trust and left legitimate internet users, victims of "collateral blocking," without a means of appeal.

Twenty-five percent of India's internet users spent time on social media in 2012,[1] and this, too, is subject to unclear regulation under the amended IT Act's punitive Section 66. During the coverage period of this report, police arrested at least 11 people for social media posts—including tags, 'likes' and closed group comments—under the section's vague ban on annoying, offensive, or menacing messaging. Though most were swiftly bailed, the detentions—which often took place at night, involved defendants as young as 19, and in three cases in restive Jammu and Kashmir lasted 40 days—threatened the constitutionally-protected right to freedom of expression. Yet the IT Act's problematic provisions have yet to be reformed.

Security threats have also driven a frenzy of directives on surveillance in the past five years, including one ordering mobile providers to monitor all users' physical locations to within 50 meters, and others pushing international service providers that encrypt their users' communications to establish domestic servers that are subject to local law. In 2013, the government began transitioning to the secretive Central Monitoring System which will potentially empower a wide range of state agencies to access any electronic communication in India in real time, without service provider cooperation—though that cooperation is assured under license agreements. Surveillance requires no judicial oversight. While some of this activity might be justifiable, the lack of transparency surrounding the system, which was never reviewed by parliament, is concerning. The system's potential for abuse—already widely documented under the existing surveillance regime—is also disquieting, as is its inadequate legal framework. Outdated laws require case-by-case

[1] "25% Online Time Spent on Social Networks, 4 out of 5 Indians use Facebook," NDTV, August 20, 2012, http://bit.ly/PqAIGY.

clearance by high-level officials for wiretaps, for example, but are insufficient to regulate a system capable of mass location-based cellphone monitoring. Meanwhile, Indian citizens are surrendering more personal information—including biometric data, such as fingerprints—to electronic government databases than ever before. Yet no privacy law offers protection or redress if citizens' personal details or communications are improperly accessed. And while officials tout the centralized "electronic audit trail" the system creates each time it's used as a security feature, this data may itself be vulnerable to criminal infiltration.

As the country gears up for national elections in May 2014, these issues will become even more pressing. The main opposition Bharatiya Janata Party will take on the ruling Congress Party for control of the Lok Sabha, or lower house. The internet is already taking center stage, with both sides accusing the other of manipulating online discourse. There is no shortage of engaged civil actors countering the sometimes hostile online debate and advocating internet freedom. Whether the next government will be receptive remains to be seen.

OBSTACLES TO ACCESS

Internet usage in India continues to increase, with tens of millions of new users getting online each year. Internet penetration remains low by global standards, at 11 percent in December 2012, according to the Telecom Regulatory Authority of India (TRAI).[2] The International Telecommunications Union put penetration closer to 13 percent.[3] A pronounced urban-rural divide persists, and many people access the internet via cybercafes, as only 3 percent of households have an internet connection, according to recent census data.[4] A lack of local language content and applications also restricts penetration, though the situation is slowly improving.[5]

Overall mobile penetration was around 70 percent in 2012,[6] and mobile access is widespread, according to the Internet and Mobile Association of India, who reported in October 2012 that more than 90 percent of active urban internet users got online using a mobile device.[7] In January 2013, the government announced plans to allocate frequencies for a 4G network, which will further facilitate mobile web use.[8] Indians under 35 are 83 percent more likely to use mobile phones to go online at least once a week, compared to 55 percent of 50-64 year olds.[9]

[2] Telecom Regulatory Authority of India, "The Indian Telecom Services Performance Indicators April—June 2012," October 11, 2012, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator%20Reports%20-%20Jun-12.pdf
[3] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://bit.ly/14IlykM.
[4] Hari Kumar, "In Indian Homes, Phones and Electricity on Rise but Sanitation and Internet Lagging," *India Ink*, *New York Times*, March 14, 2012, http://nyti.ms/1bhij8L.
[5] T. Ramachandran, "Soon, the Web Will Have .Bharat in Local Languages," *The Hindu,* March 8, 2013, http://bit.ly/VLN5St.
[6] Mobile penetration registered a slight decline from 72 percent in 2011, a reporting discrepancy due to large scale service disconnections in 2012. International Telecommunication Union, "Mobile-cellular telephone subscriptions, 2000-2012."
[7] IAMAI, "i-Cube IAMAI Urban Report 2012," September 27, 2012, available at Read Where, http://bit.ly/17cPPMC.
[8] "700MHz Spectrum Auction for 4G Services in 2014: Sibal" *Business Line, The Hindu,* January 21, 2013, http://bit.ly/V18xOC.
[9] "74% of the People with Mobile Phone Access Internet At Least Once a Week," *Moneycontrol,* November 26, 2012, http://bit.ly/1fyB2Sv.

Information and communication technologies (ICTs) have helped make education and other services more accessible and inclusive in India.[10] However, infrastructural limitations and cost restrict access, especially to broadband connections, which have overtaken dial-up as the primary access technology.[11] In particular, operators are reluctant to invest in their own tower networks, and rely instead on third-party services.[12] Cable-landing stations, where submarine cables meet the mainland, often impose hefty fees for allowing ISP traffic to pass in or out. There are 10 such stations, but the market is dominated by two players, Bharti Airtel and Tata Communications, which have a combined 93 percent market share.[13] ISPs also prefer to be physically close to international gateways, like the one in Mumbai, where the high cost of real estate drives up hosting prices.

Partly as a result of these challenges, the top 10 ISPs serve 95 percent of the total internet subscriber base. Few of the 104 service providers authorized to offer broadband have been able to penetrate the market given the strong position occupied by state-owned BSNL and MTNL.[14] Private companies have met with more success in the mobile phone service market. The top 10 providers are Bharti Airtel, BSNL, Vodafone Essar, Reliance Communications, Idea Cellular, Tata Communications, Tata Teleservices, Aircel, MTNL, and Tata Teleservices (Maharashtra) Limited (TTML).[15] Licenses are issued following a bidding process, but launching a mobile phone service business in practice requires considerable financial clout and access to important government officials. In a decision highlighting such tendencies and other corrupt practices in the telecommunications sector, the Supreme Court in February 2012 canceled 122 licenses for 2G mobile phone services. The licenses had been sold at artificially low prices in 2008 to a small number of favored firms.[16]

Broadband speeds remain slow in India. Testing by the technology firm Akamai in December 2012 indicated that the average connection speed in India was only 1 Mbps, an improvement from early 2012, but still slow by international standards.[17]

The government sought to address this through a National Telecom Policy unveiled in May 2012, focused on providing affordable and quality telecommunication services in rural and remote areas.[18] By promoting sustained adoption of technology, the policy seeks to overcome developmental challenges including access to education, health care and employment.

---

[10] Pallavi Priyadarshini , "A Quantum Leap with Virtual Classrooms," *New Indian Express*, April 22, 2013, http://bit.ly/XYKCpI.
[11] Rudradeep Biswas, "Fixed Services in India To Reach Rs 240 Billion in 2012, 2% Growth from 2011," *Telecom Talk,* July 23, 2012, http://telecomtalk.info/fixed-services-in-india-to-reach-billion-2012growth-from2011/97402/.
[12] "Need to Strengthen Telecom Infrastructure: Rakesh Mittal," *The Hindu,* December 6, 2012, http://bit.ly/XuJ1GB.
[13] Avinash Celestine, "Bandwidth Prices: Why We Pay More For Internet Services," *Economic Times,* March 31, 2013, http://articles.economictimes.indiatimes.com/2013-03-31/news/38163288_1_isps-doug-madory-providers/2.
[14] Telecom Regulatory Authority of India, *The Indian Telecom Services Performance Indicators: January–March 2010* (New Delhi: TRAI, July 2010), http://www.trai.gov.in/WriteReadData/trai/upload/Reports/51/finalperformanceindicatorReport9agust.pdf.
[15] "10 Top Telecom Service Providers in India," *Rediff*, August 9, 2010, http://bit.ly/1bhixwA.
[16] Vikas Bajaj, "Indian Court Cancels Contentious Wireless Licenses," *New York Times*, February 2, 2012, ttp://nyti.ms/19NBCn0.
[17] "India's Broadband Hits Speed Bump," *Business Line*, *The Hindu,* January 24, 2013, http://bit.ly/UZvRxS.
[18] Shalini Singh, "New Telecom Policy Seeks to Abolish Roaming Charges," *The Hindu,* May 31, 2013, http://bit.ly/16JHCvj.

While the cost of devices and data access is an obstacle to many in India, surveys indicate that lack of electricity, low digital literacy, and limited English are also major impediments. Inadequate power, in particular, is a key road block to internet adoption and usage.[19] India's average peak power shortage—the amount of electricity it failed to generate when consumption reached a maximum—was 9 percent between 2007 and 2012.[20]

Other government projects will benefit the ICT sector, such as the National Optical Fiber Network, an ambitious two-year proposal to bring broadband speeds of 100 Mbps to rural districts.[21] However, though pilot broadband networks are being developed in three states, the project is not on schedule for completion within the two years allotted, which concludes in November 2013.[22]

In addition to these nationwide challenges, select states battling insurgencies or other security threats are even more isolated. In the central states colloquially known as the red corridor—so-named for the simmering Maoist insurgency concentrated in remote, tribal areas—ICT investment is limited both by the conflict and the fact that other basic needs, such as drinking water and access to healthcare, are still unmet in many communities.

The national government can impose limits on ICT usage during times of unrest. In August 2012, officials limited SMS messages to five per user per day for fifteen days in an attempt to control religious tensions in the northeast.[23] State governments also occasionally respond to security challenges, interfering with connectivity by implementing shutdowns. In February 2013, the state of Jammu and Kashmir temporarily shut down mobile internet service when a prominent militant leader was executed.[24] Select village councils also occasionally banned women from using mobile phones on moral grounds. Though they affected a tiny fraction of the population, at least three such highly localized bans were imposed during the coverage period, one in July in Uttar Pradesh, one in August in Rajasthan that applied only to girls under the age of 18, and one in Bihar in December.[25]

The TRAI is the main telecommunications regulatory body, with authority over ISPs and mobile phone service providers. Established by parliament in 1997, it functions as an independent agency, offering public consultations and other participatory decision-making processes. The TRAI is generally perceived as fair. The Ministry of Communications and Information Technology and the Ministry of Home Affairs also exercise control over several aspects of internet regulation.

Cybercafes, initially straightforward to open and operate, are now regulated under 2008 amendments to the IT Act, which define them as any facility or business offering public internet

[19] "India still out of the Net", Debjani Ghosh, March 24, 2013. The Hindu Business Line , http://bit.ly/14hfEuu.
[20] "India suffered 9 pc peak power shortage during 2007-12: Economic Survey," February 27, 2013, http://bit.ly/13j9zh0.
[21] "Indian Government to Spend Rs 368 Billion on IT in 2013: Gartner," Channel World, February 5, 2013, http://bit.ly/1azx31S.
[22] "Bharat Broadband to Manage Optical Fibre Project" Thomas K Thomas, *The Hindu*, February 23, 2013, http://bit.ly/15kheug.
[23] Madeline Earp, "India's Clumsy Internet Crackdown," *CPJ Blog,* August 22, 2012, http://bit.ly/SofdHr.
[24] Committee to Protect Journalists, "Kashmir Restricts Cable TV, Internet Service," February 11, 2013, http://bit.ly/14T8agV.
[25] Lakshmi Sarah, "Women Banned from Using Mobile Phones in Indian Villages," *Global Voices,* December 8, 2012, http://globalvoicesonline.org/2012/12/08/women-banned-from-using-mobile-phones-in-indian-villages/.

access.[26] Obtaining a license can require approval from multiple agencies, though reporters in the city of Bangalore could not locate a single authority responsible for issuing it.[27] Some states levy license fees.[28] Regulations from 2011 oblige cybercafes to register, censor and monitor customers;[29] critics noted these requirements went beyond the IT Act provisions which prescribed them.[30] A March 2012 notice mandated each institution register for an official number,[31] a process distinct from licensing that overlaps with existing state or municipal laws,[32] but without specifying the timeframe, penalties for non-compliance or even the identity of the "registration agency" responsible. Some owners, already facing loss of revenue due to projected growth in personal connections, found the requirements burdensome.[33] Enforcement varied significantly around the country.[34]

LIMITS ON CONTENT

The government ordered ISPs to block hundreds of websites and URLs in an effort to contain religious unrest in 2012; whole platforms were affected in Jammu and Kashmir. Misguided court orders also resulted in content blocks—164 websites became inaccessible in just two days in February 2013. Corporate actors battling piracy caused ISPs to block entire video- and file-sharing sites. Intermediaries who fail to satisfy personal complainants offended by their content are liable to criminal and civil penalties under harsh guidelines that were subject to legal challenges during the coverage period. But despite civil society protests, reform has yet to materialize, while legal proceedings against several global internet companies are ongoing. Right-wing "Internet Hindus," that some say have political backing, had a negative impact on the online space in the past year, bombarding opponents with hostile comments. Women reported particularly aggressive electronic threats. Yet citizens also embraced digital tools to promote street protests after a brutal rape and murder in December 2012, prompting some legislative reforms.

Political censorship is by no means pervasive in India. It has increased, however, since a 2008 amendment to the IT Act granted the government power to block any content in the interests of defense, national security, sovereignty, friendly relations with foreign states, and public order.[35] The OpenNet Initiative reported no filtering of political and social content in India in 2007,[36] but

[26] Department of Electronics and Information Technology, "Information Technology Act," http://bit.ly/STh7NX.
[27] H.M. Chaithanya Swamy, "DNA special: Number of Licensed Cyber Cafes in City? Zero," *DNA India*, October 15, 2012, http://www.dnaindia.com/bangalore/1752626/report-dna-special-number-of-licensed-cyber-cafes-in-city-zero.
[28] "Cyber Cafes in Pune to Pay Licence Fees," *DNA India*, June 25, 2011, http://bit.ly/19dZZcD.
[29] Department of Information Technology, "Information Technology (Guidelines for Cyber Cafe) Rules, 2011," http://deity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.
[30] Bhairav Acharya, "Comments on the Information Technology (Guidelines for Cyber Cafe) Rules, 2011," Center for Information and Society, March 31, 2013, http://bit.ly/13KCBY5.
[31] Department of Information Technology, "Notification G.S.R. 153(E)," http://bit.ly/1dPHjoM.
[32] Bhairav Acharya, "Comments on the Information Technology (Guidelines for Cyber Cafe) Rules;" Debabrata Mohapatra, "Online Registration for Cyber Cafes, *Times of India,* May 8, 2013, http://bit.ly/1fyBDnk.
[33] Bhuvan Bagga, "Delhi Government to Watch Over Cyber Cafes," *India Today,* August 22, 2012, http://bit.ly/QopVsK.
[34] Sayantanee Choudhury, "Cybercafe Owners in Patna Violate Rules, *Times of India,* July 23, 2013, http://bit.ly/19K4QnT; "Police Vigilant Against Shoddy Cyber Cafes," *Times of India,* January 30, 2013, http://bit.ly/YnTOQp.
[35] Department of Electronics and Information Technology, "Information Technology Act."
[36] OpenNet Initiative, "India," 2007, https://opennet.net/sites/opennet.net/files/india.pdf.

selective blocking of both in 2012, while transparency surrounding the blocking process declined.[37] Religious and political extremist commentary was consistently targeted. Troublingly, "websites with information on human rights in India, internet tools such as proxies, and content related to free expression" were also selectively filtered. Blocks on pornography were fewer than those affecting other kinds of information.[38]

Though the 2008 amendment subjects the government's blocking authority to "procedure and safeguards," the 2009 rules which outlined these processes are inadequate, and not always followed in practice.[39] Service providers block websites at the behest of a committee of representatives from the ministries of law, justice, home affairs, information and broadcasting, and the cybercrime authority, the Indian Computer Emergency Response Team (CERT-In), which operates under the Department of Information Technology, often abbreviated as DIT. Citizens can't personally contact this group, but officials or police can submit vetted complaints on their behalf to the committee, who must give the person or intermediary who posted the contested information 48 hours to respond. Whether they do or not, the committee assesses the complaint, and sends those it considers legitimate to the IT department secretary for approval before directing service providers to implement blocks. The incumbent secretary is J. Satyanarayana.[40] In emergencies, he has the power to issue a temporary order directly if the committee subsequently reviews it within 48 hours. A review committee is expected to review all blocking decisions made under the law every other month.

Unfortunately, public misperceptions about this process undermine it in practice. Most news reports cite CERT-In as the authority behind website blocking, and the governmental department responsible as the Department of Telecom (DOT) based on earlier iterations of the act.[41] In fact, DOT has relinquished this authority to DIT, a subtle change barely clarified by the DIT's re-designation as the Department of Electronics and Information Technology (DEITY) in April 2012.[42] Meanwhile, CERT-In's power to authorize blocks passed to the committee outlined above. That body's name under rule 8(4) for section 69A of the 2008 act is "committee for examination of requests"—which can also be abbreviated as CER.[43] The imprecision surrounding these two entities is not just from the acronyms. Both CERT-In and CER are headed by the same person, Gulshan Rai.[44] The fact that he is empowered to sanction ISPs to block content is based on his role as the "designated officer" under the 2009 rules, rather than his position as director-general of the institution which manages cybercrime—though that institution, CERT-In, can issue requests to

[37] OpenNet Initiative, "India."
[38] OpenNet Initiative, "India."
[39] Department of Electronics and Information Technology, "Notification of Rules under Section 52, 54, 69, 69A, 69B," October 27, 2009, http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/Itrules301009.pdf.
[40] Department of Electronics and Information Technology, "People and Offices," http://deity.gov.in/content/people-and-offices.
[41] Department of Information Technology, "Ministerial Order on Blocking of Websites," July 7, 2003, *The Information Technology Act 2000,* (New Delhi: Universal Law Publishing, 2011) 156, http://bit.ly/1dPEKmD.
[42] "Department of Information Technology Renamed as Department of Electronics and IT," Press Trust of India via NDTV, April 18, 2012, http://bit.ly/HYXfoy.
[43] For the CER, see Pranesh Prakash, "DIT's Response to RTI on Website Blocking," Center for Information and Society, April 7, 2011, http://cis-india.org/internet-governance/blog/rti-response-dit-blocking. For pre-2008 rules, see;
[44] Sahil Makkar, "Gulshan Rai | We Believe in the Freedom of Speech and Expression," January 31, 2012, http://bit.ly/TtaW28. Rai was named India's first national cyber security coordinator in May 2013. It's not clear how this will affect his other roles. See, "Gulshan Rai to be first National Cyber Security Coordinator," *Indian Express,* May 10, 2013, http://bit.ly/148cJBC.

takedown or delete illegal content. This introduces further ambiguity, but regardless of how the authority is distributed between these groups, they all operate under the powerful Minister of Communications and Information Technology, Kapal Sibal, whose cabinet portfolio was extended in May 2013 to include the law ministry.[45] Popular criticism that content controls are too centralized may focus on the wrong institutions, but the underlying concern is often legitimate.

As in many democracies, the Indian judiciary is an independent arbiter of content disputes, and the government approves blocking orders submitted by the courts automatically. Regrettably, this gives local courts—who are often subject to social and political pressure, lack experience with internet issues, and can make rulings *ex parte,* meaning that they only hear one side of the case—considerable power to curb content. In some cases, service providers complied with blocking orders sent by lawyers informing them of a court decision, instead of an official notice, introducing additional scope for abuse.[46] In February 2013, Rai's committee instructed ISPs to block more than 70 URLs criticizing the Indian Institute of Planning and Management, a private business school, and its founder Arindam Chaudhuri, on the order of a district court in Madhya Pradesh, which was hearing a defamation suit filed by the institute.[47] One of the websites targeted belonged to the University Grants Commission,[48] which accredits higher educational institutions and refuses to recognize Chaudhuri's right to award degrees, a decision he characterized as defamatory.[49] Dozens of news articles reporting on the dispute, by *Outlook* magazine, the *Times of India,* the *Wall Street Journal* and the satirical website *fakingnews,* among others, were also blocked.[50] Since court orders are meant to be stayed by other courts, several news reports said the government would have to appeal against blocking that its own agencies had facilitated—one whose principle victim, the Commission, was a statutory body of the Indian government.[51]

Since 2011, a handful of higher courts have blocked content relating to copyright violations through particularly broad John Doe—or in India, Ashok Kumar—orders, which don't name a defendant.[52] These are not only pre-emptive—passed to prevent future violations of a movie that is not yet released—they are also misused by entertainment companies to make ISPs block entire platforms, whether or not they are hosting pirated material.[53] This was demonstrated in May 2012 when as many as 38 ISPs completely blocked a range of platforms, ranging from video site Vimeo to file-sharing websites; some reports said they were inaccessible for as long as a month.[54] The New Delhi-

[45] Anirudh Wadhwa, "A To-Do List for the New Law Minister," May 16, 2013, http://bit.ly/182ul3Y.
[46] Shalini Singh, "164 Items Blocked Online in Just 2 Days, Mostly on Court Orders," *The Hindu*, February 22, 2013, http://www.thehindu.com/news/national/164-items-blocked-online-in-just-2-days-mostly-on-court-orders/article4439917.ece.
[47] "Directed by Court, DoT Moves to Block 73 URLs Critical of IIPM," *Times of India,* February 15, 2013, http://bit.ly/XnqrPz.
[48] University Grants Commission, "Genesis," http://www.ugc.ac.in/page/Genesis.aspx.
[49] Urmi Goswami, "UGC Again Warns Students About IIPM," February 19, 2013, http://bit.ly/1hbu1CT.
[50] Danish Raza, "Glad Defamatory Links with Malicious Interests Removed: Arindam Chaudhuri," *Firstpost,* February 18, 2013, http://bit.ly/1bhiWiT.
[51] Shalini Singh, "164 Items Blocked Online in Just 2 Days;" "Govt Will Challenge Order to Block 78 Web Pages on IIPM," *Times of India,* February 20, 2013, http://bit.ly/ZvS63I.
[52] Kian Ganz, "[Update: Download Gangs of Wasseypur Order] Bombay HC Passes First Anti-piracy John Doe Order, as Law Firms Commoditise the New Vertical," *Legally India,* June 15, 2012, http://bit.ly/KIibkI.
[53] Apar Gupta, "Ashok Kumar is a Habitual Offender," *India Law and Technology Blog,* May 18, 2013, http://bit.ly/KsTdoC; Abhik Majumdar, "What's with this Kolaveri about John Doe Injunctions?" *Law and Other Things,* June 3, 2012, http://bit.ly/164cgUk.
[54] Anupam Saxena, "ISP Wise List Of Blocked Sites #IndiaBlocks," *Medianama,* May 17, 2012, http://bit.ly/JI5wlr; Software Freedom Law Center, "When Copyright Tramples on the Right to Freedom of Expression," July 2, 2012, http://bit.ly/19e0GCF.

based Software Freedom Law Center said Copyright Labs, an agency representing a movie production company, had interpreted an April court order from the Madras High Court in Chennai, state capital of Tamil Nadu, to allow absolute blocking, and that ISPs had complied; the court subsequently clarified that the order was only intended to affect specific URLs, not whole platforms.[55] Experts hope this clarification will encourage ISPs to contest widespread orders,[56] though some of the sites remained inaccessible even after the court's statement, and some news reports said more than 20 other John Doe orders issued by courts around the country are still open to wrongful implementation.[57]

These processes are not transparent for internet users, who are not informed of blocks until they encounter an error message—the 2008 IT amendment actually prohibits blocking complaints and decisions being made public. In some cases, error notifications cite a generic technical fault; in others, they add to confusion by citing an order from the DOT instead of DEITY. (Asked about one of these notifications, the DOT clarified that it was not responsible.[58]) In 2011, the Bangalore-based Center for Internet and Society obtained a list of 11 blocks via a freedom of information request, which it matched to 11 judicial orders.[59] Even then, there was no definitive way of confirming if the block came through via a court or DEITY—and consequently, no clear avenue for appeal. Results can even vary by ISP. Many rely on domain name system (DNS) tampering to stop users from visiting specific URLs or domains. In theory, this allows ISPs to interrupt the connection between an individual blog page and the person trying to retrieve it, and should not affect entire platforms. In practice, blocks are frequently overbroad, making it impossible to know which websites were targeted and which fell victim to collateral blocking.[60] In late 2012, the Toronto-based research group Citizen Lab reported three ISPs in India using PacketShaper technology, which allows more sophisticated blocking and throttling.[61] In April 2013, the *Economic Times,* citing minutes from a Home Ministry meeting, said the government planned to ask ISPs to segregate IP addresses by state to allow content blocking and monitoring on a regional basis.[62]

More nuanced filtering might seem like a welcome development in light of the court orders outlined above. In reality, it is cause for concern, given the disproportionate number of blocks ordered in the past year. In addition to the examples already considered, several hundred more pages were blocked based on communal or religious unrest. In August 2012, tensions between Muslims and non-Muslims in northeastern states including Assam, Karnataka, Tamil Nadu, and Maharashtra caused thousands to flee the region and sparked violence in cities around the country.

---

[55] Software Freedom Law Center, "When Copyright Tramples on the Right to Freedom of Expression."
[56] Nikhil Pahwa, "No More John Doe Orders? Indian ISPs Get Court Order For Specificity In URL Blocks," *Medianama*, June 20, 2012, http://www.medianama.com/2012/06/223-no-more-john-doe-orders-indian-isps-get-court-order-for-specificity-in-urls/.
[57] Prasad Krishna, "Reply to RTI Application on Blocking of Website and Rule 419A of Indian Telegraph Rules, 1951," Center for Information and Society, March 21, 2013, http://bit.ly/16JEbVd.
[58] Kul Bhushan, "Anonymous Takes Down IIPM Sites After DoT Blocks 'Defamatory URLs,'" *Think Digit,* February 18, 2013, http://www.thinkdigit.com/Internet/Anonymous-takes-down-IIPM-sites-after-DoT_13515.html.
[59] Pranesh Prakash, "DIT's Response to RTI on Website Blocking," Center for Internet and Society, April 7, 2011, http://cisindia.org/internet-governance/blog/rti-response-dit-blocking.
[60] OpenNet Initiative, "India," 2012.
[61] T. Ramachandran, "Indian ISPs Too Resorting to Censorship," *The Hindu,* February 9, 2013, http://bit.ly/1bhjIBC.
[62] Joji Thomas Philip, "Net Telephony Providers Will be Asked to Set Up Servers in India," *Economic Times,* May 20, 2013, http://bit.ly/15BHST3.

The government said that online hate speech, including falsified images of Muslims suffering violent attacks, was deliberately circulated to exacerbate the violence, and ordered blocks on at least 309 specific online items, a figure which was leaked to the press.[63] That number, which did not differentiate between blocks on entire platforms or individual URLs, was probably conservative, and the blocking was widely censured as indiscriminate.

Instead of combatting inflammatory content, the government's action disabled many objective sources of information, such as the Twitter handles of New Delhi-based journalists Shiv Aroor and Kanchan Gupta, who used their accounts to report on the unrest. News reports said that only a fifth of sites targeted mentioned the northeast, which undermined public trust in the action.[64] Officials accused Pakistani authorities of orchestrating online hate campaigns, adding a possible political motive for blocking. Other content, including a handful of political Twitter accounts such as @DrYumYumSingh, which spoofs Prime Minister Manmohan Singh, became inaccessible at the same time, although they were not on the leaked list, leading many to wonder if political critics were being singled out as well.[65] Other reports said Twitter had removed some accounts for violating user agreements.[66] In February 2013, the Press Trust of India said a "high-level government committee" had decreed that 306 blocks on Twitter accounts implemented during this period were lawful, while four were not. It's not clear which accounts were affected or whether this number related to the 309 items described above, most of which were not hosted by Twitter.[67]

Over 240 further URLs were reportedly blocked in November 2012 in relation to the anti-Islamic "Innocence of Muslims" video uploaded in the United States in September, which prompted protests by Muslim communities throughout Asia. Minister Sibal publicly announced the blocks, and said more were forthcoming.[68] Google separately reported having blocked access from India to several YouTube videos related to the "Innocence of Muslims" video, based on government request.[69]

Restrictions were more severe in the Muslim-majority state of Jammu and Kashmir, where militant groups seek political autonomy or union with Pakistan. After "Innocence of Muslims" caused mass protests in September 2012, residents of the state reported the blocking of several social networks, including Facebook and YouTube, as well as some disruption to e-mail, search engines, and Blackberry phone service; other mobile providers also blocked internet access altogether.[70] News reports said the state government ordered these shutdowns under Section 5(2) of the Indian Telegraph Act 1885, which shouldn't be possible, because it only pertains to the emergency

[63] Pranesh Prakash, "Analysing Latest List of Blocked Sites (Communalism & Rioting Edition)," Center for Internet and Society, August 22, 2012, http://cis-india.org/internet-governance/blog/analysing-blocked-sites-riots-communalism.
[64] Madeline Earp, "India's Clumsy Internet Crackdown."
[65] Pranesh Prakash, "Analysing Latest List of Blocked Sites."
[66] Kul Bhushan, "Facebook, Google to Help India Remove Hate Content; Twitter Blocks Fake Accounts," *Think Digit,* August 22, 2012, http://www.thinkdigit.com/Internet/Facebook-Google-to-help-India-remove-hate_10526.html.
[67] "Government Panel Okays Blocking of 306 Twitter Accounts," Press Trust of India, via *Times of India,* February 6, 2013, http://bit.ly/WSYZst.
[68] "Government Blocks 240 Weblinks Related to Provocative Film," Press Trust of India via NDTV, November 1, 2012, http://gadgets.ndtv.com/internet/news/government-blocks-240-weblinks-related-to-provocative-film-287053.
[69] Google, "India," July to December 2012, in *Transparency Report,* http://bit.ly/1biQu3o.
[70] "YouTube, Facebook Blocked on Mobile," *Greater Kashmir,* September 30 , 2012, http://bit.ly/QDF7Hq.

interception of electronic communications.[71] But while the state information and technology minister denied the order,[72] at least two service providers confirmed that there was a state-wide ban on Facebook and YouTube.[73] Service was subsequently restored. On February 14 and 15, however, DEITY ordered national blocks on more than 80 individual YouTube and Facebook pages after a Kashmiri sentenced to death for assisting with a Pakistani terrorist attack on India's parliament in 2001 was executed without warning or, critics said, due process.[74] *The Hindu* newspaper reported that the block was based on a court order procured by Jammu and Kashmir police.[75] Since these were implemented at the same time as the ones involving the business institute described above, Indian ISPs blocked 164 pages based on court orders in the space of two days, some due to a highly politicized conflict, others from private, commercial interests.

Administrative requests requiring service providers to take down content also spiked during these incidents. Facebook cooperated with the government during the northeastern unrest, though it was not clear how many pages were taken down as a result.[76] Twitter was asked to remove 20 accounts, but the extent of their cooperation was also unclear.[77] Google reported that removal requests from India in the second half of 2012 increased 90 percent compared to the first part of the year, notably from CERT-In during the northeastern riots, but the company did not comply with all.[78] While international companies often independently assess deletion requests to see if the flagged content violates local law or user guidelines before complying, domestic companies may be less discriminating. In March 2013, the Software Freedom Law Center said police ordered a web portal to delete an allegedly defamatory article under Section 91 of the penal code, which allows them to request information for the purposes of an ongoing investigation—even though the section does not provide for deletion of online content and is not applicable in defamation investigations. It was not an isolated incidence, the Center reported.[79]

Intermediaries are pressured into policing content by multiple actors. Both local and overseas companies are vulnerable to criminal prosecution if they fail to comply with complaints about content—not just from officials, but from anyone in India. The 2000 IT amendment made them liable for illegal content posted by third parties, though Section 79 of the 2008 amendment introduced some protections for companies and their customers.[80] In April 2011, however, Information Technology (Intermediaries Guidelines) Rules implementing the act undermined these protections—omitting, for example, any requirement to notify the person responsible for the censored material.[81] The guidelines, which cover internet and mobile service providers as well as

[71] Snehashish Ghosh, "Indian Telegraph Act, 1885," Center for Internet and Society, March 15, 2013, http://bit.ly/15Cdzq0.
[72] "Youtube and Facebook 'Blocked' in Kashmir," Al Jazeera, October 2, 2012, http://aje.me/PSPJjK.
[73] Kul Bhushan, "YouTube, Facebook Banned in Kashmir: Reports," *Think Digit,* October 1, 2012, http://bit.ly/W6Z4XA.
[74] Arundhati Roy, "Afzal Guru's Hanging Has Created a Dangerously Radioactive Political Fallout," *Guardian,* February 18, 2013, http://www.theguardian.com/commentisfree/2013/feb/18/afzal-guru-dangerous-political-fallout.
[75] Shalini Singh, "164 Items Blocked Online in Just 2 Days."
[76] "Working With Government to Remove Hateful Content: Facebook," Indo-Asian News Service via NDTV, August 21, 2012, http://www.ndtv.com/article/india/working-with-government-to-remove-hateful-content-facebook-257603.
[77] "India Faces Twitter Backlash over Internet Clampdown," Reuters, August 24, 2012, http://reut.rs/O8kGha.
[78] Google, "India."
[79] "S.91 of CrPC – the Omnipotent Provision?" Software Freedom Law Center, March 19, 2013, http://bit.ly/18zxqdo.
[80] Erica Newland, "Shielding the Messengers: Internet on Trial in India," Center for Democracy and Technology, March 20, 2012, https://www.cdt.org/blogs/erica-newland/2003shielding-messengers-internet-trial-india.
[81] Vikas Bajaj, "India Puts Tight Leash on Internet Free Speech," *New York Times*, April 27, 2011, http://nyti.ms/15BHZ0P.

web hosts, search engines and social networks, require them to disable access to offensive content within 36 hours of discovering it or receiving a complaint, either by blocking it or taking it down, or face prosecution leading to possible fines or jail terms.[82] A March 2013 clarification stated that acknowledging a complaint within 36 hours was sufficient if the content was disabled within a month.[83] This confused the process further, while doing nothing to address other glaring oversights.[84]

While the CER committee explicitly limited the power of private complainants, the Guidelines opened the floodgates. Any individual can complain to a service provider about content that they deem, for example, defamatory, disparaging, harmful, blasphemous, pornographic, promoting gambling or infringing proprietary rights.[85] None of these categories are defined. Experts say many violate the constitution by restricting legal speech—watching pornography, for example, is legal in India, and there are no limits on "disparaging,"[86]—a failing criticized by a parliamentary committee in March 2013.[87] Critics also objected to the 2011 rules telling cybercafes to stop users from accessing pornography on similar grounds; they were encouraged to install filtering software, although it's not clear how many complied.[88]

May 2012 amendments to the Copyright Act limited liability for intermediaries such as search engines that link to illegally-copied material, but mandated that they disable public access for 21 days within 36 hours of receiving written notice from the copyright holder, pending a court order to block or remove the link.[89] Rules clarifying the amendment in March 2013 appeared to give intermediaries power to assess the legitimacy of the notice from the copyright holder and refuse to comply, but critics said the language was too vague to restore the balance between the complainant and the intermediary.[90]

Civil society has been active in opposing the Intermediary Guidelines. In tests, the Center for Internet and Society demonstrated they could be used to render thousands of innocuous posts

---

[82] Ujwala Uppaluri, "Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011," Center for Internet and Society, July 16, 2012, http://bit.ly/1fRtyI2; Amol Sharma, "Is India Ignoring its own Internet Protections?" *Wall Street Journal,* January 16, 2012, http://on.wsj.com/xTjSiG.

[83] Department of Electronics and Information Technology, "Clarification on The Information Technology (Intermediary Guidelines) Rules, 2011 under section 79 of the Information Technology Act, 2000," March 18, 2013, http://bit.ly/17cRimc.

[84] B. Singh, "Clarification On The Information Technology (Intermediary Guidelines) Rules, 2011 Under Section 79 Of The Information Technology Act, 2000," Center Of Excellence For Cyber Security Research And Development In India, April 4, 2013, http://perry4law.org/cecsrdi/?p=621.

[85] Ministry of Communications and Information Technology, "Information Technology Act, 2000," April 11, 2011, http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf.

[86] Ujwala Uppaluri, "Constitutional Analysis."

[87] Ishan Srivastava, "Parliament Panel Blasts Govt Over Ambiguous Internet Laws," *Times of India,* March 28, 2013, http://articles.timesofindia.indiatimes.com/2013-03-28/internet/38098800_1_rules-self-regulation-pranesh-prakash.

[88] Javed Anwer, "No Access to Pornography in Cyber Cafes, Declare New Rules," *Times of India,* April 26, 2011, http://articles.timesofindia.indiatimes.com/2011-04-26/internet/29474462_1_cyber-cafe-cafe-owners-cubicles.

[89] Specifically, any providers offering "transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public" through "links, access or integration." See, Pranesh Prakash, "Analysis of the Copyright (Amendment) Bill 2012," Center for Internet and Society, May 23, 2012, http://bit.ly/JSDMLg; Ministry of Law and Justice, "Copyright (Amendment) Act 2012," June 7, 2012, http://bit.ly/Kt1vlQ.

[90] Chaitanya Ramachandran, "Guest Post: A Look at the New Notice and Takedown Regime Under the Copyright Rules, 2013," *Spicy IP,* April 29, 2013, http://bit.ly/16zSzWf; Ministry of Human Resource Development, "Copyright Rules 2013," March 14, 2013, http://bit.ly/YrhCS5.

inaccessible.[91] Legal challenges are pending, including one submitted by a cyberlaw expert in Kerala in early 2012, who called them unconstitutional.[92] In April 2013, the Supreme Court agreed to reexamine them based on a petition by a consumer affairs website.[93] The site, MouthShut, which hosts user-generated reviews of products and services, said it had faced "hundreds of legal notices, cybercrime complaints and defamation cases" based on the rules, as well as calls from police officers to delete negative reviews.[94] The case is still pending.[95]

Other companies have been hit with criminal and civil charges even when there was no evidence that they were aware of the offending content, when they subsequently deleted it, or when they had no control over user-generated content hosted overseas by parent companies. Some of Google's mapping practices left the company's representatives liable for 3 years imprisonment, according to one expert.[96] In December 2011, journalist Vinay Rai filed a criminal complaint against 21 internet firms, including Facebook and Google, for hosting content he considered offensive, such as images depicting religious figures.[97] The charges invoked articles of the penal code that ban the sale of offensive material, including to minors, and punish criminal conspiracy.[98] Even under the broad auspices of the Intermediary Guidelines, the case had no foundation, because there was no evidence he had complained about the images. Some subsequently blocked the content, and others had charges dismissed on technical grounds,[99] but proceedings involving 11 companies were ongoing in May 2013.[100] Civil content complaints are also being heard by Indian courts, including one against several internet firms filed by Islamic scholar Aijaz Arshad Qasmi filed in December 2011.[101] Meanwhile, Facebook was subject to a police complaint in November 2012 for disabling an activist's account. The activist, based in Uttar Pradesh, said the closure was triggered by complaints from other internet users made in retaliation for his work.[102]

Individuals, as well as companies, are liable for third-party generated content. In 2009, the Supreme Court declined to quash a lawsuit against a student relating to third party comments in a group he created on Google's social network Orkut, rendering bloggers liable to civil or criminal

[91] Kirsty Hughes, "Internet Freedom in India—Open to Debate ," Index on Censorship, January 22, 2013, http://bit.ly/Xwxtxz.
[92] Prachi Shrivastava, "Read Parts of First Writ Challenging Censorious IT Act Intermediaries Rules in Kerala," *Legally India*, March 6, 2012, http://bit.ly/w4J7AN.
[93] Ashok Bindra, "Supreme Court of India to Examine the Validity of 2011 IT Rules Act," *TMC Net,* May 1, 2013, http://www.tmcnet.com/topics/articles/2013/05/01/336479-supreme-court-india-examine-validity-2011-it-rules.htm.
[94] Nikhil Pahwa, "MouthShut Challenges IT Rules In The Supreme Court Of India," *Medianama,* April 23, 2013, http://www.medianama.com/2013/04/223-mouthshut-it-rules-supreme-court-of-india/.
[95] "Stop Crying Wolf: Just Wait and Watch!" Software Freedom Law Center, August 23, 2013, http://bit.ly/12rUOqJ.
[96] S. Ronendra Singh, "Google Should Follow Indian Laws, say Rival Mapmakers," *The Hindu,* April 7, 2013, http://bit.ly/Y6hnQV.
[97] Amol Sharma, "Facebook, Google to Stand Trial in India," *Wall Street Journal*, March 13, 2012, http://on.wsj.com/x7z1ZT.
[98] Rishi Majumder, "The War on the Web is a War on Us," *Tehelka,* February 18, 2012, http://bit.ly/1bhno11.
[99] Pratap Patnaik and Bibhudatta Pradhan, "Indian Court Quashes Charges Against Microsoft on Content," Bloomberg, March 19, 2012, http://bloom.bg/x8qhvq; Kul Bhushan, "Web Censorship: Delhi Court Drops Google India, 7 Others From Lawsuit," April 13, 2012, http://www.thinkdigit.com/Internet/Web-censorship-Delhi-court-drops-Google-India_9279.html.
[100] "US Snubs India Over Case Against Google, Facebook," Press Trust of India via NDTV, May 3, 2013, http://bit.ly/104kAkV.
[101] Kul Bhushan, "Web Censorship Row: Delhi Court to Summon Facebook Via E-mail," *Think Digit,* April 20, 2013, http://www.thinkdigit.com/Internet/Web-censorship-row-Delhi-court-to-summon_9349.html.
[102] Prasant Naidu, Lucknow Lawyer Files FIR Against Facebook For Disabling His Account," *Lighthouse Insights,* November 20, 2012, http://lighthouseinsights.in/lucknow-lawyer-files-fir-against-facebook-for-disabling-his-account.html.

prosecution for comments posted by third parties.[103] No prosecutions have been reported since this ruling, but it may have encouraged self-censorship. Online journalists and bloggers approach certain topics with caution, including religion, communalism, the corporate-government nexus, links between government and organized crime, Kashmiri separatism, and hostile rhetoric from Pakistan.

The central authorities are not known to systematically employ progovernment commentators, but other factors exert a manipulative influence on digital discourse. Paid news, or "advertorials," are common in the traditional media in India, from unclear disclosure of paid endorsements to bribery and other kickbacks for coverage. In mid-2013, Indian digital media website *Medianama* reported this phenomenon had increased on digital platforms in the past three years.[104]

Of greater concern for political and social expression are the estimated 20,000 nationalistic "Internet Hindus" trolling websites to attack those who discuss sensitive topics online, some posting up to 300 comments a day.[105] While far from the only group with an agenda on the Indian web, they are "so numerous, so committed and can appear so organized" that they may have a disproportionate impact on legislators. Commentators note that official content regulation has occurred in step with the increase of aggressive, partisan debates being driven by national events like the 2008 terror attacks.[106] Some go further, tying the activity directly to the opposition Bharatiya Janata Party, who acknowledged operating 100 paid social media campaigners posting under multiple IDs in early 2013, but denied allegations that they "flood the internet with right-wing propaganda."[107] The ruling Congress party launched a rival online campaign in April but denied compensating participants. Internet users in India occasionally accuse individuals or media in Pakistan of manipulating discussions about the disputed Kashmir valley in domestic online forums, and some insurgent groups have also used digital tools to spread propaganda.[108] There is plenty of outspoken pushback against politicized trolling, but others may be deterred from expressing their views.

Many traditionally marginalized groups benefit from internet access to share information and connect with others, including Dalits, who are at the bottom of the Hindu caste system.[109] While rural and impoverished communities are underserved by internet access, mobile initiatives like CGNet encourage villagers to report news and information to the moderators of a central online

[103] Marshall Kirkpatrick, "Orkut User Loses in Indian Supreme Court," *ReadWrite,* February 24, 2009, http://readwrite.com/2009/02/24/orkut_user_loses_in_indian_sup#awesm=~ogYvZHQ5ELvHTf.
[104] Nikhil Pahwa, "Our Views On Paid News In Digital Media & Blogs In India," *Medianama,* June 21, 2013, http://bit.ly/17r8VRE.
[105] Jason Overdorf, "India: Meet the 'Internet Hindus,'" *Global Post,* June 18, 2012, http://bit.ly/Pac0bP.
[106] Ramachandra Guha, "Who Milks this Cow?" *Outlook,* November 19, 2012, http://bit.ly/Z25RV0.
[107] Kunal Pradhan, "Election #2014: As Cyber War Rooms Get Battle-Ready, BJP and Congress are Reaching Out to a New Constituency Spread Across Social Media," *India Today,* February 8, 2013, http://bit.ly/16DM9Rv.
[108] Rashmi Drolia, Chhattisgarh Cyber Police asks Facebook to Shut Down Maoist Page," *Times of India,* June 1, 2013, http://articles.timesofindia.indiatimes.com/2013-06-01/india/39673868_1_facebook-page-facebook-authorities-profile.
[109] Pramod K. Nayar, "The Digital Dalit: Subalternity And Cyberspace," *The Sri Lanka Journal of the Humanities 37* (1&2) 2011, available at Academia, http://www.academia.edu/1482588/THE_DIGITAL_DALIT_SUBALTERNITY_AND_CYBERSPACE.

forum via calls or SMS.[110] Begun in Chhattisgarh, the project has moved to nearby Madhya Pradesh and receives around 500 reports a day.[111]

Online activists are also vocal on internet freedom issues, such as the content regulation that followed the northeastern riots.[112] Charges against social network users under the IT Act's vague Section 66 also sparked strong public opposition, though these have yet to see effective results (see Violations of User Rights). Human rights issues spurred online actions during the coverage period, particularly in the aftermath of a shocking gang rape on December 16, 2012. Inspired by the success of a 2011 social media movement in support of anti-corruption campaigner Anna Hazare,[113] a number of social media campaigns became part of what some dubbed the *nirbhaya* ("fearless one") movement, helping propel women's rights onto the public agenda.[114] This helped drive public protests, which achieved some results when the government introduced two new pieces of legislation that parliament ratified in February and April, strengthening the legal penalties for sexual harassment.[115] However, others called for tighter regulation of online pornography as the driver behind the rise in sexual assaults against women.[116] The debate has yet to improve the online environment for women. Many say authorities are reluctant to recognize online threats and harassment as violations of the IT Act.[117] An all-female rock band in the Kashmir valley disbanded after online threats from radical religious groups.[118]

VIOLATIONS OF USER RIGHTS

Police around the country abused laws to threaten internet users during the coverage period. They were particularly active in Maharastra state, where blogger and cartoonist Aseem Trivedi was held for several days on sedition charges, and five people were detained for social media posts, sometimes in the middle of the night. At least eight more were charged for social media activity in other states under Section 66 of the IT Act, including three men in Jammu and Kashmir who were held for 40 days. Civil society opposition has yet to result in significant reform. Government surveillance, which requires no judicial oversight, is transitioning to a secretive, multi-million dollar Central Monitoring System, allowing officials to retrieve content and metadata from any electronic communication in India in real time, without the help of service providers. Much of the architecture of the system is already in place, and is scheduled to be fully operational by 2014,

[110] Preeti Mudliar, Jonathan Donner, and William Thies, "Emergent Practices Around CGNet Swara, A Voice Forum for Citizen Journalism in Rural India," Microsoft Research, March 2012, http://research.microsoft.com/apps/pubs/?id=156562.
[111] Elisa Tinsley, "In Rural India, a Hub for Tech, Mobile Innovation Gives Isolated People a Voice," International Journalists Network, September 5, 2013, http://ijnet.org/blog/rural-india-hub-tech-mobile-innovation-gives-isolated-people-voice.
[112] "Govt vs Twitter Provokes Angry Reactions, Hashtags like Emergency 2012," NDTV, August 23, 2012, http://bit.ly/OyHngx.
[113] Jaimon Joseph, "How Anna Hazare Became a Media Phenomenon," IBN Live, August 22, 2011, http://bit.ly/16JFofn.
[114] Shoma Chaudhary, "The Girl Who Fired an Outcry in India," *Daily Beast,* April 3, 2013, http://thebea.st/11V6lMR; Swasti Chatterjee, "8 Months After the Nirbhaya Case, Where Do We Stand?" *Times of India,* August 25, 2013, http://bit.ly/19NCqs5.
[115] Nagendra Sharma, "Two Bills, Two Punishments for Sexual Harassment," *Hindustan Times*, April 8, 2013, http://www.hindustantimes.com/India-news/NewDelhi/2-bills-2-punishments-for-sexual-harassment/Article1-1038995.aspx.
[116] Neha Thirani Bagri and Heather Timmons, "India Considers Banning Pornography as Reported Sexual Assault Rises," *New York Times,* April 22, 2013, http://nyti.ms/15CasOX.
[117] Divya Arya, "Why Are Indian Women Being Attacked on Social Media?" BBC, May 7, 2013, http://bbc.in/109OXot.
[118] "Kashmir Girls Pursue Career in Music Amid Fatwa," *Hindustan Times*, May 2, 2013, http://bit.ly/18eiNeJ.

despite never having been reviewed by parliament. Meanwhile, a privacy law proposed by experts in October 2012 has yet to be drafted.

Article 19 (1) of the Indian constitution protects freedom of speech and expression.[119] ICT usage is governed primarily by the Telegraph Act, the penal code, the code of criminal procedure, and the IT Act. Section 66 of the 2008 IT amendment punishes ill-defined "offensive," "menacing," or "false" electronic messages that cheat, deceive, mislead, or annoy, with jail terms of up to three years.[120] Experts say the Official Secrets Act has been used to limit expression in the past, and is not adequately balanced by the Right to Information Act.[121]

The Armed Forces Special Powers Act affects freedom of speech and expression in conflict zones, allowing security forces to bypass due process while shielding them from prosecution for human rights violations in non-military courts. Human rights groups and the international community have criticized the act, which is in effect in Jammu and Kashmir and several northeastern states, for compromising constitutional guarantees and protections.[122]

Criminal charges have been filed against cartoonists and journalists in relation to content published online. In September 2012, police in Maharastra arrested 25-year old cartoonist Aseem Trivedi, on charges of sedition—which carries a life sentence—as well as violating the Prevention of Insult to National Honor Act and the IT Act.[123] Trivedi was released on bail and the sedition charge was dropped after a public campaign, but the others remain pending.[124] Trivedi's anti-corruption cartoons first attracted official sanctions in December 2011 when his website *Cartoons against Corruption* was suspended by its hosting company based on a complaint to Mumbai police; Trivedi reposted the cartoons, which are widely available online.

While Trivedi's case was widely reported, local officials who abuse legal charges to suppress online reporting are less likely to be called to account. In May 2012, a district official in Jharkhand filed bribery charges against a video journalist who had submitted a right to information request about the use of public funds intended for job creation, apparently trumped up to pressure him to drop the investigation.[125]

Ordinary internet users in India also risk prosecution for online postings criticizing powerful figures. In April 2012, a professor at a university in West Bengal and several others were arrested for circulating a caricature via e-mail and Facebook that mocked a number of government officials,

---

[119] Government of India, "The Constitution of India," http://lawmin.nic.in/coi/coiason29july08.pdf.
[120] "Govt to Issue Fresh Guidelines to Prevent Misuse of Sec 66 (A)," Press Trust of India via *The Hindu,* November 29, 2012, http://bit.ly/19e28VH; Apurva Chaudhary, "Indian Govt Issues Guidelines To Prevent Misuse Of Sec 66A; PIL In Supreme Court," *Medianama,* November 29, 2012, http://bit.ly/SvBdiN.
[121] Iftikhar Gilani, "Government to review Official Secrets Act," *Tehelka,* October 15, 2011, http://bit.ly/1aztkkV.
[122] "Repeal AFSPA: UN Expert to India," Hueiyen News Service, May 2, 2013, http://e-pao.net/GP.asp?src=17..030513.may13
[123] Committee to Protect Journalists, "Indian Cartoonist Jailed for Images Criticizing Government," September 10, 2012, http://cpj.org/2012/09/indian-cartoonist-jailed-for-images-criticizing-go.php.
[124] Sumit Galhotra, "Sedition Dropped, but Indian Cartoonist Faces Other Charges," *CPJ Blog,* October 18, 2013, http://cpj.org/blog/2012/10/sedition-dropped-but-indian-cartoonist-faces-other.php.
[125] Committee to Protect Journalists, "Charges Against Indian Video Journalist Must be Dropped," May 25, 2012, http://cpj.org/2012/05/charges-against-indian-video-journalist-must-be-dr.php.

and charged under Section 66 of the IT Act as well as criminal defamation provisions of the penal code, before being released on bail.[126]

Abuse of Section 66 escalated during the coverage period, most notoriously in the western state of Maharashtra. On November 19, 2012, police in Palghar, a town in Thane district near the state capital Mumbai, detained two Facebook users for complaining that the funeral of Bal Thackeray, leader of the right wing Hindu party, Shiv Sena, was disrupting Mumbai services—an opinion shared by the Supreme Court, who ruled that bringing the city to a halt to observe the mourning was illegal.[127] Twenty-one year old Shaheen Dhadha posted the complaint and Renu Srinivasan 'liked' it, angering Shiv Sena supporters who gathered outside the police station and smashed a medical clinic belonging to Dhadha's uncle.[128] The detentions were widely criticized, both on social media and by public figures, and the women were released on bail within hours. Two policemen who ordered the arrest were suspended, the magistrate who granted them bail transferred, and the charges ultimately dropped, though Shiv Sena activists were still trying to challenge this decision in early 2013.[129] Yet the case had a disturbing coda. A Palghar branch of Shiv Sena launched a strike to protest the suspension of the two police officers, which was publicly criticized on Facebook under an account belonging to 19 year old Sunil Vishwakarma on November 28. Shiv Sena supporters delivered him to local police, who detained him for several hours, supposedly for his own protection. Vishwakarma denied authoring the comment, and police filed charges against an unknown individual for hacking his account.[130]

Journalists ferreting out other abuses of the act learned that Mumbai police had detained two Air India employees, Mayank Sharma and K.V. Jaganathrao, in May 2012 under Sections 66 and 67 on grounds that they made derogatory comments about politicians and insulted the national flag in a closed Facebook group.[131] The charges apparently stemmed from a personal spat with a colleague, Sagar Karnik.[132] The men said they were arrested in an overnight weekend raid and jailed for 12 days months after the complaint against them was filed.[133] Following media reports, police scrambled to rectify the situation by accepting a complaint from Jaganathrao about Karnick—also under Section 66 of the IT Act—for insulting his reputation on Facebook and Orkut.[134]

Other Section 66 charges were filed against social media users around the country during the coverage period. Many, like the Palghar girls, were young, like 22 year old Henna Bakshi and her friend, Kamalpreet Singh, charged by Chandigarh police in September 2012 for criticizing traffic

[126] Soudhriti Bhabani, "Professor Held for Uploading Caricature of Mamata on Social Site," *Daily Mail*, April 13, 2012, http://dailym.ai/19K2TYK.
[127] Julie Mccarthy, "Facebook Arrests Ignite Free-Speech Debate In India," NPR, November 28, 2012, http://n.pr/TuViZ3.
[128] Julie Mccarthy, "Facebook Arrests Ignite Free-Speech Debate;" "Two Girls Held for FB Post Questioning Bandh for Thackeray's Funeral," *Zeenews*, November 19, 2012, http://bit.ly/XsFr0A.
[129] "Palghar Court Closes Case Against Girls Arrested for Facebook Comments," Press Trust of India via NDTV, February 1, 2013, http://www.ndtv.com/article/india/palghar-court-closes-case-against-girls-arrested-for-facebook-comments-325157.
[130] "I Did Not Post on Raj Thackeray, FB Account was Hacked: Palghar Boy," *Firstpost,* November 29, 2012, http://bit.ly/18ej1CL.
[131] Jaganathrao was called K.V.J. Rao in some reports. Saurabh Gupta, "Arrested for Facebook Posts, They Spent 12 Days in Jail, Lost Their Air India Jobs," NDTV, November 25, 2013, http://bit.ly/1eQaRpk.
[132] "Cyber Police Station Files FIR Under 66A Against Sagar Karnik," *The Hindu,* December 3, 2012, http://bit.ly/15CaGFE.
[133] Meena Menon, "Jailed Air India Employees Demand Compensation," *The Hindu,* March 23, 2013, http://bit.ly/ZVPNDe.
[134] Saurabh Gupta, "Facebook Row: Mumbai Police Book Man Whose Complaint Led to Air India Employees' Arrests," NDTV, December 2, 2012, http://bit.ly/TCdOen.

officials.[135] Many were detained, usually briefly, and sometimes on grounds it would protect them, though this may well have amplified the impression that they were guilty of wrongdoing—especially when detentions occurred at night or bail was denied. Anti-corruption activist Ravi Srinivasan was arrested in his home in the union territory of Puducherry at 5am in October 2012 for offending a local politician on Twitter.[136] Orissa police arrested 20-year-old Pintu Sahu in December for posting an image of a Hindu deity sitting on a mosque on Facebook, representing a controversy between Mulsims and Hindus over a local shrine.[137] In February, police in Uttar Pradesh arrested Sanjay Chowdhary, a civil servant, for insulting a religious community and political leaders on Facebook, and denied at least one application for bail.[138] The most extreme case was in Jammu and Kashmir, where three men were arrested in October in connection with a video on Facebook, considered blasphemous, that spurred thousands of people to protest.[139] They were held for more than 40 days under the IT Act before being granted bail on December 12, although there was no evidence they had uploaded the video, which police said originated in Pakistan.[140]

The cases appeared to stall at the police level, without coming to trial. Yet legal arguments in bail hearings concentrated on proof—such as whether the police took screen shots of the offending posts—while the accused often blamed the content on hackers. This distracted from the fact that the charges themselves undermine constitutional free speech protections.

Section 66 faced numerous legal challenges in the past year. One petitioner told the Bombay High Court in 2013 that it should not apply to social media, which is mostly in the public domain, when the same content in print would not lead to prosecution.[141] Several members of parliament said they were working on amending it, though one motion to amend it was deferred pending a Supreme Court ruling.[142] The motion was revealing, however. In it, Member of Parliament P. Rajeev said that the 2008 IT amendment passed in the Lok Sabha in just seven minutes—along with six other bills—and went through the upper Rajya Sabha without discussion.[143] One inspiring challenge was filed with the Supreme Court in November 2012 by 21 year old student Shreya

[135] "Chandigarh Police Awaits Logs From Facebook in Abusive Remarks Case," *Indian Express,* September 20, 2012, http://m.indianexpress.com/news/chandigarh-police-awaits-logs-from-facebook-in-abusive-remarks-case/1005204/.
[136] Puducherry was formerly known as Pondicherry. Dhananjay Mahapatra, "Puducherry Justifies Arrest Under Section 66A of IT Act," *Times of India,* January 12, 2013, http://bit.ly/16zV4bY; Priscilla Jebaraj, "IAC Volunteer Tweets Himself into Trouble, Faces Three Years in Jail," *The Hindu,* November 1, 2012, http://bit.ly/16zV4bY.
[137] "Orissa: Youth Held for FB Photos of Hanuman on Mosque," *Outlook,* December 8, 2012, http://bit.ly/VEwiB3.
[138] "Man Held for Facebook Posts Denied Bail," Indo-Asian News Service via *Hindustan Times,* February 6, 2013, http://www.hindustantimes.com/India-news/UttarPradesh/Man-held-for-Facebook-posts-denied-bail/Article1-1007698.aspx.
[139] Arif Munshi, "Blasphemous Picture on Facebook Triggers Massive Protest," *Greater Kashmir,* October 29, 2013, http://www.greaterkashmir.com/news/2012/Oct/30/blasphemous-picture-on-facebook-triggers-massive-protest-27.asp.
[140] "Arrested For Video on Facebook, Three Men in Jammu and Kashmir Spend Over 40 days in Jail," NDTV, December 7 2012, http://bit.ly/SCmvH9; "India 2012 International Religious Freedom Report," in *International Religious Freedom Report for 2012,* Bureau of Democracy, Human Rights and Labor, United States Department of State, http://1.usa.gov/16zVajO.
[141] "Section 66A of IT Act Challenged as 'Unconstitutional', Court Seeks Center's Reply," Press Trust of India, February 28, 2013, http://bit.ly/WlM44R.
[142] Rajeev Chandrasekhar, "Don't Kill Freedom of Speech," *Times of India*, November 30, 2012, http://bit.ly/16zVf73; Apurva Chaudhary, "Indian Govt Issues Guidelines To Prevent Misuse Of Sec 66A; PIL In Supreme Court," *Medianama,* November 29, 2012, http://bit.ly/SvBdiN.
[143] P. Rajeeve, "Resolution Re. Need To Amend Section 66a Of Information Technology Act, 2000," December 14, 2012, available at Software Freedom Law Center, http://sflc.in/wp-content/uploads/2013/03/P.RajeeveResolution_RS.pdf.

Singhal.[144] Despite this activity, the sole, insufficient reform was a government advisory requiring senior police officers to approve arrests for social media postings, which the Supreme Court enforced in mid-2013, outside the coverage period of this report.[145]

State surveillance, like content control, is growing in scale and sophistication, and India's inadequate legislative framework provides almost no privacy protections. A 2007 Supreme Court ruling held that wiretapping would potentially violate constitutional protections under Article 19, the right to freedom of speech and expression and Article 21, the right to life and personal liberty, unless it was "permitted under the procedure established by law." The court ordered the creation of a government committee to review phone tap orders, which are governed by the Telegraph Act, but did not require judicial oversight.[146] A 2007 amendment was made to 419A Rules which govern the act, elaborating the procedure and limiting national and state home ministry officials of a certain rank to order phone taps.[147]

The amended 2008 IT Act also allowed both central and state officials to intercept, monitor or decrypt electronic communications or direct others to do so. Both this and the Telegraph Act stipulate surveillance should be done to protect defense, national security, sovereignty, friendly relations with foreign states, and public order, and that it should be subject to approval, limited to 60 days—fewer in emergencies—and renewable for a maximum of 180 days.[148] Yet the IT Act adds a clause allowing surveillance for "investigation of any offense;" moreover, while the procedure for high-level government authorization seems to involve a case-by-case assessment, systematic, mass surveillance is not prohibited.[149]

Additional requirements followed in 2011. The government authorized eight separate bodies to issue surveillance-related orders directly to service providers, from intelligence agencies to the tax bureau.[150] IT Act regulations required cybercafe owners to copy and retain customers' photo ID and browser history for a year.[151] Officials railed against international providers that prevent the government from tracking users by encrypting communications,[152] and required some, such as

---

[144] Bhadra Sinha, "SC Slams Facebook Arrests, Takes Up 66A," *Hindustan Times*, November 29, 2012, http://bit.ly/QOlCy2; Cordelia Jenkins, "Who is Shreya Singhal?" *Live Mint,* November 29, 2012, http://bit.ly/RkLiCm.

[145] J. Venkatesan, "No Blanket Ban on Arrests for Facebook Posts, says SC," *The Hindu,* May 16, 2013, http://bit.ly/1839Eou. "PUCL Leader Gets Bail in Facebook Post Case," *The Hindu,* May 14, 2013, http://bit.ly/129FnAB.

[146] Privacy International, "Chapter ii: Legal Framework," in *India,* November 14, 2012, http://bit.ly/17cVl1Q; Justice Ajit Prakash Shah, "Report of the Group of Experts on Privacy," October 16, 2012, http://bit.ly/VqzKtr.

[147] Jadine Lannon, "Rule 419A of the Indian Telegraph Rules, 1951," Center for Information and Society, June 20, 2013, http://cis-india.org/internet-governance/resources/rule-419-a-of-indian-telegraph-rules-1951.

[148] Jadine Lannon, "Indian Telegraph Act, 1885, 419A Rules and IT (Amendment) Act, 2008, 69 Rules," Center for Information and Society, April 28, 2013, http://bit.ly/14N1qCT.

[149] Pranesh Prakash, "How Surveillance Works in India," *New York Times,* July 10, 2013, http://nyti.ms/164b2sm.

[150] Research and Analysis Wing, the Intelligence Bureau, the Directorate of Revenue Intelligence, the Enforcement Directorate, the Narcotics Control Bureau, the Central Bureau of Investigation, the National Technical Research Organization and the state police. See, Privacy International, "Chapter iii: Privacy Issues," in *India Telecommunications Privacy Report,* October 22, 2012, https://www.privacyinternational.org/reports/india/iii-privacy-issues#footnoteref1_ni8ap74.

[151] "Information Technology Act, 2000," Ministry of Communications and Information Technology, April 11, 2011, http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf.

[152] Joji Thomas Philip, "Can't Track Blackberry, Gmail: DoT," *Economic Times,* March 16, 2011, http://bit.ly/1bhkFo8; Joji Thomas Philip and Harsimran Julku, "E-services like Gmail, BlackBerry, Skype Can't be Banned for Lack of Scrutiny: Telecoms Security Panel," *Economic Times,* June 16, 2011, http://bit.ly/16TBotD.

Nokia and BlackBerry, to establish local servers subject to Indian law under threat of blocking their services.[153] (This effort was still ongoing in April 2013, when internal Home Ministry minutes suggested the government intends to require internet phone services like Skype to install local servers.[154]) Under a 2011 Equipment Security Agreement that did not appear on the DOT website,[155] telecom operators were told to develop the capacity to pinpoint any customer's physical location within 50 meters. "Customers specified by Security Agencies" were prioritized for location monitoring by June 2012, with "all customers, irrespective of whether they are the subject of legal intercept or not," by June 2014;[156] operators were in "various stages" of compliance by August 2012.[157] In October 2012, a government-appointed group described this framework as "an unclear regulatory regime that is inconsistent, nontransparent, prone to misuse, and that does not provide remedy or compensation to aggrieved individuals."[158]

Service providers are required by license agreements to cooperate with official requests for data.[159] Experts said that while non-compliance carries a possible seven year jail term, unlawful interception is punishable by just three years' imprisonment.[160]

Google and Facebook received more user data requests from India in 2012 than any other country except the U.S, but didn't always comply.[161] In January 2012, responding to a freedom of information request, the Home Ministry reported Indian officials issuing 7,500 to 9,000 phone interceptions per month.[162] During the coverage period, some news reports cited the "review committee" responsible for reviewing electronic interception orders every 90 days, established following the 2007 Supreme Court ruling and comprised of Cabinet Secretary Ajit Seth, Telecom Secretary R. Chandrasekhar and Legal Affairs Secretary B.A. Agrawal. In October 2012, *The Hindu,* citing this unnamed committee's "internal note," said interception involving 10,000 phones and 1,000 email IDs had been authorized by several agencies between June and August—some new, and some renewing existing orders.[163] In January 2013, the *Economic Times* said it had reviewed a

[153] In 2013, outside the coverage period of this report, BlackBerry confirmed their "lawful access capability" met "the standard required by the Government of India," though business customers would be unaffected. Anandita Singh Mankotia, "Government, BlackBerry Dispute Ends," *Times of India,* July 10, 2013, http://bit.ly/187FX9z. For Nokia, see Thomas K Thomas, "Despite India Server, IB Unable to Snoop into Nokia E-mail Service," *The Hindu,* July 14, 2011, http://bit.ly/1fRqjAt.
[154] Joji Thomas Philip, "Net Telephony Providers Will be Asked to Set Up Servers in India" *Economic Times,* May 20, 2013, http://bit.ly/15BHST3.
[155] Nikhil Pahwa, "New Telecom Equipment Policy Mandates Location Based Services Accuracy Of 50Mtrs: COAI," *Medianama,* June 17, 2011, http://bit.ly/keKNxY.
[156] Cellular Operators Association of India, "Additional Cost Implication for the Telecom Industry as Government Mandates Location Based Services to Meet its Security Requirements," press release, June 16, 2011, http://bit.ly/18zURS6.
[157] "Operators Implementing Location-based Services: Govt," Press Trust of India via NDTV, August 9, 2012, http://bit.ly/S4zNcT.
[158] Justice Ajit Prakash Shah, "Report of the Group of Experts on Privacy."
[159] Saikat Datta, "A Fox On A Fishing Expedition," *Outlook,* May 3, 2010, http://www.outlookindia.com/article.aspx?265192.
[160] Pranesh Prakash, "How Surveillance Works in India," *New York Times,* July 10, 2013, http://nyti.ms/164b2sm.
[161] "Indian Govt Snooped on 13 Users Per Day in 2012, says Google Report," Press Trust of India, March 11, 2013, http://bit.ly/Y5oepb; Facebook, "Global Government Requests Report," January—June 2013, http://on.fb.me/1dmxPnW. By contrast, India did not appear in the top five countries that made the most requests to Microsoft. See, Microsoft, "2012 Law Enforcement Requests Report," http://bit.ly/ZwBiGV.
[162] Shyamlal Yadav, "9,000 Orders for Phone Interception a Month: Govt," *Indian Express*, January 23, 2012, ttp://bit.ly/ylTTmN.
[163] Sandeep Joshi, "10,000 Phones, 1,000 E-mail IDs Under the Scanner," *The Hindu,* October 12, 2012, http://bit.ly/14T5EHr.

committee document covering October—December 2012, and involving surveillance orders for 10,000 phones and 1,300 emails.[164]

Abuse of surveillance has been widely reported, including monitoring of lawmakers, politicians, and journalists[165]—in one case, implemented by an ISP on the basis of an emailed government order that turned out to be fake.[166] In 2011, two senior Mumbai police officers were found to have sold phone records for money;[167] another in 2012 apparently requisitioned cell phone records "to keep an eye on his girlfriend."[168]

Much of this activity is driven by what *The Hindu* newspaper characterized as "massive purchases of communications intelligence equipment from secretive companies from India and abroad" by both state and other actors. Two suppliers are domestic: Clear Trail markets a "data traffic inspect engine" for mobile surveillance. Shoghi Communications supplies GSM monitoring and other equipment, but its only client is the government.[169] In 2010, *Outlook* magazine documented intelligence agencies operating dozens of cellphone monitoring devices that don't require the target's number—and therefore don't require cooperation from service providers. "We have deployed the system … in the hope that we might pick up critical conversations, but most of the time, we end up getting private calls," an unnamed intelligence official told *Outlook*.[170] Security agencies have even tried to limit the spread of these technologies. In 2011, the federal Intelligence Bureau was reported trying to shut down at least 33 passive interception units at internet hubs around the country. Many were being operated by state police with a tendency to misuse the equipment—or even mislay it.[171] On May 8, 2013, the Bureau issued a directive banning junior police officers from requesting mobile data records.[172] Yet the Bureau is itself a civilian organization without a statutory foundation or parliamentary oversight.[173]

Rather than correct this abuse, the government is transitioning to a nationwide surveillance project known as the Central Monitoring System (CMS), which allows government agents to bypass service providers in favor of interception equipment on intermediary premises allowing them to monitor electronic traffic on any platform or device directly, in real time.[174] Reports estimated the total cost was in the region of 8 billion rupees ($132 million).[175] Proponents said the system improved security by reducing the number of third parties involved in interceptions, and by documenting the

[164] Harsimran Julka and Joji Thomas Philip, "Home Ministry Ordered 10k Wire Taps in Last 90 Days, Orders Tapping of 1300 Email ids," *Economic Times,* January 3, 2013, http://bit.ly/XcPjaC.
[165] Saikat Datta, "We, the Eavesdropped," *Outlook*, May 3, 2010, http://www.outlookindia.com/article.aspx?265191; "800 New Radia Tapes," *Outlook*, December 10, 2010, http://www.outlookindia.com/article.aspx?268618; "Government Mulling Law to Regulate Phone Tapping," *DNA India*, December 16, 2010, http://bit.ly/eFX89N.
[166] Praveen Swami, "The Government's Listening To Us," *The Hindu*, December 1, 2011, http://bit.ly/rH8bO2.
[167] "Two Delhi Cops May Land in the Dock for Selling Cell Call Records," *Times of India*, March 11, 2012, http://bit.ly/1bhmHor.
[168] "Only Top Cops can Seek Call Records: State Intelligence Bureau," *Times of India,* May 17, 2013, http://bit.ly/1bhkSaX.
[169] Privacy International, "Chapter iii: Privacy Issues."
[170] Saikat Datta, "A Fox On A Fishing Expedition."
[171] Praveen Swami, "The Government's Listening To Us."
[172] "Only Top Cops Can Seek Call Records: State Intelligence Bureau," *Times of India,* May 17, 2013, http://bit.ly/1bhkSaX.
[173] A Subramani, Ex-officer questions Intelligence Bureau's legal status, *Times of India,* March 26, 2012, http://bit.ly/1aHbVKN.
[174] Anurag Kotoky, "India Sets Up Elaborate System;" Shalini Singh, "Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic," *The Hindu,* September 9, 2013, http://bit.ly/1etaS0t.
[175] Pranesh Prakash, "How Surveillance Works in India."

nature and duration of requests in a streamlined "electronic audit trail."[176] But this may itself be vulnerable to cyberattacks.[177] It was never reviewed by parliament.

Some news reports said the eight agencies already empowered to conduct surveillance would be able to use it, with the addition of the National Investigation Agency, which was reported petitioning for inclusion in October 2012,[178] and possibly the Securities and Exchange Board of India.[179] Others said select military agencies would also be involved.[180] In April 2013, the Center for Information and Society submitted a freedom of information request to clarify the exact range of agencies authorized to conduct electronic surveillance, but had not received a response by the end of the coverage period.[181]

Operated by a little-known Department of Telecommunications unit, the Center for Development of Telematics,[182] it is not known how extensively the CMS has been implemented. One mid-2013 news report said it was active in New Delhi and neighboring Harayana state, with Kolkata, the capital of West Bengal, and the southwestern states of Kerala, Karnataka to follow.[183] Another said operation was yet to begin, pending technical certification of 21 regional monitoring centers.[184] But many internet and telecommunications firms already have monitoring capabilities installed, some of which are already controlled by the government, according to *The Hindu,* and the CMS will consolidate this equipment, too.[185] Since there is no legal requirement to notify the target of surveillance—even after the end of an investigation—its implementation may not be apparent, but several accounts said it would be fully operational by 2014.

Some of this activity, conducted to counter terrorism, is legitimate. But the surveillance architecture has been put in place without a privacy law, leaving individuals vulnerable, even as the kind of personal data they are surrendering to the government diversifies. Since 2010, millions of Indian citizens have been issued unique Aadhaar ID numbers as part of an anti-poverty initiative. Though not compulsory, officials say not possessing one could limit access to some government assistance. The authority that issues the numbers maintains a database of numbers tied to personal information including biometric data, such as fingerprints.[186] There is no law governing the authority—in fact, one was rejected by parliament in 2011.

---

[176] Bharti Jain, "Govt Tightens Control for Phone Tapping," *Times of India,* June 21, 2013, http://bit.ly/1bXQy3r.
[177] Anjani Trivedi, "In India, Prism-like Surveillance Slips Under the Radar," *Time,* June 30, 2013, http://ti.me/17cT6vA.
[178] Yatish Yadav, "NIA Seeks Central Monitoring System to Tap Phones," *Indian Express,* October 15, 2012, http://bit.ly/OAHjzx.
[179] "Govt to Install 'Fool-Proof' Phone Tapping Setup Soon," *Outlook,* June 17, 2013, http://bit.ly/1hbvWHu.
[180] Maria Xynou, "India´s 'Big Brother:' The Central Monitoring System (CMS)," Center for Internet and Society, April 8, 2013, http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system.
[181] Prasad Krishna, "RTI on Officials and Agencies Authorized to Intercept Telephone Messages in India," Center for Information and Society, July 15, 2013, http://bit.ly/1fRqJXu.
[182] "About C-DOT," http://www.cdot.co.in/rti/pdf/rti-2Inf-01a-AboutCDOT(E).pdf. News reports also said national Telecom Enforcement, Resource and Monitoring cells, also under the Department of Telecommunications, had a role in implementation. Department of Telecommunications, "TERM/Security," http://www.dot.gov.in/term/term-security.
[183] Shalini Singh, "India's surveillance project may be as lethal as PRISM," *The Hindu,* June 21, 2013, http://bit.ly/15EeV2o.
[184] Kalyan Parbat, "India's Surveillance System CMS to be Operational Soon," *Economic Times,* September 5, 2013, http://bit.ly/17QbPit.
[185] Shalini Singh, "Govt. Violates Privacy Safeguards."
[186] Nandan Nilekani, "The Science of Delivering Online IDs to a Billion People: The Aadhaar Experience," World Bank's Development Economics Lecture, April 24, 2013, http://bit.ly/15AS1O8.

In 2011, data protection rules improved privacy protections in commercial transactions but drew some criticism from the business community.[187] The EU does not consider India "data secure."[188] In October 2012, a group of experts issued a government-commissioned report providing a foundation for a future privacy bill, though the timeframe for drafting and implementing it isn't clear. Critically, this report clarified that exceptions to the right to privacy, such as national security and privacy investigations, be assessed according to values of proportionality, legality, and democratic rule.[189]

Violence targeting journalists, right to information activists and whistleblowers is common in India.[190] However, there were no significant accounts of physical assaults on bloggers or online activists during the coverage period. Some did face threats and pressure in retaliation for online activity. Many individuals facing charges under the IT Act, for example, were sought out by destructive mobs. Police and security agents were also accused of conducting violent raids while investigating alleged digital offenses, including some targeting cybercafe clients.[191]

Cyberattacks did not systematically target opposition groups or human rights activists during the coverage period. Loopholes in cyber security were exposed, however, when the international hacking group Anonymous targeted establishment sites, including that of the Supreme Court, in June 2012 to protest against decisions regarding file-sharing and copyright issues.[192]

---

[187] Outsourcing firms are exempt. Miriam H. Wugmeister and Cynthia J. Rich, "India's New Privacy Regulations," Morrison and Foerster Client Alert. May 4, 2011, http://bit.ly/IJSePF; John Ribeiro, "India Exempts Its Outsourcers from New Privacy Rules," *Network World*, November 2, 2011, http://bit.ly/16TCbuF.

[188] "India to EU: Declare us a Data Secure Country," Press Trust of India via *Times of India,* October 18, 2012, http://bit.ly/WCNAOh; Amiti Sen, "EU Not Ready to Give India 'Data Secure' Status," *The Hindu,* June 15, 2013, http://bit.ly/12wvF0g.

[189] Justice Ajit Prakash Shah, "Report of the Group of Experts on Privacy."

[190] Committee to Protect Journalists, "29 Journalists Killed in India Since 1992/Motive Confirmed," accessed August 2013, http://bit.ly/mnq7Mr; Prabhu Mallikarjunan, "Attacks on RTI Activists in India Raise Questions Over Safety Measures," *Indian Express,* January 17, 2013, http://newindianexpress.com/states/karnataka/article1423834.ece.

[191] Jaideep Mazumdar, "The Imphal Taliban," July 13, 2013, http://www.timescrest.com/opinion/the-imphal-taliban-10718.

[192] Rezwan, "India: Netizens Respond To Anonymous India's Protests," *Global Voices,* June 9, 2012, http://bit.ly/LbCEzI.

INDONESIA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	11	11
Limits on Content (0-35)	11	11
Violations of User Rights (0-40)	20	19
Total (0-100)	**42**	**41**

* 0=most free, 100=least free

POPULATION: 241 million
INTERNET PENETRATION 2012: 15 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The Supreme Court cleared Prita Mulyasari on criminal and civil defamation charges relating to a personal email she sent in 2009 (see **VIOLATIONS OF USER RIGHTS**).
- Electronic defamation could lead to 6 years imprisonment or $80,000 fines; offline, most sentences are less than 2 years—fines amount to 40 cents (see **VIOLATIONS OF USER RIGHTS**).
- Overbroad blocks on pornography compromised legitimate websites, including LGBT content (see **LIMITS ON CONTENT**).
- In October 2012, the Constitutional Court rejected a request for judicial review of the State Intelligence Law (see **VIOLATIONS OF USER RIGHTS**).
- In mid-2013, an expert told the Associated Press 50 to 100 militants had been recruited directly through Facebook in the past two years (see **LIMITS ON CONTENT**).

INTRODUCTION

Economic development and a democratic political system have spurred internet use in Indonesia, though poor infrastructure across the archipelago's 16,000 islands keeps connections spotty in rural areas. Where people once relied on cybercafés, however, they are increasingly using mobile phones to go online. This change has fuelled the nation's extraordinary appetite for social media. Facebook usage in the world's fourth most populous country has shot up in the past four years, while Twitter is a lifestyle staple for young internet users, and increasingly politicians. President Susilo Bambang Yudhoyono, who will complete his second term in office in 2014, has over 3 million followers.

Though introduced in 1994, internet access only gained momentum after 1998, when the authoritarian leader Suharto resigned in the face of public protests and Indonesia began its transition to democratic rule. Yet the political upheaval, which facilitated extensive human rights abuses that were underreported in the traditional media, may still be impeding online discourse. Of the millions of active blogs and social media accounts, comparatively few are dedicated to domestic politics.

Home to the world's largest Muslim population, as well as many different ethnicities, Indonesia's religious and racial tensions are felt in the online space. A sweeping ban on pornography affects many sites offering legitimate information on sex education, LGBT groups, and tribal culture. Security threats have resulted in a total of nine laws granting various agencies power to intercept electronic communications, but existing privacy protections are inadequate. Just two of the laws require judicial oversight, and civil society groups declared one of these—a 2011 law governing monitoring for intelligence purposes—unconstitutional in 2012. The Constitutional Court rejected their petition for judicial review of the law in October 2012.

Civil society opposition to laws criminalizing legitimate online speech also has yet to bear fruit. Dozens of ordinary internet users have faced criminal charges for defamation via social media or personal email under a 2008 Information and Electronic Transactions (ITE) law. By international standards, civil laws are more appropriate than criminal in defamation disputes.[1] Yet the 2008 law made existing sentences in the penal code even harsher for defamation committed electronically. Spoken or written insults could result in a few months or, at worst, four years behind bars; the same content shared online or on a cell phone comes with a maximum of six years imprisonment. Meanwhile, fines for defamation outlined in the penal code could be paid with less than 50 cents, according to the conversion rate on April 30, 2013.[2] Under the ITE law, defamation could cost the defendant around $80,000.

In 2012, the Supreme Court overturned the landmark convictions of housewife Prita Mulyasari on criminal as well as civil defamation charges relating to a personal email she sent in 2009. Astonishingly, this has yet to result in reform of the ITE law's disproportionate penalties.

[1] Article 19, "Criminal Defamation," accessed August 2013, http://www.article19.org/pages/en/criminal-defamation.html.
[2] All conversion rates date from April 30, 2013 or the date of the source document, unless otherwise specified.

Meanwhile, an anticybercrime bill drafted in 2010, which would also provide heavier punishments for crimes committed online than existing laws, appears to be still pending. Authorities cite the wider reach of the internet as justification for this bias against ICTs. But they fail to recognize that when criminal complaints can be filed by any individual, the web is just as likely to create new opportunities for vindictive prosecution as it is to damage reputations.

OBSTACLES TO ACCESS

Internet penetration in Indonesia was just over 15 percent in 2012, according to the International Telecommunication Union, citing a national statistics agency.[3] Other estimates were above 20 percent.[4] Access is not evenly distributed, however. Cable is costly to install across the world's largest archipelago, and poor infrastructure, combined with poverty in rural areas, keeps internet use heavily concentrated in cities, particularly on the islands of Java and Bali. One November 2012 survey estimated more than 90 percent of web users lived in urban areas.[5] The country's main network-access providers, which link retail level ISPs to the internet backbone, are also clustered on Java, particularly in Jakarta. Mobile phone usage, on the other hand, is almost ubiquitous. Mobile penetration was measured at 115 percent in 2012, indicating some users have more than one device.[6]

In the past, personal internet access was reserved for older, middle, or upper class urban residents. That may be changing, since the nation's largest broadband provider reported a 41 percent jump in fixed-line subscribers from 2012 to 2013.[7] Yet broadband service, which averages IDR 150,000 ($12) per month for a fixed-line connection, remains expensive and inconvenient for many. Wireless service is transforming the market, and mobile access has become more popular than cybercafes, according to one survey, which reported that 62 percent of urban respondents went online using a phone in 2012. Less than half used a cybercafe, down from 83 percent in 2009.[8]

The government, particularly the Ministry of Communications and Information Technology (MCI), has made internet expansion a priority. To connect rural areas, the MCI launched a program to establish *desa pintar* (smart villages) with high quality internet and mobile phone reception. By 2012, the MCI reported connecting 5,958 villages.[9]

---

[3] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://bit.ly/14IlykM.
[4] The Indonesian Internet Service Provider Association reported 63 million internet users in a population of 240 million in 2012, putting penetration at 26 percent, while digital market research firm eMarketer reported 24 percent penetration in 2012. See, Asosiasi Penyelenggara Jasa Internet Indonesia, "Indonesia Internet User, 2012" http://bit.ly/19KvxsR; Muhammad Al Azhari, "LTE May Herald an Internet Revolution in Indonesia," May 3, 2013, http://bit.ly/13lfjln; eMarketer, "In Indonesia, a New Digital Class Emerges," March 12, 2013, http://bit.ly/10yQ2ET.
[5] eMarketer, "In Indonesia, a New Digital Class."
[6] International Telecommunication Union, "Mobile-cellular Telephone Subscriptions, 2000-2012."
[7] "Info Memo," Telkom Indonesia, 1Q2013, http://bit.ly/1bhCVOb.
[8] Survey respondents were aged between 15 and 50. eMarketer, "In Indonesia's Cities, Mobile Boost Internet to No 2 Media Spot," January, 30, 2013, http://bit.ly/XgM0yu.
[9] "*Inilah Sederet Prestasi Yang Diklaim Kominfo*" [Communications Ministry Achievements of 2012], *Detik*, January 14, 2013, http://bit.ly/16AfDFc.

Indonesia has a range of digital service providers, although some privately-owned providers have close ties to government ministers. The two largest ISPs are PT Telecom, which is majority state-owned, and Indosat.[10] Their dominance—along with regulatory obstacles imposed by the government— poses challenges for small ISPs entering the market. Nevertheless, the Indonesian Internet Service Provider Association, APJII,[11] had over 250 member ISPs and network access providers in 2013, accounting for around 90 percent of the national total.[12]

Of the nine mobile phone service providers in operation, the most prominent are PT Telkomsel, which covers 60 percent of the market, PT Indosat, with 21 percent, and PT XL Axiata with 19 percent.[13]

Despite their individual allegiances to officials, Indonesian ISPs are a close-knit community thanks to the APJII, which was founded in 1996. In 1997, tired of routing local traffic through expensive and inefficient international channels—and wary of a government-led solution—they independently created the Indonesia Internet Exchange to allow member ISPs to interconnect domestically.[14] APJII also engages the government on behalf of providers regarding censorship, legal, and regulatory issues in ways that freedom of expression experts view as largely constructive.

In January 2013, experts were particularly vocal when the attorney general's office filed corruption charges against one ISP, IM2, for selling bandwidth under a public frequency licensed only to its parent company, Indosat.[15] IM2 was accused of avoiding a private tax rate on the frequency, causing state losses of IDR 1.3 trillion ($134 million).[16] The investigation was ongoing during the coverage period of this report; a judge ordered IM2 to pay the full amount in damages and jailed a former executive for four years in a highly contested verdict in July.[17] Since ISPs generally rent frequencies from other companies in Indonesia, the APJII condemned the investigation along with the business community and even Tifatul Sembiring, the communication and information minister. Their concerns seemed well-founded in February when an anti-corruption organization filed a report with the attorney general's office accusing 16 more ISPs and 5 mobile service providers of a similar fraud.[18] It is not clear if those providers will face prosecution.

---

[10] Ronald J. Deibert et al., "Indonesia," in *Access Contested: Security, Identity, and Resistance in Asian Cyberspace,* ed. (Massachusetts Institute of Technology, 2012), http://www.apjii.or.id/index.php?option=com_content&view=article&id=53&Itemid=11.

[11] *Asosiasi Penyelenggara Jasa Internet Indonesia*.

[12] Irvan Nasrun, "Indonesia ISP Association" (presentation, APJII, August 13, 2013), http://www.apjii.or.id/v2/upload/Artikel/APJII-JAPAN-ASEAN%20Information%20Security.pdf; Muhamad Al Azhari, "An Internet Case of Fraud, Tax Evasion," *Jakarta Globe,* February 22, 2013, http://bit.ly/1ajhRsL.

[13] Oxford Business Group, "The Big Three: A Battle for Subscribers and Profit, Indonesia 2012," http://www.oxfordbusinessgroup.com/news/big-three-battle-subscribers-and-profit

[14] Andy Kurniawan, "Indonesia Internet eXchange, IIX: IIX and IIXv.6 Development Update 2007" (presentation, Asia Pacific Network Information Centre), accessed August 2013, http://archive.apnic.net/meetings/25/program/ix/id-ix-update.pdf.

[15] "IM2 Preparing Defense Ward Internet Doomsday," *Jakarta Post*, January 15, 2013, http://bit.ly/15CrmNm; Al Azhari, "An Internet Case of Fraud."

[16] Conversion as of January 15, 2013, according to Oanda. The value of the rupiah plunged in 2013; as of July 19, 2013, when news reports announced the verdict, the same amount came to US$128 million.

[17] Mariel Grazella, "Telco firms rattled by IM2 verdict," *Jakarta Post*, July 9, 2013, http://www.thejakartapost.com/news/2013/07/09/telco-firms-rattled-im2-verdict.html.

[18] Al Azhari, "An Internet Case of Fraud."

The MCI's Directorate General of Post and Informatics (DGPT) is the primary body overseeing telephone and internet services, responsible for issuing licenses to ISPs, cybercafes, and mobile phone service providers. The Indonesia Telecommunication Regulation Body (BRTI) also regulates and supervises telecommunications. There is some overlap between the mandates and responsibilities of the two agencies. Based on the ministerial decree that established it, BRTI is supposed to be generally independent and includes nongovernment representatives. However, observers have questioned its effectiveness and independence, as it is headed by the DGPT director, and draws its budget from DGPT allocations. In May 2012, Sembiring inaugurated nine full BRTI members for the years 2012 through 2015. Two additional members remain from the previous term.[19]

LIMITS ON CONTENT

Tens of thousands of websites related to pornography, violent extremism, or censorship circumvention are blocked in Indonesia under laws that grant the government power to filter content without judicial oversight. While there is no systematic abuse of this system to restrict political content, many minority groups, like the LGBT community, find their content inaccessible with no clear avenue of appeal. Social media and communications apps are avidly used, though their potential for spreading hate speech remains a concern. Google blocked the notorious 'Innocence of Muslims' video on YouTube after it sparked unrest.

The internet has expanded Indonesians' access to information, as they are no longer dependent on traditional media for news; many have adopted the internet as their main information source. In response, the government's approach has shifted. The 2008 ITE Law granted the MCI powers to monitor and censor online content at its own discretion without a court order, though it did not outline the process involved.[20] An anti-pornography law was also passed in 2008[21]—and upheld by the courts in 2010, despite being challenged as unconstitutional.[22]

Since then, filtering of pornographic material has increased, particularly after some public celebrity sex tape scandals in 2010. [23] Defining what constitutes pornography, however, has proved a stumbling block in the Muslim majority nation. The U.S.-based website of the Free Speech Coalition, a trade association for the adult entertainment industry, is censored, along with multiple other legitimate sites. Sex education resources and websites hosted by LGBT organizations, both

[19] BRTI, "*Pelantikan Anggota Komite Badan Regulasi Telekomunikasi Indonesia Periode 2012-2015*" [Inaugural Regulatory Committee Members Indonesian Telecommunications Regulatory Body Period 2012-2015], May 3, 2013, http://brti.or.id/component/content/article/75-press-release/239-pelantikan-anggota-komite-regulasi-2012-2015

[20] Article 40(2) of the ITE Law states that "the government, in compliance with the prevailing laws and regulations, aims at protecting public interest from all forms of disturbances that result from the abuse of electronic information and electronic transaction. Law No. 11 of 2008 on Electronic Transaction and Information, available at http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=1969&filename=UU%2011%20Tahun%202008.pdf.

[21] "Law No. 44 on Pornography."

[22] Karishma Vaswani, "Indonesia Upholds Anti-pornography Bill," BBC, http://news.bbc.co.uk/2/hi/8586749.stm.

[23] OpenNet Initiative, "Country Profile—Indonesia," August 9, 2012, http://opennet.net/research/profiles/indonesia.

domestically and overseas, are consistently filtered, and even art and traditional attire can be considered explicit.

The ministry is not known to systematically filter political content or anti-government criticism, though other broad restrictions are in place. Encryption and circumvention tools are blocked,[24] though some can be found in practice. Sites that promote terrorism and file-sharing are also subject to restrictions. In 2011, after a suicide bomber attacked a church in central Java, the MCI announced that it would block 300 out of 900 Islamist websites that the public had reported for promoting violence, radicalism or terrorism, though the list of sites was not published.[25] The same year, representatives of the Indonesian music industry urged the MCI to shutter 20 websites that enabled users to download songs without permission from the artists;[26] four remain closed.[27] In July 2012, the APJII mooted banning all websites that allow illegal downloads, but this had yet to appear by the end of the coverage period.[28]

There is a general lack of clarity about censorship decisions and how to challenge them. The MCI maintains an online database of blacklisted domains and URLs, *Trust Positif,* as a reference for providers on what to filter. *Trust Positif* listed over 745,000 domain names and 55,000 URLs for pornographic content in 2013, a slight—but not dramatic—increase over the previous year;[29] the site also provides an email address and form for individuals to report illegal content. Implementation of these blocks, however, is often inconsistent across service providers. Some requests are apparently also issued directly to providers on an ad hoc basis, while individual companies have been willing to reverse or ignore censorship orders. In early 2012, the U.S.-based International Gay and Lesbian Human Rights Commission reported that a handful of mobile service providers had begun blocking its website on MCI instructions, though at least one operator did not comply.[30]

Besides the ministry, the independent Nawala Foundation provides a free DNS server enabling service providers to block hundreds of thousands of websites for pornography and gambling, among other categories; a 2013 news report said it had blocked 600 fraudulent stores.[31] It does not publish its database, and users generally learn sites are unavailable when they encounter the service's error

[24] Deibert, "Indonesia."
[25] Ratri Adityarani, "To Fight Terrorism Indonesia Blocks 300 Websites," *TechinAsia,* September 29, 2011, http://www.penn-olson.com/2011/09/29/terrorism-indonesia-blocks-300-websites/.
[26] Achmud Rouzni Noor II, "*Menkominfo Didesak Tutup 20 Situs Musik Ilegal*" [MCI Pushed to Close Down 20 Illegal Music Website], *Detik*, July 21 2011, http://www.detikinet.com/read/2011/07/21/161521/1686205/398/menkominfo-didesak-tutup-20-situs-musik-ilegal.
[27] *Mp3lagu, Pandumusica*, *Musik-flazher*, and *Freedownloadmp3* are no longer accessible, but it was not clear if they were shut down or voluntarily discontinued.
[28] "Indonesia's ISPs to Block Pirated Music Sites," *Jakarta Post,* July 6, 2012, http://www.thejakartapost.com/news/2012/07/06/indonesia-s-isps-block-pirated-music-sites.html.
[29] The full database is available at Trust Positif, http://trustpositif.kominfo.go.id/files/downloads/index.php?dir=database%2F.
[30] International Gay and Lesbian Human Rights Commission, "IGLHRC Website Banned," February 7, 2012, http://www.iglhrc.org/content/iglhrc-website-banned.
[31] "*Selain Situs Porno, DNS Nawala Hadang Toko Online Palsu*" [In Addition to Porn, DNS Nawala Blocks Fake Online Stores], *Detik*, April 22, 2013, http://inet.detik.com/read/2013/04/22/082832/2226480/323/selain-situs-porno-dns-nawala-hadang-toko-online-palsu.

message while browsing. Nawala provides a form for website owners subject to accidental blocking, though how it processes these complaints and how often it complies is not clear.[32]

The government has threatened service providers with intermediary liability for failing to implement censorship in the past. In 2011, Research in Motion (RIM) agreed to filter pornographic websites on their BlackBerry devices in Indonesia after the government regulator warned that the firm's market access could be restricted if it failed to comply.[33] When attempting to access a blocked site, BlackBerry users reportedly encounter a technical error rather than a message informing them that access to the site has been deliberately restricted.

In 2012, the Indonesian government made 45 requests to Google to delete videos on YouTube, an increase over the previous year.[34] Most requests cited religious reasons, likely in connection with the "Innocence of Muslims" video uploaded in the United States, ostensibly to promoting a movie that denounced Islam.[35] Many Indonesians joined restive street demonstrations to protest against the video, and police said the film drove an increase in terror plots, including one targeting the U.S. embassy in Jakarta.[36] Tifatul Sembiring publicly confirmed the government had requested that Google block 16 URLs to make it inaccessible in Indonesia.[37]

Some activists have successfully used digital tools to mobilize in defense of internet freedom. Strong opposition from civil society actors and even some ISPs has successfully derailed some plans for more stringent censorship. A draft Regulation on Multimedia Content introduced in early 2010 prompted a public outcry and fears of increased internet censorship, but it has remained on hold since. The blogging community also rallied round Prita Mulyasari, an internet user accused of criminal defamation in 2009, with a huge campaign called *Koin Keadilan* ("Justice Penny,") collecting tens of thousands of dollars on her behalf.[38]

Indonesia has enjoyed a thriving blogosphere since around 1999, though traditional media outlets—rather than blogs—typically cover important political developments and corruption investigations. Many of the earliest blogs were written by overseas Indonesians working in IT, until the younger generation adopted the medium to write about their daily lives. By 2005 and 2006, blogs had begun

[32] Nawala.org, http://www.nawala.org/

[33] Femi Adi, "RIM Says Committed To Indonesia, Will Block Porn on BlackBerrys," Bloomberg, January 17, 2011, http://www.bloomberg.com/news/2011-01-17/rim-says-committed-to-indonesia-will-block-porn-on-blackberrys.html; Ardhi Suryadhi, "Sensor di Blackberry terus diawasi" [Censorship on Blackberry Continuously Observed], Detik Inet, January 21, 2011, http://www.detikinet.com/read/2011/01/21/142056/1551687/328/sensor-di-blackberry-terus-diawasi.

[34] Google Transparency Report, http://www.google.com/transparencyreport/removals/government/ID/?by=product

[35] Ian Lovett, "Man Linked to Film in Protests Is Questioned," *New York Times*, September 15, 2012, http://www.nytimes.com/2012/09/16/world/middleeast/man-linked-to-film-in-protests-is-questioned.html?_r=2&ref=internationalrelations&; Michael Joseph Gross, "Disaster Movie," *Vanity Fair*, December 27, 2012, http://www.vanityfair.com/culture/2012/12/making-of-innocence-of-muslims.

[36] The Associated Press, "Indonesia Terror Attack: 'Innocence Of Muslims' Film Said To Fuel Embassy Plot," via *Huffington Post,* October 19, 2012, http://www.huffingtonpost.com/2012/10/29/indonesia-terror-attack_n_2038441.html.

[37] "*Soal Video 'Innocence of Muslims', Tifatul: Sudah 16 URL Diblokir*" ['Innocence of Muslims Video, Tifatul: 16 URLs Already Blocked], *Detik*, September 18, 2013, http://news.detik.com/read/2012/09/18/160114/2024496/10/soal-video-innocence-of-muslims-tifatul-sudah-16-url-diblokir?nd771104bcj.

[38] Mega Putra Ratya, "Penghitungan selesai total koin Prita Rp. 650.364.058" [Counting of Coins for Prita has collected a total of Rp. 650,364,058], *Detik*, December 19, 2009, http://m.detik.com/read/2009/12/19/113615/1262652/10/penghitungan-selesai-total-koin-prita-rp-650364058.

to specialize in various topics, including politics, economics, media, food, and entertainment. The *Salingsilang* directory of Indonesian bloggers counted over 5.2 million Indonesian blogs as of the end of 2011, covering issues such as popular culture and international current affairs.[39]

Indonesians are also avid users of social media, which a January 2013 survey listed as the nation's number one online activity, followed by instant messenger, search engines and e-mail.[40] Social media and communication apps, including YouTube, Facebook, and Twitter, are freely available, and Indonesia had the fourth largest number of Facebook users in the world in 2013, with 47 million accounts, according to one report.[41] President Susilo Bambang Yudhoyono, who began tweeting in April 2012 as @SBYudhoyono, gained two million followers in less than two weeks.[42] Another study described the Indonesian capital, Jakarta, as the world's most active city on Twitter, ahead of Tokyo, London, Sao Paulo, and New York. In addition to this distinction, Indonesia was the only country with two cities in the top ten; the second was Bandung, the capital of West Java.[43] As Facebook and Twitter use has grown, the popularity of blogging has declined.

Social media growth has produced new concerns about content manipulation. Analysts say anonymous or pseudonymous Twitter accounts circulating politically-motivated rumors and attacks on politicians may be part of sponsored campaigns to influence online discourse, or even blackmail well-known figures seeking to protect their reputations.[44] Social media pages have also been used by religious extremists. In mid-2013, an expert told the Associated Press that 50 to 100 militants had been recruited directly through Facebook in the past two years.[45]

VIOLATIONS OF USER RIGHTS

In September 2012, the Supreme Court finally cleared Prita Mulyasari on criminal and civil charges relating to a personal email she sent in 2009 complaining about a local hospital, after three weeks in jail, a suspended prison sentence, and earlier court orders that she pay the institution nearly $15,000 in damages. Yet the provisions of the law which allowed the spurious prosecution are still on the books, and the status of a promised reform remains unclear. Another legal ruling was less positive. In October 2012, the Constitutional Court rejected a civil society petition for judicial review of the 2011 State Intelligence Law, one of a handful of laws that allow authorities to intercept electronic communications with inadequate privacy protections.

---

[39] Salingsilang has since closed and no 2012 count is available.
[40] eMarketer, "Indonesia's Cities, Mobile Boosts Internet."
[41] Quintly, a company which provides statistics on global Facebook and Twitter use, is based in Germany. Facebook Country Stats, http://www.quintly.com/facebook-country-statistics?period=1month.
[42] "Yudhoyono's Arrival on Twitter Lets Down Pundits, Porn Star," *Jakarta Post*, April 15, 2013, http://www.thejakartapost.com/news/2013/04/15/yudhoyono-s-arrival-twitter-lets-down-pundits-porn-star.html.
[43] Semiocast, "Twitter Reaches Half a Billion Accounts, More Than 140 Million in the US," July, 30, 2012, http://semiocast.com/publications/2012_07_30_Twitter_reaches_half_a_billion_accounts_140m_in_the_US.
[44] "The Anonymous Denizens of the Indonesian 'Twitterverse,'" *Jakarta Post,* May 7, 2013, http://www.thejakartapost.com/news/2013/05/07/the-anonymous-denizens-indonesian-twitterverse.html.
[45] Niniek Karmini, "AP Exclusive: Facebook Broke Indonesia Terror Case," The Associated Press, June 21, 2013, http://bigstory.ap.org/article/ap-exclusive-facebook-broke-indonesia-terror-case.

Indonesia's constitution guarantees freedom of opinion in its third amendment, adopted in 2000.[46] The constitution also includes the right to privacy and the right to gain information and communicate freely.[47] These rights are further protected by various laws and regulations.[48] However, other laws limit free expression, despite legal experts' opinions that they conflict with the constitution.[49]

Approximately seven different laws involve internet use, the most prominent being the 2008 ITE Law. A 2011 State Intelligence Law introduced penalties of up to ten years' imprisonment and fines over $10,000 for revealing or disseminating "state secrets," a term which is vaguely defined vaguely in the legislation.[50] This framework provides authorities with a range of powers to penalize internet users, even though not all are regularly implemented.

Provisions of the 2008 ITE Law have been used repeatedly to prosecute Indonesians for online expression. The law's penalties for criminal defamation, hate speech, and inciting violence online are harsh compared to those established by the penal code. Sentences allowed under Article 45 can extend to six years in prison; the maximum under the penal code is four years, and then only in specific circumstances—most sentences are less than a year and a half.[51] Financial penalties show an even more surprising discrepancy. While the ITE law allows for fines up to one billion rupiah ($80,000), the equivalent amounts in the penal code have apparently not been adjusted for inflation. Article 310, for example, allows for paltry fines of IDR 4500 for both written and spoken libel.[52] As of May 1, 2013, that amounted to 40 cents.

The trial of housewife Prita Mulyasari for online defamation under the ITE Law is the most notable, and only concluded in September 2012. Police first detained Prita—who is widely known by her first name—for three weeks in 2009 for an email to friends that criticized her treatment at a private hospital in Tangerang city, Banten province.[53] The Tangerang District Court acquitted her on all criminal charges,[54] but prosecutors appealed to the Supreme Court, who sentenced her to a six-month suspended sentence and placed her on probation for one year 2011.[55] Though she did not

[46] Constitution of 1945, Article 28E(3).
[47] Constitution of 1945, Articles 28F and 28G(1).
[48] Among others, "Law No. 39 of 1999 on Human Rights," "Law No. 14 of 2008 on Freedom of Information," and "Law No. 40 of 1999 on the Press."
[49] Wahyudi Djafar et al., "*Elsam, Asesmen Terhadap Kebijakan Hak Asasi Manusia dalam Produk Legislasi dan Pelaksanaan Fungsi Pengawasan DPR RI*" [Assessment of the Human Rights Policy in Legislation and the Implementation of Parliament Monitoring], Institute for Policy Research and Advocacy, 2008.
[50] "Indonesian Parliament Passes Controversial Intelligence Bill," *Engage Media*, October 25, 2011, http://www.engagemedia.org/Members/emnews/news/indoneisan-parliament-passes-controversial-intelligence-bill.
[51] Human Rights Watch, "The Legal Framework: Criminal Defamation Law in Indonesia," in *Turning Critics Into Criminals,* May 4, 2010, http://www.hrw.org/node/90020/section/6.
[52] "*Kitab Undang-Undang Hukum Pidana"* [Criminal Law], available at *Universitas Sam Ratulangi* law faculty, http://hukum.unsrat.ac.id/uu/kuhpidana.htm#b2_16.
[53] Nadya Kharima, "*UU ITE Makan Korban Lagi*" [ITE Bill creates a victim again], *Primaironline*, May 28, 2009, http://primaironline.com/berita/detail.php?catid=Sipil&artid=uu-ite-makan-korban-lagi.
[54] Ismira Lutfia et al, "Prita Acquitted, But Indonesia's AGO Plans Appeal," *Jakarta Globe*, December 29, 2009, http://www.thejakartaglobe.com/home/prita-mulyasari-cleared-of-all-charges/349844.
[55] Faisal Maliki Baskoro and Rangga Prokosso, "Shock Guilty Verdict in Prita Mulyasari Saga," *Jakarta Globe,* July 9, 2011, http://www.thejakartaglobe.com/jakarta/shock-guilty-verdict-in-prita-mulyasari-saga/451797.

serve any jail time, the decision was criticized for setting a dangerous precedent.[56] The hospital also filed a parallel civil suit, despite widespread opposition from bloggers and civil society groups.[57] A court ordered her to pay the hospital 204 million rupiah ($14,300) in damages in the civil suit,[58] though the Supreme Court reversed the ruling on appeal.[59] In 2012, the Supreme Court reviewed the criminal case again, and found her innocent of all charges.[60]

The opposition to Prita's indictment did not prevent other, similar cases from going to trial. In 2012, Ira Simatupang, a doctor from a hospital in Tangerang, was charged over private emails to friends that accused a colleague of sexual harassment; the colleague denied the charge.[61] She was sentenced to five months' probation without jail time in July 2012. In November, the high court extended it to two years; she said she would appeal.[62]

Several other criminal cases disproportionate to the offence have been filed under the ITE Law in the past two years, including defamation charges filed by a member of parliament involving photos of her on Twitter,[63] and an SMS defamation complaint between two politicians.[64] No indictments were reported in these cases, which appeared to stall at the police level. Still, they increase self-censorship, and have begun to spur public demand for the law to be amended. Unfortunately, while an MCI spokesman promised to prioritize revising the online defamation provisions in 2013, they had yet to materialize during the coverage period of this report.[65]

In 2010, the government introduced a draft Computer Crimes Law into parliament.[66] Although mostly addressing business transactions, it also stipulated restrictions on computer and internet usage, and continued the trend of prescribing harsher penalties for offenses already criminalized

---

[56] "*Membaca Putusan Kasasi MA Dalam Kasus Prita*" [Reading into Supreme Court Decision in Prita Case], *Dunia Angara*, July 22, 2011, http://anggara.org/2011/07/22/membaca-putusan-kasasi-ma-dalam-kasus-prita/.

[57] Hertanto Soebijoto, "*Kasus Prita: Lima LSM Ajukan 'Amicus Curiae'*" [Prita case: 5 NGOs submit Amicus Curiae], *Kompas,* October 14, 2009, http://bit.ly/15BWpOA.

[58] Cyprianus Anto Saptowalyono, "*Humas PT Banten: Putusan Buat Prita Belum Berkekuatan Hukum Tetap*" [Banten Corporate Public Relations: Verdict for Prita Does Not Have Legal Power], *Kompas,* December 7, 2009, http://m.kompas.com/news/read/data/2009.12.07.13135791.

[59] Ina Parlina, "Supreme Court Overturns Acquittal of Housewife Prita," *Jakarta Post,* July 9, 2011, http://www.thejakartapost.com/news/2011/07/09/supreme-court-overturns-acquittal-housewife-prita.html.

[60] "Ini Dia Kronologi Prita Mencari Keadilan," *Detik*, September 18, 2013, http://news.detik.com/read/2012/09/18/124551/2023887/10/ini-dia-kronologi-prita-mencari-keadilan?nd771104bcj.

[61] "Prosecutor Demands Six Months in Prison for Doctor Who Sent Offensive Emails," *Jakarta Globe*, June 13, 2012, http://bit.ly/16AfH7O.

[62] Andi Saputra, "*Tangis Dr. Ira, Curhat Perilaku Cabul Atasan via Email Malah Dipidana*" [Dr Ira Sentenced for Obscene Email, Weeps," *Detik*, http://bit.ly/ZLLoRx.

[63] Lia Harahap, "*Kartika Siap Hadapi Laporan Anggota F-Gerindra Noura Gara-gara Twitter*" [Kartika ready to report Gerindra Faction Member Noura because of Twitter], *Detik*, May 13, 2011, http://bit.ly/18Ahben.

[64] Aprisal Rahmatullah, "*Yusuf Supendi Coba Jerat Presiden PKS Dengan Pasel ITE*" [Yusuf Supendi use ITE law to report PKS (Social Justice Party) President], *Detik,* March 29, 2011, http://news.detik.com/read/2011/03/29/180409/1604007/10/yusuf-supendi-coba-jerat-presiden-pks-dengan-pasal-ite.

[65] "*Kemenkominfo Prioritaskan Revisi UU ITE Tahun Ini*," *Kompas*, January 13, 2013, http://tekno.kompas.com/read/2013/01/16/11530420/Kemenkominfo.Prioritaskan.Revisi.UU.ITE.Tahun.Ini.

[66] The Computer Crimes Law is abbreviated as TPT or the "Tipiti bill" after its Bahasa name, *Tindak Pidana Teknologi Informasi*. Wendy Zeldin, "Indonesia: Cyber Crime Bill," Library of Congress, January 13, 2010, http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205401769_text.

under existing legislation.[67] Passage of the measure would potentially increase the number of laws regulating criminal defamation to eight, with each calling for a different sentence.

A draft law on ICT convergence to replace the Telecommunications Law, the Broadcasting Law, and possibly the ITE Law, is also under discussion. Critics have raised concerns that under the law, websites and other ICT applications would be required to obtain a license from the MCI for a fee, a process that could place restrictions on freedom of expression and the open source community, as well as Wi-Fi hotspots. [68] As of May 2013, neither of the drafts had been enacted.

The police,[69] the Indonesian Corruption Commission,[70] and the national narcotics board Badan Narkotika Nasional have legal authority to conduct surveillance in Indonesia,[71] while the anti-pornography law requires cybercafe owners to monitor their customers. There is little oversight and there are few checks in place to prevent abuse of monitoring powers used to combat terrorism, the best known use of surveillance techniques. Surveillance concerns intensified in 2011 with the passage in October of a new State Intelligence Law, though several problematic provisions were removed prior to passage, partly thanks to civil society activism.[72] International and domestic human rights groups said the law authorized the state intelligence body, Badan Intelijen Negara, to intercept communications. Although a court order is required in most cases, concerns remain that due to limits on judicial independence, permission will be granted too easily.[73] The law is one of at least nine that allow surveillance or wiretapping, yet the only other law that explicitly requires judicial oversight involves narcotics. Even then, the procedures are unclear. In October 2012, the Indonesian Constitutional Court rejected a request for judicial review of the State Intelligence Law by the Alliance for Independent Journalists, four other civil society groups, and thirteen individuals.[74]

In 2013, news reports said the MCI was investigating three ISPs after the University of Toronto-based Citizen Lab detected FinSpy spyware from the FinFisher surveillance apparently being operated by the providers or their customers.[75]

---

[67] Muhammad Aminudin, "Cyber Crime Menggurita, DPR Kebut UU Tindak Pidana TI" [Cybercrimes Imminent, Parliament Speedup Cybercrime Law], *Detik*, March 3, 2012, http://inet.detik.com/read/2012/03/25/091604/1875607/399/cyber-crime-menggurita-dpr-kebut-uu-tindak-pidana-ti.
[68] Harry Sufehmi, Twitter post, October 8, 2010, 23:30, https://twitter.com/sufehmi.
[69] "Law No. 16 of 2003 on the Stipulation of Government Regulation in Lieu of Law No. 1 of 2002 on the Eradication of Crimes of Terrorism" (State Gazette No. 46 of 2003, Supplement to the State Gazette No. 4285), available at: http://bit.ly/18zYER7.
[70] Ministry of State Secretariat of the Republic of Indonesia, "Law No. 30 of 2002 on the Anti-Corruption Commission," http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=300&filename=UU_no_30_th_2002.pdf.
[71] Ministry of State Secretariat of the Republic of Indonesia, "Law No. 35 of 2009 on Narcotics," http://bit.ly/19etZoD.
[72] International Crisis Group, "Indonesia: Debate over a New Intelligence Bill," Asia Briefing no. 124, July 12, 2011, http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/B124-indonesia-debate-over-a-new-intelligence-bill.aspx.
[73] Human Rights Watch, "Indonesia: Repeal new Intelligence Law. Overbroad Provisions Facilitate Repression," October 26, 2011, http://www.hrw.org/print/news/2011/10/26/indonesia-repeal-new-intelligence-law.
[74] Arif Abrams, "*MK Tolak Uji Materi UU Intelijen Negara*" [The Court Rejected State Intelligence Law Judicial Review], *Kontan,* October 10, 2012, http://nasional.kontan.co.id/news/mk-tolak-uji-materi-uu-intelijen-negara.
[75] Enricko Lukman, "Indonesian Top Internet Service Providers Accused of Spying on Users," March 18, 2013, http://www.techinasia.com/indonesian-top-internet-service-providers-accused-spying-users/.

Mobile phone users are technically required to register their numbers with the government by text message when they buy a phone, though this obligation is often ignored. Some telecommunication companies are known to have complied with law enforcement agencies' requests for data. In 2011, amidst concerns that the RIM's Blackberry encrypted communication network would hinder anti-terrorism and anti-corruption efforts, the company reportedly cooperated with the authorities in isolated incidents,[76] and agreed to establish a local server. When they developed this in Singapore instead of Indonesia, the government threatened to introduce a regulation requiring telecommunications companies to build data centers in-country. This has yet to materialize, and RIM has resisted the pressure,[77] although some recent news reports said it was losing its market dominance.[78]

There have been no reports of extralegal attacks, intimidation, or torture of bloggers or other internet users. However, it is common for police—and sometimes Islamic fundamentalist groups—to conduct searches of cybercafes without prior notice, since the venues are perceived as promoting immoral conduct.[79] Most of the searches are conducted without warrants and are rarely followed by court proceedings, leading observers to believe police carry out some raids to extract bribes from the owners.

Politically motivated cyberattacks against civil society groups have not been reported in Indonesia. However, several government websites have been targeted in the past.

[76] Arientha Primanita and Faisal Maliki Baskoro, "Pressure on BlackBerry Maker to Build Servers in Indonesia," *Jakarta Globe*, December 14, 2011, http://www.thejakartaglobe.com/business/pressure-on-blackberry-maker-to-build-servers-in-indonesia/484588.

[77] "*RIM: Buat Apa Bangun Server Blackberry di Indonesia*" [RIM: Create a Server for BlackBerry in Indonesia?], *Detik,* February 21, 2012, http://inet.detik.com/read/2012/02/21/151942/1847914/317/rim-buat-apa-bangun-server-blackberry-di-indonesia.

[78] "BlackBerry Searching High and Low in India, Indonesia," Reuters, February 4, 2013, http://in.reuters.com/article/2013/02/04/blackberry-india-asia-idINDEE91300220130204.

[79] "Shariah Police Arrest Five in Banda Aceh Punk Raid," *Jakarta Globe,* September 5, 2012, http://www.thejakartaglobe.com/archive/shariah-police-arrest-five-in-banda-aceh-punk-raid/.
"Police Bust High School Students for Cutting Class in Favor of Facebook," *Jakarta Globe,* March 3, 2010, http://www.thejakartaglobe.com/home/police-bust-high-school-students-for-cutting-class-in-favor-of-facebook/361673.

IRAN

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	21	22
Limits on Content (0-35)	32	32
Violations of User Rights (0-40)	37	37
Total (0-100)	**90**	**91**

* 0=most free, 100=least free

POPULATION: 78.9 million
INTERNET PENETRATION 2012: 26 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- In a bid to increase domestic speeds and decrease international data costs, authorities throttled encrypted traffic from outside connections and set out to transfer Iranian content to domestically-hosted servers (see **OBSTACLES TO ACCESS**).
- Blogs and news sites which support President Ahmadinejad were blocked as part of a larger conflict between conservative factions due to the June 2013 presidential election (see **LIMITS ON CONTENT**).
- The government has moved to more sophisticated instruments for blocking text messages, filtering content, and preventing the use of circumvention tools in anticipation of the election (see **LIMITS ON CONTENT**).
- Sattar Beheshti, a prominent blogger and critic of Ahmadinejad, was killed while in police custody (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

This report covers events between May 1, 2012 and April 30, 2013. On June 14, 2013, Iranians took to the polls to elect a new president for the first time since the deeply-flawed presidential elections of 2009, which led to large-scale protests and a violent crackdown on supporters of the opposition "Green Movement." With an eye on preventing a repeat of 2009, authorities waged an aggressive campaign of filtering websites, blogs, and even text messages that expressed support of certain political candidates. In the week leading up to the vote, the disruption of services reached its peak. Encrypted traffic was throttled to 1 to 5 percent of normal speeds and the authorities used a "white list" to block all international connections that were not pre-approved. Because of this, most online tools that allow users to circumvention censorship and communicate anonymously were blocked or dysfunctional. A large number of Iranian activists and journalists were targeted by sophisticated malware attacks or smear campaigns on social media.

Hassan Rouhani, a cleric and political opponent of President Mahmoud Ahmadinejad, was commonly seen as the most moderate or pragmatic candidate in the race. This also applied to issues of internet freedom, on which he stated that some Iranian authorities were "living in the 19th century while today's world is the information world."[1] Rouhani was elected president after only the first round with just over 50 percent of votes and took office on August 3, 2013.

INTRODUCTION

The internet was first introduced in Iran during the 1990s to support technological and scientific progress in an economy that had been badly damaged by eight years of war with Iraq. Until 2000, the private sector was the main driver of internet development. This changed under the government of the reformist President Mohammad Khatami (1997–2005), when the authorities invested heavily in expanding the internet infrastructure, but also began to clamp down on free expression online. Meanwhile, Supreme Leader Ali Hosseini Khamenei first asserted control over the internet through a May 2001 decree that centralized service providers' connections to the international internet. Internet filtering, which began toward the end of the Khatami presidency in 2005, has become more severe since the disputed presidential election in June 2009.

Alongside the expansion of existing controls, in July 2011 the Iranian authorities began referring to the creation of a "National Information Network" (NIN), ostensibly to create a "safe internet."[2] Though confirmed details of the plan remain sketchy, objectives include the mandatory registration of internet protocol (IP) addresses, the moving of government-approved websites to servers based inside the country, and the launching of Iranian equivalents of major online services like e-mail, social-networking sites, and search engines. These measures will restrict online anonymity, increase monitoring capabilities, and allow Iranian authorities to control access to particular international

[1] *Iranian Internet Infrastructure and Policy Report, April – June 2013*, June 2013, Small Media, available at http://smallmedia.org.uk/InfoFlowReportAPRIL.pdf.http://smallmedia.org.uk/IIIPJune.pdf.
[2] "Iran to launch national data network," Press TV, August 10, 2011, http://www.presstv.ir/detail/193306.html;.

communication flows during periods of political unrest without the need to shut down all domestic services.

Despite all of these limitations, the internet remains the only viable means for Iranian citizens and dissenters to obtain news and organize themselves. Traditional media outlets are tightly controlled by the authorities, and satellite broadcasting from outside Iran is subjected to heavy jamming. Paralleling the rise in censorship, the use of virtual private networks (VPNs), proxies, and other circumvention tools has also grown dramatically since 2009. Nonetheless, authorities blocked these tools in March 2013, forcing users to switch to a different set of well-known tools, which were then blocked two months later. These actions were taken as a set of broader measures to increase security and cut down on dissent in the run up to the June 2013 presidential election. While sites related to discriminated religions, liberal opposition movements, human rights, and international news outlets remain blocked, the past year saw an increase in filtering of websites and blogs supportive of President Mahmoud Ahmadinejad, whose relationship with the Supreme Leader has soured. Currency-exchange sites were also blocked as the government sought to control the devaluation of the Iranian *rial*. Finally, numerous activists and ordinary Iranians remained in prison, while many more were detained over the past year. The brutality of the security forces is well-known, and this year the death of blogger Sattar Beheshti caused outrage after it was exposed over social media.

OBSTACLES TO ACCESS

Current statistics on the number of internet users in Iran are inconsistent and highly disputed, though most observers agree that usage continues to grow. On the one hand, data from the Statistical Center of Iran, a government body, suggests that over 21 percent of the country's 20.3 million households were connected to the internet in 2011. These statistics also put the number of total internet users at 11 million or a penetration rate of almost 15 percent.[3] On the other hand, Iran's Center for Managing National Development of Internet (MATMA), a government-affiliated organization, claimed that 60 percent of Iranians are connected to the internet, though the methodology of the study includes the use of cybercafes. Iran's Media News reports that around 13 percent of Iranian internet users have access to high-speed internet, while 84 percent still rely on dial-up connections.[4]

In contrast, the International Telecommunication Union (ITU) estimated the number of internet users in Iran at 26 percent for 2012.[5] Citing the Iranian Information Technology Organization as its source, the ITU also claimed that there are only four fixed-broadband subscriptions per every 100

[3] "21.4 of Iranian families have access to the Internet", Wimax News, accessed June 24, 2013, http://wimaxnews.ir/NSite/FullStory/News/?Id=3190.
[4] Radio Zamaneh, "Most internet users still use dial-up in Iran," Payvand Iran News, March 24, 2012, http://www.payvand.com/news/12/mar/1222.html.
[5] "Percentage of individuals using the Internet," International Telecommunications Union, accessed April 25, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

inhabitants.[6] Less than four percent of Iranians have access to a high-speed internet connection of at least 1.5 Mbps.[7] In terms of user demographics, men are 58 percent more likely to use the internet than women, and 94 percent of fixed-internet subscriptions are located in urban areas. [8]

Internet speeds are incredibly slow in Iran, which ranked 164 out of 170 countries in a recent study.[9] Furthermore, Iranians have the most expensive internet service in the world when price is calculated relative to speed, quality, and download capacities.[10] In December 2012, the Communication Regulatory Authority approved an increase of broadband internet tariffs by about 50 percent, resulting in a cost increase for end users by about 10 to 15 percent. According to the CRA, the change in price is due to fluctuations in foreign exchange rates which have increased the cost of international data traffic.[11]

A directive by the CRA asking all ISPs to separate internet traffic from intranet traffic, in line with the continued implementation of the National Information Network (NIN), has resulted in a significant increase in speeds when accessing sites hosted inside Iran.[12] It has been said that the full implementation of the NIN plan will result in a tenfold increase in the country's bandwidth.[13] However, the speed of access to sites hosted outside Iran remains very low and the connection is one of the most unstable in the world.[14] A number of major ISPs suffer an average of 10 to 20 percent of packet loss. Renesys, a global network monitoring service, also reported substantial and frequent disruptions to the connectivity of specific ISPs in Iran.[15] (For more on the National Information Network, please see "Limits on Content.")

Iran's mobile telephone sector continues to grow as well. According to the ITU, Iran had a mobile phone penetration rate of 76.9 percent, up from 41.7 in 2007.[16] Iran is also considered the largest potential market for mobile phones in the Middle East and is reportedly investing heavily in its mobile infrastructure.[17] RighTel, the third largest mobile service provider of Iran, increased its coverage for 3G and now has 17 cities under partial 3G mobile coverage. However, Iran's security-

[6] "Fixed (wired)-broadband subscriptions," International Telecommunications Union, accessed April 25, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[7] "Less than 1 percent of Iranians have high-speed internet," Trend, September 3, 2012, http://en.trend.az/regions/iran/2061143.html.
[8] "21.4 of families have access to the Internet", Wimax News, accessed June 26, 2103 http://wimaxnews.ir/NSite/FullStory/News/?Id=3190.
[9] Radio Zamaneh, "Most internet users still use dial-up in Iran," Payvand Iran News, March 24, 2012, http://www.payvand.com/news/12/mar/1222.html.
[10] Radio Zamaneh, "Most internet users still use dial-up in Iran," Payvand Iran News.
[11] "The effects of sudden increase of cost accessing Internet,", ISNA, accessed 26 June, 2013, see http://bit.ly/ZdJ7o1.
[12] "The separation of Internet and Intranet traffic has been initiated", IT Iran, accessed 26 June, 2013 http://itiran.com/?type=news&id=17699.
[13] "Launch of National Information Network, First half of this year", IT Iran, accessed 26 June, 2013 http://itna.ir/vdcfmcd0.w6dy0agiiw.html.
[14] "BGP Update Report", SecLists.Org Security Mailing List Archive, accessed 26 June, 2013 http://seclists.org/nanog/2012/Nov/312.
[15] Renesys Iran Internet Events Bulletin http://www.renesys.com/eventsbulletin-cgi-bin/mt-search.cgi?search=iran&IncludeBlogs=1&limit=20.
[16] "Mobile cellular," International Telecommunications Union, accessed April 25, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[17] "Surfing the web on am iPhone in Iran, Guardian, accessed June 24, 2013, http://socialenterprise.guardian.co.uk/it/articles/media-network-partner-zone-publici/web-iphone-iran.

driven view of the internet has slowed the development of internet infrastructure in the country. For example, a plan to make high-speed wireless internet available in public spaces in Tehran, proposed by the ISP MobinNet, was blocked by the CRA after it failed to provide a license to the company with no official explanation.[18] In April 2013, the Psychological Association of Qom Hawza sent a letter to the parliament requesting that RighTel's 3G service be blocked in order to prevent "the breakdown of Iranian families" and "immorality among the youth."[19] The use of mobile wireless is often criticized for allowing video calls between members of the opposite gender.

In Iran, the limitations imposed on ICTs closely follow the country's internal political dynamics. For example, beginning around October 6, 2012, and timed with sporadic protests over economic conditions, the Telecommunications Company of Iran temporarily blocked several types of foreign-hosted media files. According to initial reports, this blocking targeted audio (.MP3), video (.MP4, .AVI), and Adobe Flash/Shockwave content.[20] Over late 2012 and early 2013, authorities periodically throttled the speeds of virtual private networks (VPNs) in order to dissuade Iranians from their use. In anticipation of the June 2013 presidential elections, the authorities blocked all circumvention tools in March 2013 (see "Limits on Content") and engaged in extreme throttling of encrypted traffic, with secure traffic running at between one to five percent of the speeds for unsecured and domestic traffic. Authorities effectively ran a "white list" of permitted applications and services, using deep packet inspection (DPI) to monitor content and distinguish between unencrypted, encrypted, and abnormal traffic. International connections and traffic that did not fall within an approved "white list" were throttled and terminated after 60 seconds. Domestic traffic, which is monitored, did not fall under these restrictions.[21]

In a bid to decrease costs and improve speeds, authorities have been looking to move Iranian content to servers hosted within the country. This would allow the state-owned internet company to avoid paying high international traffic costs, especially taxing during this time of currency fluctuations brought on by economic sanctions. According to Iran's Deputy Minister of ICT, the government has already moved more than 90 percent of its websites to providers based inside the country and is now pressuring privately-owned websites to follow suit.[22] Compliance has been limited, however, primarily because hosting services offered by Iranian companies are significantly more expensive than those of their overseas competitors due to economic sanctions on technology imports.

Iran's deputy minister for ICT has stated that more than 90 percent of the government's websites have been moved to domestic servers, and the authorities are pressuring privately-owned websites to follow suit. However, since Iranian companies cannot offer the same low prices as many

[18] "License to launch a public WiFi network was not issued", Mehrnews, accessed June 24, 2013, http://www.mehrnews.com/detail/News/1640766.
[19] *Iranian Internet Infrastructure and Policy Report, March – April 2013*, April 2013, Small Media, available at http://smallmedia.org.uk/InfoFlowReportAPRIL.pdf.
[20] "Some audio and video formats have been blocked in Iran", BBC Persian, accessed June 24, 2013, http://www.bbc.co.uk/persian/science/2012/10/121005_na_audio_and_video_format_blocked_in_iran.shtml.
[21] *Iranian Internet Infrastructure and Policy Report, March – April 2013*, April 2013, Small Media, available at http://smallmedia.org.uk/InfoFlowReportAPRIL.pdf.
[22] "The ministry promises 20 Mbps internet again," [translated] Mashregh News, July 23, 2011, see http://bit.ly/16tlGLu.

international companies, many have yet to make the move. Still, authorities have already requested that ISPs separate traffic destined to servers within the country from that traffic going outside, resulting in relatively high-speeds for accessing approved content, versus incredibly slow access to websites hosted internationally that are already filtered. Many observers and former officials, however, are pessimistic about the situation of the internet in the country. In an interview, Seyed Ahmad Motamedi, a communications minister under former president Khatami, referred to the country's ICT sector as unsustainable and "a serious catastrophe."

The telecommunications industry in Iran is tightly controlled by the government or related entities. In recent years, the role of the Islamic Revolutionary Guards Corps (IRGC)—a politically important branch of the security forces that also controls large sections of the economy—in the ICT sector has notably increased.[23] In September 2009, for example, the IRGC purchased a controlling stake in the Telecommunications Company of Iran (TCI), the country's main provider of internet and mobile phone services. The Data and Communication Company (DCC), which operates under the TCI, retains a monopoly on internet traffic flowing in and out of Iran. Other providers must purchase bandwidth from the DCC. Direct access to the internet via satellite is only permitted to certain institutes and is prohibited for personal use. The mobile phone market is under similar state influence. IranCell, the second mobile operator behind the TCI, is owned in part by a web of proxy companies controlled by the IRGC (there are a number of high profile IRGC ex-commanders among its management). The third operator, RighTel, was launched in early 2011. It, too, is a government-owned entity.

There is no independent regulatory body for ICTs in Iran. The Communications Regulatory Authority (CRA) is responsible for telecommunications licensing. It is part of the Ministry for Information and Communication Technologies and its head is appointed by the minister.[24] In March 2012, the broader decision-making process related to ICTs underwent a change, when Iran's Supreme Leader Khamenei issued a decree establishing "The Supreme Council on Cyberspace" (SCC). The SCC is intended to provide a centralized focal point for policy-making and regulation of Iran's virtual space, effectively removing such authority from the executive, legislative, and judiciary branches of the government and bringing it under Khamenei's direct control. Observers believed this reflected Khamenei's dwindling trust of President Ahmadinejad and his hesitation to leave such an important area of policy under the president's authority.

LIMITS ON CONTENT

The Iranian authorities continued to restrict access to tens of thousands of websites, particularly those of international news sources, the opposition Green Movement, ethnic and religious minorities, and human rights groups. A member of the Commission to Determine the Instances of Criminal Content (CDICC) stated in April 2013 that about 1,500 "anti-religious websites,"

[23] "The Revolutionary Guards is entering the IT market," Digarban, December 12, 2011, http://www.digarban.com/node/3715.
[24] Communications Regulatory Commission of Iran, accessed July 31, 2012, http://www.cra.ir/Portal/Home/.

including sites that promote the Wahhabi or the Baha'i faiths, are blocked each month.[25] Major international social media tools, such as the social-networking site Facebook, the video-sharing portal YouTube, the microblogging service Twitter, and the photo-sharing application Flickr, are blocked. In late 2012 and early 2013, several political and economic events sparked new reactions by those in charge of the filtering system in Iran, including the devaluation of Iran's currency and the increasing frictions among pro-state (conservative) bloggers.

Iranian authorities employ a centralized filtering system that can effectively block a website within a few hours across the entire network in Iran. Private ISPs are forced to either use the bandwidth provided by the government or route their traffic (which contains site-visit requests) through government-issued filtering boxes developed by software companies inside Iran. The filtering boxes search for banned text strings—either keywords or domain names—in the URL requests submitted by users, and block access accordingly. On April 15, 2012, the Ministry of Communication's ICT Research Center announced a plan to create a local and integrated system for "refining" internet content, rather than implementing filters at the country's internet gateways as it does currently. The Research Center, in describing the reasoning behind the plan, stated that "although the internet has many advantages, it is polluted with immoral websites, and can endanger society's moral health."[26]

In 2013, Mehdi Akhavan Behabadi, the Secretary of the Supreme Council of Cyberspace, announced a plan to change the filtering system from "URL Filtering" to "Content Filtering" ahead of the presidential election in June 2013. This change would potentially increase restrictions on content that the state does not currently sanction.[27] The list of cybercrimes was also updated ahead of the elections. According to the updated list, the following activities are considered to be illegal: encouraging people to boycott the elections by publishing online content, publishing fake results of surveys about the elections, and publishing any content that mocks the election or its candidates.[28]

Internet traffic over cell phones is subjected to a similar level of restrictions as fixed-line connections. Iranian mobile users also do not have access to major app stores such as Apple's iTunes or Google Play, either due to a blockage by the Iranian government (in the case of the former) or by the providing company (with regard to the latter). Warnings were also issued against the potential misuse of SMS advertisements ahead of the presidential election. According to the director of Iran's Information Technology and Digital Media Development Center, Hassan Alizadeh, the content of bulk instant messages would be supervised more heavily.[29] According to a report from the official website of *Ansar-e Hezbollah*, the conservative Islamic paramilitary group

25 "Internet delivery case is likely suit," [translated] IT Analyze.ir, April 17, 2013, http://itanalyze.com/news/2013/04/17/20866.php?utm_source=feedly

26 "The new scheme of ICT research center of Ministry of Communications for filtering", Jam News, accessed June 24, 2013, http://www.jamnews.ir/NSite/FullStory/News/?Id=74737.

27 "Proposition of establishment of special court for filtering/sites that receive government subsidies", Khabar online, accessed 24 June, 2013, http://www.khabaronline.ir/detail/275237/ict/ict.

28 "Examples of presidential elections were announced in the criminal context" [translated], Baharnews.ir, accessed June 24, 2013, http://www.baharnews.ir/vdci.zavct1avubc2t.html.

29 "Precise control over the content of bulk SMS, Non Iranians to be prevented from using SMS", Mehrnews, accessed June 24, 2013, http://www.mehrnews.com/fa/newsdetail.aspx?NewsID=1731245.

warned that phones with internet connections should be considered a threat to the Islamic Republic, especially ahead of the upcoming election, as they are at risk of being hijacked by Western powers to incite post-election violence.[30] Around politically sensitive dates, authorities have filtered SMS messages or even blocked all text messaging capabilities to prevent the spread of information. For example, on April 4, 2013, short-message service (SMS) text messages containing the word "Mashaie" were blocked, referring to Esfandiar Rahim Mashaei, the presidential candidate supported by Ahmadinejad. Texts containing political slogans related to Mashaie and Ahmadinejad had also been blocked in the past.

On September 24, 2012, Iran blocked access to Gmail in a move that caused outrage among internet users and even some Iranian officials who were using the site as their primarily e-mail service. It was later said that the Gmail block was an "involuntary" consequence of trying to reinforce censorship of Google's YouTube video-sharing site in response to the inflammatory, anti-Islam clip "Innocence of Muslims."[31] Mohammad Reza Miri, a member of the telecommunications ministry committee, was quoted as saying the ministry lacked the "technical knowhow to differentiate between these two services."[32] The provided explanation did not seem to make sense, however, since at the time of blocking Gmail, YouTube was already blocked. Nonetheless, the Gmail blockage was lifted after a few days, mainly due to public pressure. It seems these measures are designed to frustrate users and eventually force them to seek more easily-monitored alternatives based in Iran. Although many Iranians have been able to access the blocked platforms using various circumvention techniques, the authorities have actively worked to disrupt such efforts, forcing users to constantly search for new solutions.

In another attack on Google's services, Adwords, its online advertising service, was also blocked by the Iranian authorities. In spite of economic sanctions and various difficulties, many Iranian businesses had been using Adwords to advertise their products on Google. These small businesses have suffered greatly as the result of the Adwords blockage.[33] There are also reports that while access to the main Google domain is available, other country-specific domains are blocked. These include Google Canada, Germany, UK, Japan, China, Netherlands, France, Italy, and Spain.[34] This restriction may be in place in an attempt to maintain tighter control on Iranian users' access to Google services. Voice over Internet Protocol (VoIP) and chatting services are also disrupted inside Iran, whether by the intentional throttling of VoIP-linked data speeds or the blocking of services altogether. According a report published in April 2013, the government-owned TCI is the only ISP to not officially block services such as Viber, Skype, ooVoo, and Yahoo Messenger.[35]

---

[30] "Serious weakness in the management of satellite discussion", Yalasarat, accessed June 24, 2013, http://yalasarat.com/vdcipvar.t1avv2bcct.html.
[31] "Internet in Iran: Google not filtered, Gmail filtered", BBC Persian, accessed June 24, 2013, http://www.bbc.co.uk/persian/iran/2012/09/120924_asf_iran_gmail_block.shtml.
[32] "Iran unblocks access to Gmail", AFP, accessed June 24, 2013, https://www.google.com/hostednews/afp/article/ALeqM5hR36K96WD9GYoBp51umwiKBb0nYQ?docId=CNG.94fb48b493fa1aacf4fc347be86ebaf0.7c1.
[33] "Google ads in Iran has become more complicated", BBC Persian, accessed June 24, 2013, http://www.bbc.co.uk/persian/science/2012/09/120907_na_google_adwords_banned_in_iran.shtml.
[34] "Google country domain filtering", ITNA, accessed June 24, 2013, http://www.itna.ir/vdchqkni.23nzkdftt2.html.
[35] *Iranian Internet Infrastructure and Policy Report, March – April 2013*, April 2013, Small Media, available at http://smallmedia.org.uk/InfoFlowReportAPRIL.pdf.

This coverage period was marked by increased frictions within pro-regime conservatives, mainly between the pro-Ahmadinejad and pro-Khamenei camps, catalyzed by the June 2013 presidential election. There was a sustained wave of filtering of blogs supportive of President Ahmadinejad, in addition to campaign sites linked to presidential candidate Mashaei and former president Mohammad Khatami, whom many Iranians called on to run in the elections. Iran's Supreme Leader expressed his approval of filtering out pro-Ahmadinejad blogs while speaking at a gathering of university students.[36] Ahmadinejad, however, has confronted the judiciary to free his many online supports who have been arrested (see "Violations of User Rights" for more information on the arrest of bloggers).[37] The Persian-language Wikipedia page for Ahmadinejad was also reportedly blocked at points during the coverage period for containing "insults"' to the president, according to the head of the Commission to Determine the Instances of Criminal Content.[38]

Several news websites associated with high-profile conservatives were also blocked. The website of Alef News, which belongs to Tehran's conservative parliamentarian Ahmad Tavakkoli, was filtered after publishing news on the corruption of Iran's powerful Larijani brothers, who are in top positions in the Islamic Republic. Tabnak and Baztab Emrooz, news websites associated with Mohsen Rezaie, a former IRGC commander and a candidate in the upcoming presidential election, were also blocked due to the content of user comments. All of these sites were unblocked after several days, apart from Baztab Emooz, which has been taken down completely.

In an attempt to control the spiraling devaluation of the *rial*, Iran's currency, authorities blocked a majority of websites and applications that provide data on foreign exchange trading and gold markets. Many ordinary Iranians are converting their rials into foreign currencies and gold in an effort to preserve the value of their savings. Authorities took a multifaceted approach to the blocking. Any references to the price of the dollar, currency, and gold coins were filtered in mobile text messages.[39] In addition, internationally-hosted sites were blocked and individuals behind sites hosted within Iran were arrested or intimidated.[40] Some local sites were also blocked to traffic from outside Iran, like the domestically-hosted website of the Association of Iranian Exchanges, an independent, apolitical and nonprofit organization of currency traders licensed by the Central Bank of Iran.[41] Some sites were allowed to operate again on the condition that they only displayed the government-established exchange rates, rather than the market rate.[42] The move to restrict foreign

[36] "Remarks in meeting with students", Khamenei.ir, accessed June 24, 2013, http://farsi.khamenei.ir/speech-content?id=20686.
[37] "I personally follow up the blogger's arrest,partisanship is a symbol of tribalism" , Mehrnews, accessed June 24, 2013, http://www.mehrnews.com/detail/News/1668142.
[38] *Iranian Internet Infrastructure and Policy Report, March – April 2013*, April 2013, Small Media, available at http://smallmedia.org.uk/InfoFlowReportAPRIL.pdf.
[39] "The words gold,foreign exchange,coin, dollar have been blocked in SMS system", Smsmart, accessed June 24, 201, see http://bit.ly/1eK6FY7.
[40] Examples of these websites were parstools.com, zar.ir, eranico.com and mazanex.com.
[41] The website of the Association of Iranian Exchanges is kanoonsarafan.com.
[42] "Sites announcing the rate of gold and foreign exchange have been blocked", Radio Farda, accessed June 24, 2013, http://www.radiofarda.com/content/f4_iran_ban_exchange_rate_websites/24727416.html.

access to domestically-hosted websites was interpreted by many as a sign of what may come after the full implementation of the National Information Network.[43]

The online restrictions were not limited to political and economic content. Persian-language music blogs, dating sites, digital security information, and movie download hubs were subjected to increased filtering and content takedown orders. For instance, Travian, a popular online roleplaying game available in Persian, was blocked despite having obtained a license from the Ministry of Culture and Islamic Guidance. According to Fars News Agency, Travian was blocked in order to support "the development of domestic online game companies," "to protect personal information," and "protect against the transfer of money out of the country."[44] The founder of the first domestically produced game, "Asmandez," reacted to the incident saying that filtering is not a solution to support national game production.[45] Travian was unblocked on January 10, 2013, but the company notified users that the website will be completely shut down on March 21, 2013. As of December 2012, Travian had 150,000 users in Iran, of which 100,000 were active.[46] The Persian-language version of the site now redirects to the English version.

Aside from filtering, the regime also employs administrative measures to remove unwanted content from the web. The 2009 Computer Crime Law (CCL) makes service providers, such as blogging platforms, responsible for any content that appears on their sites. This has led to the suspension of blogs or shuttering of news websites hosted on platforms inside Iran, under orders from government officials. Website owners have been forced to register their sites with the Ministry of Culture and have then received requests to remove particular posts deemed unacceptable by the government. According to Alireza Shirazi, the founder and manager of Blogfa, such massive censorship has damaged the Iranian blogosphere by discouraging users from blogging.[47] Mehdi Botourabi, the director of the popular blogging platform Persianblog, also stated that the censorship of blogs has increased exponentially. According to him, new blocking requests were occurring at a rate of six times more than in 2011.[48] As with blocking, the targets of such censorship have included websites and blogs associated with high-ranking officials.

In a change from previous practices, there were reports of incidents in which hosting companies were ordered to directly remove content from websites without any notification to the website owners. For instance, one post on the site Weblognews that criticized the internet censorship method in Iran was deleted by the host company without notifying the site owners.[49] Weblognews is one of the prominent conservative websites that publishes news from around the Persian blogosphere and the internet. Nonetheless, Iranian officials continue to insist that censorship in Iran

[43] Iranian Internet Infrastructure And Policy Report, January 2013 http://smallmedia.org.uk/sites/default/files/reports/IIIP01.pdf.
[44] "The online game "Travian" has been filtered", Farsnews, accessed June 24, 2013, http://www.farsnews.com/newstext.php?nn=13911013000562.
[45] "Supporting local games doesn't mean filtering", ITNA, accessed June 24, 2013, http://itna.ir/vdcdsn0x.yt0o96a22y.html.
[46] "Why Travian has been filtered in Iran?" , BBC Persian, accessed June 24, 2013, http://www.bbc.co.uk/persian/science/2013/01/130104_na_travian_blocked_iran.shtml.
[47] Ibid.
[48] "Persian blog manager: compared to last year, weblog filtering has increased 6 times", Kalameh, accessed June 24, 2013, http://www.kaleme.com/1391/07/19/klm-115654/.
[49] "A strange incident", Weblognews, accessed June 24, 2013, http://weblognews.blog.ir/post/2.

is done a lawful manner. According to the Director of the Internet Unit at the Center for Digital Media at the Ministry of Culture and Islamic Guidance, "unlike some countries like the U.S., where internet monitoring is done in a dictatorial manner, in Iran, refining websites is based on laws with orders from the Working Group to Determine Instances of Criminal Content online or by judiciary officials, in a democratic and completely lawful manner."[50]

In an effort to show that content filtering is based on a legal framework, institutions to oversee internet filtering have been created. The Committee in Charge of Determining Unauthorized Websites is empowered to identify sites that carry forbidden content and report that information to the TCI and other major ISPs for blocking. The committee is headed by the prosecutor general and other members are representatives from 12 governmental bodies. The CLL also identifies the violations that might result in a website being marked for filtering. These are defined very broadly and range from insulting religious figures and government officials to distributing pornographic content and the use of illegal circumvention tools.[51]

In practice, little information is available about the inner workings of the committee, and censorship decisions are often arbitrary and nontransparent. According to the law, the committee should meet biweekly to decide on any website bans, though the bulk of filtering decisions are likely made upon discovery of objectionable content, or by a small technical team. In addition, owners of websites registered with the Ministry of Culture have complained that they received no explanation when their websites were filtered.[52] The authorities claim there is a procedure for disputing filtering decisions. However, the process is highly inefficient, and even conservative bloggers have failed to have their webpages unblocked by lodging complaints.[53] Moreover, the dispute process requires the website owner to disclose his or her personal information and accept responsibility for any misconduct in the future, a commitment that few are willing to make given the risk of severe punishment.

Self-censorship is extensive, particularly on political matters. The widespread arrests and harsh sentences meted out to reporters and activists after the 2009 elections, as well as perceptions of pervasive surveillance, have increased fear among online journalists and bloggers. Many of them either abandoned their online activities or use pseudonyms. The result has been a palpable drop in the amount of original content being produced by users based inside the country.

In addition to filtering, censorship, and intimidation, the state counters critical content and online organizing efforts by extending regime propaganda into the digital sphere. There are at least 400 news websites either directly or indirectly supported by the state. They seek to set the agenda by providing pro-government commentary or publishing rumors. There have also been a large number of government-backed initiatives to promote blogging among its supporters and members of the

[50] "Filtering in Iran is fully democratic", Wimaxnews, accessed June 24, 2013, http://wimaxnews.ir/NSite/FullStory/News/?Id=3185.
[51] "12 memebers of Committee in Charge of Determining Unauthorized Sites," Weblognews, December 16, 2009, http://weblognews.ir/1388/09/mediablog/5740/.
[52] "The News stie's reporter will be insured," Hamshahri Online, November 1, 2011, http://www.hamshahrionline.ir/news-150108.aspx.
[53] "On filtering of Ahestan," Ahestan (blog), January 15, 2010, http://ahestan.wordpress.com/2010/01/15/ahestan.

Basij paramilitary group. In July 2011, the head of the Basij said there were three million members active online.[54]

Furthermore, the majority of independent content producers lack the financial resources to operate in such a hostile environment. The online advertising market in Iran is exclusively limited to apolitical and progovernment websites. Even businesses based outside Iran avoid political websites to maintain trading relationships with the country. Although the United States adjusted its sanctions against Iran to enable American internet companies to provide services to Iranian users, Google Advertising does not recognize Persian as one of the languages in its system, disadvantaging Persian content producers.[55]

The Iranian government has intensified its fight against the use of circumvention tools. The use of virtual private networks (VPNs), which use a secure protocol to encrypt users' data and bypass filtering in Iran, was particularly targeted in late 2012 and early 2013. Kamal Hadianfar, the head of a specialized unit within the cyber police, claimed that between 20 to 30 percent of Iranian users make use of VPNs.[56] Mehdi Akhavan Behabadi, Secretary of the Supreme Council of Cyberspace, announced the launch of legal, state-approved VPNs to replace "illegal" VPNs. Shortly after, on March 8, 2013, all unauthorized VPNs were blocked inside Iran.[57] There are also reports that the use of other circumvention tools such as Tor, the popular anonymizer and anti-filter tool, was hampered due to sophisticated disruption and blocking practices by the authorities.[58] Many users quickly shifted to other well-known circumvention tools, such as Psiphon, Freegate, and Kerio VPN, and within a month Psiphon reported between 700,000 to 900,000 daily users in Iran.[59] However, two months later, the authorities had severely limited access to these and all other tools, leaving Iranian users with few options.[60]

Following the Chinese model of internet control, Iran is very keen to develop national versions of popular online services as part of its National Information Network. Since Western-built tools such as Gmail or Skype provide a degree of privacy or encryption, the government is instead diverting funds to launch Iranian equivalents of major online services like e-mail, social networking sites, and search engines that can be easily controlled for political purposes. In July 2012, Iran's ICT minister Reza Taghipour indicated that Iran would use China's and South Korea's extensive experience in

[54] "Basij have had large and effective measures in cyberspace," Fars News, October 11, 2011, http://www.farsnews.com/newstext.php?nn=13900719001180.
[55] Jamal Abdi, "Obama Norooz promise a good step, more needed to ensure U.S. not part of 'Electronic Curtain,'" NIAC InSight, March 21, 2012, http://www.niacinsight.com/2012/03/21/obama-promises-to-ease-internet-restrictions-in-norooz-message/.
[56] "Iran to crack down in web censor-beating software",AFP, accessed June 24, 2013, https://www.google.com/hostednews/afp/article/ALeqM5jIFi-LdqBsdtrj7mRYnCMTlSGjCA?docId=CNG.f710ad6e0ee1dc52f64c985918d1bac1.741.
[57] "Iran blocks VPN use ahead of elections", accessed June 24, 2013, http://www.wired.co.uk/news/archive/2013-03/11/iran-vpn-block.
[58] "Iranian Internet infrastructure and policy report", Small Media, accessed June 24, 2013, http://smallmedia.org.uk/sites/default/files/reports/IIIP01.pdf.
[59] "Cyber Dialogue on Iran", Shahrvand, March 28, 2013, http://www.shahrvand.com/archives/37590.
[60] *Iranian Internet Infrastructure and Policy Report, March – April 2013*, April 2013, Small Media, available at http://smallmedia.org.uk/InfoFlowReportAPRIL.pdf.

order to develop a national search engine for use in Iran.[61] The government also indicated plans to launch a national Facebook-type service and e-mail systems. In December 2012, Iran launched its own video-sharing website in a move by officials to create a state-run competitor to sites like YouTube. The site, called Mehr.ir, is run by the government-controlled broadcaster, the Islamic Republic of Iran Broadcasting (IRIB). The IRIB is looking to create new digital platforms as a means of attracting new audiences and extending its broadcasting monopoly—guaranteed by the constitution—into cyberspace. The IRIB is under the direct supervision of Iran's Supreme Leader, who appoints its director. In April 2013, the head of the Ministry of Information and Communication Technology (ICT) stated "Basir," referred to as "the Islamic Google Earth," will come online in the next few months. However, many of these initiatives have failed to attract large numbers of users due to poor design. In addition, international sanctions on Iran over its nuclear program have limited the government's ability to purchase the equipment required to run data centers on the scale needed to host a national e-mail service, for example.[62]

Due to the limited nature of Iran's online sphere, many people have shifted to posting on closed social-networking platforms like Facebook, which is perceived to offer a safer environment for expressing views among a limited audience of contacts, compared to publicly posting comments on websites or keeping a blog. Social media is also used extensively by Iranian human rights activists to document abuses and launch advocacy campaigns. For instance, users have mobilized on Facebook and Twitter to demand the release of the jailed human rights lawyer Nasrin Soutodeh. Soutodeh's husband employs Facebook as a means of updating followers on her condition in prison, including her 49-day hunger strike from October to December 2012.[63] Sotoudeh, together with Iranian filmmaker Jafar Panahi, is a recipient of the European Union's 2012 Sakharov Prize for Freedom of Thought.[64] The son and daughter of imprisoned blogger Dr. Mehdi Khazali also post updates and prison letters on their respective Facebook pages, which are widely covered by Iranian blogs. An online petition was organized to call for his release.[65] Iranians also used social media to document and promote environmental campaigns and to call for blood drives to assist the victims of several devastating earthquakes.[66]

Nonetheless, some individuals associated with the regime have sought to discourage these practices. The Iranian Cyber Police, in November 2011, warned users that exchanging information on foreign social-networking sites could constitute a criminal act and lead to prosecution.[67] Speaking from a

[61] "Iranian search engine in the works: official," Payvand, accessed June 24, 2013, http://www.payvand.com/news/12/apr/1192.html.
[62] "Persian email service, Chaapaar will be launched in December," IRNA, September 27, 2011, http://www.irna.ir/NewsShow.aspx?NID=30583255.
[63] Hadi Nili, "Iranian Lawyer Nasrin Sotoudeh on Hunger Strike in Prison," GlobalVoices, November 16, 2012, http://globalvoicesonline.org/2012/11/16/iranian-lawyer-nasrin-sotoudeh-on-hunger-strike-in-prison/.
[64] Thomas Erdbrink, "Her Demand Met, Imprisoned Iranian Ends Hunger Strike," New York Times, December 4, 2012, http://www.nytimes.com/2012/12/05/world/middleeast/nasrin-sotoudeh-iranian-rights-advocate-ends-hunger-strike.html?_r=0.
[65] See "Immediate & Unconditional Release of Medhi Khazali," http://www.gopetition.com/petitions/immediate-unconditional-release-of-mehdi-khazali.html.
[66] Hooman Askary, "Iran's Most Memorable Internet Moments in 2012," GlobalVoices, December 27, 2012, http://globalvoicesonline.org/2012/12/27/irans-most-memorable-internet-moments-in-2012/.
[67] "Is being a member of social networks a crime?" Jahan News, November 17, 2011, http://www.jahannews.com/vdcdkk0fxyt0no6.2a2y.html.

religious perspective, in January 2012 an Iranian cleric declared Facebook to be un-Islamic and that membership constituted a sin.[68] Similarly, in April 2013, a prominent cyber police commander referred to Facebook as "the most disgusting spyware and the most dangerous warfare of the U.S."[69]

Despite these declarations, Supreme Leader Khamenei joined Facebook on December 13, 2012, through an announcement on his Twitter page. As mentioned, both Facebook and Twitter are blocked inside Iran, as they are considered tools of the soft war against Iran.[70] Secretary of the SCC Mehdi Akhavan Behabadi addressed the issue of Iran's Supreme Leader joining Facebook by stating that although membership in social networking websites is legal, using circumvention tools to access these networks is illegal. He added that the government of Iran has no decision to remove the filtering from social networking websites, such as Facebook.[71] Despite the restrictions imposed on Facebook and Twitter, both platforms were widely used by the Iranians to discuss election-related issues. In addition, all six presidential candidates had accounts on these platforms.[72]

VIOLATIONS OF USER RIGHTS

Iranian internet users suffer from routine surveillance, harassment, and the threat of imprisonment for their online activities, particularly those critical of the authorities and among the members of ethnic and religious minorities. The constitution provides for limited freedom of opinion and expression, but numerous, haphazardly-enforced laws restrict these rights in practice. The 2000 Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or detrimental to public rights, none of which are clearly defined.[73] The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize critical opinions. The 2009 Computer Crime Law (CCL) identifies punishments for spying, hacking, piracy, phishing, libel, and publishing materials deemed to damage "public morality" or to be a "dissemination of lies." [74] Punishments mandated in the CCL are severe. They include the death penalty for offenses against public morality and chastity, as well as long prison sentences, draconian fines, and penalties for service providers who fail to enforce government content restrictions. Numerous users were arrested over the coverage period and, in the gravest violation of user rights, blogger Sattar Beheshti was killed while in police custody.

Since June 2009, the authorities have cracked down on online activism through various forms of judicial and extralegal intimidation. An increasing number of bloggers have been threatened,

[68] Amrutha Gayathri, "Muslim Cleric Says Facebook is Un-Islamic, Membership Sin," International Business Times, January 11, 2012, http://www.ibtimes.com/articles/280026/20120111/muslim-cleric-facebook-un-islamic-membership-sin.htm.
[69] Hadi Nili, "Iran: Facebook is 'the most disguisting US spyware'," GlobalVoices, April 25, 2013, http://globalvoicesonline.org/2013/04/25/iran-facebook-is-the-most-disgusting-us-spyware/.
[70] "Official responses to Ayatollah Khamenei's Facebook page: registration is not a crime", BBC Persian, accessed June 24, 2013, http://www.bbc.co.uk/persian/iran/2012/12/121225_l_khamenei_facebook_reax.shtml.
[71] "Change in the organising national cyber defense", Jamejam, accessed June 24, 2013, http://www.jamejamonline.ir/papertext.aspx?newsnum=100826926096.
[72] http://www.rferl.org/content/iran-internet-disruptions-election/25028696.html
[73] Press Law, http://press.farhang.gov.ir/fa/rules/laws2.
[74] *Islamic Republic of Iran: Computer Crimes Law Article 19*, January 30, 2012, www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB[4].pdf.

arrested, tortured, kept in solitary confinement, and denied medical care, while others have been formally tried and convicted. Four individuals—Saeed Malekpour (a web developer), Mehdi Alizadeh Fakhrabad (web developer), Vahid Asghari (blogger and IT student), and Ahmad Reza Hashempour (website designer)—were sentenced to death between October 2011 and January 2012 under extremely questionable circumstances on charges relating to insulting religion or conspiring with foreign enemies. Malekpour, for example, was prosecuted on charges of "insulting and desecrating Islam" because a software program he had designed was used to upload pornography, although it was done without his knowledge.[75] Numerous bloggers remain in prison and are currently serving prison terms of up to 20 years, including Hossein Ronaghi-Maleki[76] and Hossein Derakhsan, considered the father of the Iranian blogosphere.[77]

The most significant human rights violation that occurred during the coverage period was the death of Sattar Beheshti, an Iranian blogger. Beheshti was arrested on October 30, 2012 by the Cyber Police of Iran for criticizing the government in posts he made online. He was pronounced dead after four days in custody. News of his death was first published on opposition websites close to the Green Movement, and then spread to other media outlets. Despite initial difficulties in obtaining an official confirmation of his death, it quickly became one of the top news headlines in the media and across social networking sites and blogs. Combined with pressure from the international community, the sustained attention across the Iranian media and political spectrum forced an official investigation. The head of the Tehran Cyber Police was dismissed by the Commander of the Islamic Republic Security Forces for "shortcomings in the supervision and handling of the case."[78]

Dr. Mehdi Khazali, a dissident blogger, ophthalmologist, and director of a publishing house, was arrested on October 30, 2012 during a meeting of the writers association *Saraye Ghalam* (Pen Society).[79] Dr. Khazali has been arrested multiple times for fiercely criticizing President Ahmadinejad.[80] Ironically, he is also the son of Ayatollah Khazali, a leading conservative cleric, though they have differing political views. After a 140-day hunger strike, he was finally released on June 3, 2013.[81] Kaveh Taheri, a blogger from Shiraz, Iran, was arrested on September 23, 2012 for

[75] Saeed Malekpour, interviewed by Olivia Ward, "Saeed Malekpour: A Canadian on Iran's death row," The Star, February 18, 2012, http://www.thestar.com/news/world/article/1132483--a-canadian-on-iran-s-death-row; Amnesty International, "Iran must halt execution of web programmer," January 19, 2012, http://www.amnesty.org/en/news/iran-must-halt-execution-web-programmer-2012-01-19.

[76] Ronaghi-Maleki is a blogger serving a 15-year sentence imposed in December 2009 for "spreading propaganda against the regime" and insulting the Supreme Leader.

[77] Deraksan lost his appeal against a 19-year sentence imposed on charges of cooperating with hostile countries, spreading propaganda against the regime, and insulting Islamic thought and religious figures.

[78] "Tehran's Cyber Police Chief Fired Over Blogger's Case" , December 12, 2012. http://www.payvand.com/news/12/dec/1003.html?utm_source=Payvand.com+List&utm_campaign=867f41c0f8-RSS_EMAIL_CAMPAIGN&utm_medium=email

[79] "Dr. Mehdi Khazali Has Been Re-Arrested And Has Launched A Dry Hunger Strike," Persianbanoo, October 31, 2012, http://persianbanoo.wordpress.com/2012/10/31/dr-mehdi-khazali-has-been-re-arrested-and-has-launched-a-dry-hunger-strike/.

[80] "Cyber Dissident Database: Dr. Mehdi Khazali," CyberDissidents.org, accessed April 30, 2013, http://cyberdissidents.org/bin/dissidents.cgi?id=125&c=IR.

[81] "Iranian Political Prisoner Mehdi Khazali Released After Weight, Health Plummet," Payvand Iran News, June 4, 2013, http://www.payvand.com/news/13/jun/1024.html.

acting against national security and disseminating online propaganda against the government. As of March 2013, he remained in detention pending any formal trial.[82]

As previously mentioned, even conservative supporters of President Ahmadinejad faced abuse over their online activities. For instance, Ahmad Shariat, who runs the conservative blog *Nedaee az Daroon*, was arrested on July 22, 2012 after publishing a post critical of the Revolutionary Guards and Iran's judiciary system.[83] The arrest was widely condemned in the Iranian blogosphere.[84]

Iranians outside of Iran were also intimidated for their online activities. Shahin Najafi, an Iranian rap artist, faced heavy criticism for a song that he published online titled *Naghi* (the name of a Shi'a Imam). Some have called the song blasphemous and a number of Grand Ayatollahs issued apostasy sentences (*fatwas*) against him.[85] The father of an Iranian student in the Netherlands was also arrested for his son's satirical posts on Facebook. The authorities threatened the son that if he does not return to Iran, his father will be executed.[86] Finally, Iman Amiri, an internet security student at Malmo University in Sweden, was arrested on January 21, 2013 upon returning to Iran. He is now in detention at Evin Prison and was reportedly subject to torture to force a confession.[87] Numerous other dissidents who are active online were arrested in late 2012 and early 2013, although many of their cases relate more strongly to their offline activities.[88]

There was a significant rise in the reports of individuals arrested for their activities on Facebook. In October 2012, four internet users in Sirjan were arrested because of their supposed use of antigovernment activities and the insulting of officials on Facebook. In an interview, Mehdi Bakhshi, the attorney general of Sirjan, warned internet users "to avoid any illegal online activities, such as publishing photos of women not wearing hijab, otherwise there would be legal consequences awaiting them."[89] In the same month, the individuals behind a Facebook page that published photos of Iranian girls were arrested for promoting "vulgarity and corruption among Iranian youths."[90] Iran's Cyber Police warned well-known athletes and artists against publishing personal photos on social networking websites. Ali Niknafs, the deputy supervisor of recognition and prevention at

[82] "A weblogger is in detention without trial for more than five months," Human Rights Activists News Agency, March 4, 2013, https://hra-news.org/en/a-weblogger-is-in-detention-without-trial-for-more-than-five-months.
[83] "The editor of Nedaee az Daroon was arrested", accessed June 24, 2013, http://www.digarban.com/node/7984
[84] Fred Petrossian, "Iran: Pro-Ahmadinejad Blogger Jailed," GlobalVoices, July 31, 2012, http://globalvoicesonline.org/2012/07/31/iran-pro-ahmadinejad-blogger-jailed/.
[85] "Harsh reactions to a song by an Iranian Rapper", BBC Persian, May 09, 2012 http://www.bbc.co.uk/persian/rolling_news/2012/05/120509_u07_shahin_najafi_reaction.shtml.
[86] "Iranian seizes father for son's facebook post", RNW, accessed June 24, 2013, http://www.rnw.nl/english/article/iran-seizes-father-sons-facebook-posts.
[87] "A network security student was arrested after his arrival to Iran," Human Rights Activists News Agency, March 12, 2013, https://hra-news.org/en/a-network-security-student-was-arrested-after-his-arrival-to-iran#more-2482.
[88] "2013: Netizens Imprisoned," Reporters Without Borders, accessed June 27, 2013, http://en.rsf.org/press-freedom-barometer-netizens-imprisoned.html?annee=2013.
[89] "Four people arrested in Iran for 'insulting authorities' in Facebook", BBC Persian, accessed June 24, 2013, http://www.bbc.co.uk/persian/iran/2012/10/121026_l39_facebook_iran_arrest.shtml.
[90] "Facebook band 'Tehran babes' has been disintegrated," [translated] Momtaznews, accessed June 24, 2013, see http://bit.ly/15vXiTi.

Cyber Police, stated that sharing personal photos through social media would increase the chances of improper use of photos, harming the reputation of Iranian celebrities.[91]

In March 2012, the Communications Regulatory Authority issued Bill 106,[92] which required the registration of all IP addresses in use inside Iran. Implementing such registration will allow the authorities to track users' online activities even more thoroughly and is a fundamental part of implementing the National Information Network through the restriction of anonymity online.

As of March 2012, customers of cybercafes must provide personal information (such as their name, father's name, national ID number, and telephone number) before using a computer. Cafe owners are required to keep such information, as well as customers' browsing history, for six months. They are also required to install closed-circuit surveillance cameras and retain the video recordings for six months.[93] Mehdi Mir-Mohammadi, head of the IT-Union of Tehran commented that some of the elements in the new regulations infringe on user's privacy and expressed concern over the fact that they could be taken advantage of and lead to new forms of cybercrimes. [94]

In addition, the CCL obliges ISPs to record all the data exchanged by their users for a period of six months, but it is not clear whether the security services have the technical ability to process all this data. When purchasing a mobile phone subscription or prepaid SIM card, users must present identification, facilitating the authorities' ability to track down the authors and recipients of specific messages.

Despite international legal restrictions placed on the selling of surveillance equipment to the Iranian government, there have been numerous media reports that Chinese and some Western companies have been providing the Iranian authorities with technology to monitor citizens' digital activities. Specifically, investigative reports by Reuters and the *Wall Street Journal* found that Huawei Technologies[95] and ZTE Corporation,[96] both Chinese firms, were key providers of surveillance technology to Iran's government, allegations both companies have denied. According to an uncovered PowerPoint presentation outlining the system's capabilities, Iran's MobinNet ISP would potentially have the capacity to utilize deep packet inspection (DPI) to conduct real-time

[91] "There is no compensation for lost dignity", IRSport24, accessed June 24, 2013, http://www.irsport24.com/Default.aspx?PageName=News&Action=Subjects_Details&ID=15222.

[92] Bill 105, Communication Regulation Authority, http://cra.ir/Portal/File/ShowFile.aspx?ID=f1a93935-938c-4d93-9eed-b47bc20685d4.

[93] Golnaz Esfandiari, "Iran Announces New Restrictions For Internet Cafes," Payvand, January 5, 2012, http://www.payvand.com/news/12/jan/1048.html?utm_source=Payvand.com+List&utm_campaign=d6730c3065-RSS_EMAIL_CAMPAIGN&utm_medium=email.

[94] "Internet cafes are required to authenticate users, all the pages viewed in the Internet cafes should be recorded", Asriran, accessed June 24, 2013, see http://bit.ly/1fIAhE5.

[95] Steve Stecklow, Farnaz Fassihi, and Loretta Chao, "Chinese Tech Giant Aids Iran," The Wall Street Journal, October 27, 2011, http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html.

[96] "UANI Calls on Chinese Telecom Giant ZTE to Withdraw from Iran," Market Watch, press release, March 26, 2012, http://www.telecomyou.com/newscenter/news/uani-calls-on-chinese-telecom-giant-zte-to-withdraw-from-iran-marketwatch-press-release.

monitoring of communication traffic, block websites, track users, and reconstruct e-mail messages as a means of monitoring citizens. [97]

Filtering and physical intimidation are supplemented by hacking and distributed denial-of-service (DDoS) attacks on the websites of government critics, including leading opposition figures. Throughout 2012 and early 2013, there was a rise in the number of hacking incidents. Numerous Facebook accounts of Iranians users who were deemed to be un-Islamic were hacked and defaced with a statement from Iran's judiciary saying, "By judicial order, the owner of this page has been placed under investigation." The friends of such users were also tagged in posts containing similar messages. [98] Mana Neyestani, a well-known Iranian caricaturist, had his Facebook fan page hacked by a group called "Islam's Soldiers." The hacking group added its logo and a number of caricatures with pro-Assad, anti-Israel, and anti-Saudi Arabia themes to Neyestani's Fan page during the few hours they had control. [99] It is not clear what role the Iran's Cyber Police or other security forces played in this incident.

Iran has significantly increased its hacking capabilities in recent years. According to Jeff Bardin, the chief intelligence officer at the American open source intelligence company Treadstone 7, Iran has become much more sophisticated and pervasive in its use of online tools. There have also been several officially announced plans on recruiting and training hackers. The Deputy of IT and Communications at Iran's Civil Defense Organization announced that a Cyber Defense program of study would be introduced to some universities in the country on the graduate level. He added, "Familiarizing managers and commanders with the concepts of cyber defense is one of the main strategies of the Civil Defense Organization."[100] In the first such plan by a tertiary institution in Iran, the University of Lorestan announced that it will actively work to take down and hack into national and international websites that display anti-Islamic content.[101] Researchers at Amirkabir University are currently developing a "national network of cyber defense" while a team at Shiraz University is creating its own domestically-produced anti-virus software in support of a government ban on foreign digital security software.[102]

According to Zone-H, a website dedicated to tracking hacking incidents, there were a total of 1,387 website defacements attributed to Iranian hackers during March 2013 alone, with a similar number in February. The majority of these are attributed to the Ashiyane Digital Security Team, which ranks as the second most active group in world, with defacements of thousands of websites linked to foreign governments and high-level organizations.[103] It is also noteworthy that the head of

[97] "Special report: How foreign firms tried to sell spy gear to Iran", Reuters, accessed June 24, 2013, http://www.reuters.com/article/2012/12/05/us-huawei-iran-idUSBRE8B409820121205.
[98] "Combating immoral crimes in Facebook", Fardanews, accessed June 24, 2013, http://bit.ly/OQdomi.
[99] "Iran: 'Soldiers of Islam' hack catoonist's Facebook page", Cyberwarzone, accessed June 24, 2013, http://cyberwarzone.com/iran-%E2%80%9Csoldiers-islam%E2%80%9D-hack-cartoonists-facebook-page.
[100] "Iranian gov't pays paramilitary hackers, bloggers to bring you Islamic Revolution 2,0", Arstechnica, accessed June 24, 2013, http://arstechnica.com/tech-policy/2012/06/iran-expands-online/
[101] "New mission of Lorestan University: Hacking anti-regime sites inside and outside the country", Daneshjoonews, accessed June 24, 2013, http://www.daneshjoonews.com/node/7380.
[102] "Middle East and North Africa CyberWatch – March 2013," CitizenLab, April 2, 2013, https://citizenlab.org/2013/04/middle-east-and-north-africa-cyberwatch-march-2013/.
[103] Ashiyane Digital Security Team Report on Zone-H

Ashiyane, Behrouz Kamalian, was sanctioned under the European Union's human rights sanctions regime for being linked with the IRGC and responsible for cyber-crackdown both against domestic opponents and reformists and foreign institutions. [104] In the weeks leading up to the presidential elections, there was also a significant increase in targeted cyberattacks against high profile activists and journalists traced back to Iranian servers.[105]

http://zone-h.org/archive/filter=1/notifier=Ashiyane%20Digital%20Security%20Team/page=3.

[104] Council of the European Union, "Council Regulation (EU) No 1002/2011 of 10 October 2011 Implementing Article 12(1) of Regulation (EU) No 359/2011 Concerning Restrictive Measures Directed Against Certain Persons, Entities and Bodies in View of the Situation in Iran," The Official Journal of the European Union, October 10, 2011, p.5. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:267:0001:0006:EN:PDF) - See more at: http://www.defenddemocracy.org/behrouz-kamalian#_ftn2.

[105] Iranian Internet Infrastructure And Policy Report, March – April 2013 http://smallmedia.org.uk/InfoFlowReportMARCH.pdf.

ITALY

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	4	5
Limits on Content (0-35)	7	6
Violations of User Rights (0-40)	12	12
Total (0-100)	23	23

* 0=most free, 100=least free

POPULATION: 60.9 million
INTERNET PENETRATION 2012: 58 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Despite limited progress, Italy continued to lag behind most other countries of the European Union in terms of internet penetration and average speed (see **OBSTACLES TO ACCESS**).
- Dozens of file-sharing and video-streaming websites were blocked over the past year for illegally hosting copyrighted materials (see **LIMITS ON CONTENT**).
- The Court of Cassation clarified that a 1948 law prohibiting "clandestine press" could not be applied to blogs, easing fears that blogs could face blocking for failing to register with the authorities (see **LIMITS ON CONTENT**).
- Social media and blogging were critical in the nascent Five Star Movement's success in the February 2013 parliamentary elections, in which it received more votes than any single party (see **LIMITS ON CONTENT**).
- A Livorno court decided that an insulting Facebook post can be considered as defamation by "other means of publicity," since the social network allows for the broad diffusion of posts. In the case, a user was found guilty of defaming her former employer and ordered to pay a fine. The ruling may open the door for further defamation cases related to Facebook posts (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Italy's first computer network emerged in 1980, when a group of nuclear physicists connected all of the country's nuclear research institutes. At the beginning, the internet was just one of several packet-switching networks that coexisted in Italy. The dominant telecommunications firm at the time, Telecom Italia, tried to impose its privately owned system, while various center-left governments, aware of the importance of interconnectivity, supported integration among the networks. Ultimately, the adaptability and simplicity of the internet prevailed. Access to the internet was available to private users after 1995, and the number of internet service providers (ISPs) soared within a short period of time. Among the remaining obstacles to greater internet penetration include a lack of familiarity with computers and with the English language, as well as the dominance of commercial television and the diversion of consumers' telecommunications spending to mobile telephony.

High ownership concentration in the media sector continued to impact the country's information landscape in late 2012 and early 2013.[1] Former prime minister Silvio Berlusconi still owns, directly and indirectly, a private media conglomerate. After his *Il Popolo della Libertà* (The People of Freedom, PdL) party withdrew its support, the technocratic government of Mario Monti collapsed in December 2012. While the PdL did not have sufficient political power to push through controversial initiatives such as the wiretapping bill, it did manage to block any move that might undermine Berlusconi's position in the media market.[2] When fresh election did arrive in February 2013, the use of social media and the web proved to be a major innovation, resulting in a strong showing from the digitally-savvy *Movimento 5 Stelle* (Five Star Movement, M5S). The highly-fragmented outcome of the elections, in which no party was able to obtain an outright majority, is unlikely to produce the stable environment required for new prime minister Enrico Letta to address some of the outstanding legal issues regarding freedom of expression online.

Italy's internet penetration rate lags behind many other European Union countries. Mobile telephone usage is ubiquitous, however, and internet access via mobile phones has grown significantly in recent years. Italian authorities do not generally engage in political censorship of online speech, although authorities are highly active in blocking file-sharing and live-streaming sites if they are shown to illegally provide access to copyrighted content. As in previous years, no bloggers were imprisoned as of mid-2013, though a Facebook user was fined over a defamatory post concerning her former employer. Defamation and libel are central issues in the country, particularly when sensitive information obtained from government wiretaps is leaked to the public, often at the expense of high-profile individuals. Furthermore, despite a number of judicial decisions asserting that intermediaries cannot be prosecuted for content posted by users, existing laws are

[1] For an overview see, for example, the ITU, "Europe: Level of Competition" Report at http://www.itu.int/ITU-D/icteye/Reporting/ShowReport.aspx?ReportFormat=PDF&ReportName=%2FTREG%2FLevelOfCompetition2007&RP_intRegionID=5&RP_intLanguageID=1&RP_intYear=2012&ShowReport=true, accessed February 08, 2013.

[2] As an important political leader, and supporter of the Monti government (albeit quite reluctantly) Silvio Berlusconi also retained significant influence over the appointment of state regulators. Such conditions also made the country's leadership resistant to confront the peculiar "imperfections" of Italy's editorial and broadcasting sectors.

applied in a contradictory manner and are often overturned at every appeal, resulting in extended legal battles.

OBSTACLES TO ACCESS

Since the 1990s, the Italian government has supported the internet as a catalyst for economic growth, increased tourism, reduced communication costs, and more efficient government operations. According to the International Telecommunication Union (ITU), Italy had an internet penetration rate of 58 percent at the end of 2012, an increase from 40.8 percent in 2007.[3] While Italy's internet penetration rate is higher than the global average, it is below the norm for the European Union (EU). The relatively low penetration rate is often attributed to unfamiliarity with the internet among the older generations, as well as a lack of understanding about the internet's utility among certain segments of the population.

From March 2012 to March 2013, over 250,000 broadband subscription lines were added, sending the total to 13.82 million. Average download speeds also increased, with almost 89 percent of Italian subscribers achieving nominal speeds of 2 Mbps or more.[4] Despite the progress, Italy has fallen behind most EU countries in this area, and the country's users access the internet at an average speed of 4.4 Mbps; by comparison, the average speed in the Netherlands is 9.9 Mbps, in the Czech Republic 9.6 Mbps, and in Portugal 5.3 Mbps.[5]

The main point of internet access is the home, with some 22 million people using home connections at least once a month, as of early 2012.[6] The workplace is the second most common access point, followed by schools and universities. While less than half of Italy's internet users are female, women comprise 55 percent of new users. Cost is not a significant barrier to access. The price for a broadband connection may range from €20 to €40 ($27 to $53) per month, compared to average monthly per capita income of around $2,750.[7]

ADSL broadband connections are available on about 97 percent of Italy's territory and plans were outlined to bring it to 99 percent by the end of 2012 with the help of mobile broadband.[8] Little

[3] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011 & 2006, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[4] "Quarterly Telecommunications Markets Observatory, AGCOM, March 31, 2013, http://www.agcom.it/Default.aspx?message=visualizzadocument&DocID=11333.

[5] Akamai, "State of the Internet: 1st Quarter, 2013," Volume 6, Number 1, http://www.akamai.com/dl/whitepapers/akamai_soti_q113.pdf?curl=/dl/whitepapers/akamai_soti_q113.pdf&solcheck=1&WT.mc_id=soti_Q113& (subscription required).

[6] Giancarlo Livraghi, ed., "Dati sull'internet in Italia" [Data on the Internet in Italy], accessed February 15, 2013, http://www.gandalf.it/dati/dati3.htm.

[7] "Broadband—Italy," Socialtext, accessed February 19, 2013, https://www.socialtext.net/broadband/index.cgi?italy; "GDP per capita (current US$)" The World Bank, 2008-2012, accessed August 5, 2013, http://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

[8] "Domestic Market," Telecom Italia, March 3, 2012, http://www.telecomitalia.com/tit/en/about-us/profile/domestic-market.html. The goal of 99 percent by the end of 2012 appears still unfulfilled as of early 2013. Socialtext puts the figure for ADSL at 88 per cent (as of October 2012).

progress has been made on the five-year, €2.5 billion ($3.3 billion) plan to connect 15 of Italy's largest cities using fiber-optic cable, proposed in 2010 by Italy's three largest telecommunications operators. A similar investment plan for €9 billion ($11.8 billion) by Telecom Italia also faced delays. These plans are now suspended given Italy's precarious financial crisis.

Mobile phone use is much more widespread than internet access, with the penetration rate reaching 158 percent in 2012, which translates to 4.3 mobile subscribers for every fixed-line subscriber.[9] The majority of subscriptions are prepaid. Telecom Italia Mobile (TIM), Vodafone, Wind, and 3 Italia are the major carriers, and all of them operate third-generation (3G) networks. Access to mobile internet has been increasing in recent years, and as of 2011, some 59.4 percent of internet users reported accessing the internet through their smart phones.[10] As elsewhere, sales of tablet computers have been on the rise among the younger generation since 2010 and are likely to keep growing in the coming years.

In March 2012, the government launched the "Digital Agenda" initiative, intended to expand broadband access and e-government functions.[11] A project of the infrastructure and economic development minister, several other ministries (economy, research and university, public health, and so on) should be involved in this operation, which is supposed to profoundly "transform" Italy's public administration. The six strategic areas of the "Digital Agenda" include infrastructure and cyber security, e-commerce, e-government, e-learning (e-books, digital policy literacy and e-participation), research and innovation in ICT, and smart cities and communities. As recent as April 2013, Prime Minister Enrico Letta reiterated the need to pursue many of the Digital Agenda items first proposed by his predecessor, Mario Monti.[12]

Access to the internet for private users is offered by 13 different ISPs. Telecom Italia has the largest share of the market, followed by Vodafone, Fastweb, and Tiscali. Telecom Italia owns the physical network, but it is required by European Union (EU) legislation to provide fair access to competitors. Further, Telecom Italia has announced plans to divest its infrastructure holdings into a separate subsidiary in a bid to increase profits and avoid legal repercussions associated with its current monopoly holdings.[13]

The main regulatory body for telecommunications is the Authority for Communications Security (AGCOM), an independent agency that is accountable to the parliament. Its responsibilities include providing access to networks, protecting intellectual property rights, regulating advertisements, and overseeing public broadcasting. The parliament's majority party appoints AGCOM's president,

---

[9] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2012, accessed February 19, 2013 http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[10] ITU, *Measuring the Information Society 2011,* p.154, http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf.

[11] Italian text at http://www.gazzettaufficiale.it/moduli/DL_181012_179.pdf. See also http://www.agenda-digitale.it/agenda_digitale/.

[12] Mauro del Vecchio "Agenda Digitale, nuova corsa", Punto Informatico, April 30, 2013, http://punto-informatico.it/3780111/PI/News/agenda-digitale-nuova-corsa.aspx.

"Telecom Italia: CDA approva il progetto di societarizzazione della rete di accesso", [Telecom Italia: CDA approves corporate reorganization of the network grid," [13] Telecom Italia, May 30, 2013, http://www.telecomitalia.com/tit/it/archivio/media/comunicati-stampa/telecom-italia/corporate/economico-finanziario/2013/05-30a.html

and commissioners have been known to come under pressure from the government to take certain actions regarding television broadcasts, particularly when Berlusconi was prime minister.[14] Angelo Marcello Cardani was appointed as AGCOM president in July 2012 and remains the current head under Prime Minister Letta.[15]

Another important player in the field of communications is the Italian Data Protection Authority (DPA). Set up in 1997, the DPA today has a staff of more than 100 people, and four of its main members are elected by parliament for seven-year terms. The DPA is tasked with supervising compliance by both governmental and nongovernmental entities with data protection laws, and "banning or blocking processing operations that are liable to cause serious harm to individuals."[16] It is generally viewed as professional and fair in carrying out its duties.

LIMITS ON CONTENT

In Italy, websites are principally blocked or taken down for offenses related to defamation or copyright infringement. There are little restrictions on politically-orientated content, although the vague legal environment does lead to a degree of self-censorship as ISPs and users seek to avoid prosecution. Intermediaries and content providers often required to take down illegal content at the request of executive bodies or judicial authorities. Facebook, Twitter, YouTube, and international blog-hosting sites are freely available. Further, social media and blogging has been employed by political groups to mobilize potential voters and even crowd-source party decisions.

Websites related to gambling, child pornography, and illegal file-sharing are blocked in Italy. Since 2006, online gambling has been permitted only through state-licensed websites; ISPs are required to block access to a list of international or unlicensed gambling sites identified by the Autonomous Administration of State Monopolies (AAMS), available on its website and updated regularly.[17] A similar list of illegal sites is maintained by the National Center for the Fight against Child Pornography on the internet, established in 2006 within the Postal and Communications Police Service. This list, which is forwarded onto ISPs for implementation, is formulated through internal research as well as complaints submitted by users.[18] The public availability of the child pornography blacklist has drawn consternation from some child advocates, who have expressed concern that this encourages visits to the sites by users with circumvention tools. Internet subscribers can also pay a small fee to sign up for a voluntarily "family internet" package from ISPs, in which access to adult pornography and sites with violent content is blocked.

[14] Michael Day, "Silvio Berlusconi caught out trying to stifle media," The Independent, March 18, 2010, http://www.independent.co.uk/news/world/europe/berlusconi-caught-out-trying-to-stifle-media-1923147.html .
[15] Cardani is a former chief of staff of Mario Monti when the latter was EU Anti-Trust commissioner. He also worked within the EU Commission for a while; http://www.agcom.it/Default.aspx?message=contenuto&DCId=184.
[16] "The Italian Data Protection Authority: Who We Are," Data Protection Authority, November 17, 2009, http://www.garanteprivacy.it/garante/doc.jsp?ID=1669109.
[17] The blacklist is available (in Italian) at http://www.aams.gov.it/site.php?id=2484.
[18] "Centro nazionale per il contrasto alla pedopornografia sulla rete" [National Center for the Fight against Child Pornography on the Internet], State Police, March 10, 2010, http://www.poliziadistato.it/articolo/view/10232/.

The website Avaxhome.ws was blocked on November 23, 2012, after a Milan court received a complaint from Mondadori, a publishing company owned by the Berlusconi family.[19] Among other things, the site hosted links to several global newspapers and magazines available in PDF form. Since the website profited from the hosting of copyrighted publications, Mondadori argued that it could not enjoy the protection granted to ordinary news websites. Nevertheless, information on how to circumvent the blocking was soon abundantly available on social media and elsewhere.[20] Following an order from a court in Monza, near Milan, ISPs were also asked to block the web forum downloadzoneforum.net, which hosted links to movies and other copyright protected material.[21] Both of these actions were made possible by a 1941 Law on Author Rights,[22] explicitly amended by the Berlusconi government in 2005 to include the web.[23]

In April 2013, the Postal and Communications Police of Rome blocked 27 websites that allowed users to illegally download or stream music and movies online.[24] Italy's *Guardia di Finanza* (GdF, Finance Guard) has continually targeted file-sharing websites for disseminating material that infringes copyright.[25] Several popular BitTorrent sites, such as The Pirate Bay and BTjunkie, remain blocked. Access to Proxyitalia.com, a proxy often used to circumvent government censorship, is also blocked since April 2011.

At the end of 2011, Italy's Supreme Court overturned a lower court's verdict by declaring that editors of online magazines were not responsible for defamatory comments posted by readers, taking note of the difference between the printed and electronic press.[26] Nevertheless, in the ensuing years defamation cases have still been brought against online content providers and intermediaries that have led to the removal or blocking of content (for more on Italy's legal environment, see "Violations of User Rights").[27] For example, in February 2010, three Google executives were sentenced in absentia to imprisonment for allowing the circulation of an offensive video on YouTube.[28] However, since early 2011, other decisions have ultimately asserted that

[19] Il Messaggero "Avaxhome sotto sequestro per ricettazione: sul sito giornali pirata", November 28, 2012, http://www.ilmessaggero.it/primopiano/cronaca/avaxhome_sequestrato_sito_edicola_digitale/notizie/234594.shtml. The web site is originally from Russia, and for the first time the charge was that of "receiving of stolen goods" (a more serious action) in addition to copyright violation.
[20] Giornalettismo "Avaxhome chiuso: come raggiungerlo", November 28 2012, http://www.giornalettismo.com/archives/629365/avaxhome-chiuso-come-raggiungerlo/. As of February 2013, the web site is easily accessibile.
[21] Mauro Vecchio "Italia, DownloadZone al cimitero warez", January 31, 2013, http://punto-informatico.it/3705271/PI/Brevi/italia-downloadzone-al-cimitero-warez.aspx.
[22] Law n.633 of April 22, 1941, available at http://www.altalex.com/index.php?idnot=34610
[23] Law decree n.7 of January 31, 2005, available at http://www.altalex.com/index.php?idnot=5918.
[24] "Italian police blocks access to 27 file-sharing websites," Telecompaper, April 24, 2013, http://www.telecompaper.com/news/italian-police-blocks-access-to-27-file-sharing-websites--939415.
[25] Enigmax, "Italian Court Orders All ISPs to Block KickAssTorrents," TorrentFreak, May 24, 2012, http://torrentfreak.com/italian-court-orders-all-isps-to-block-kickasstorrents-120524/.
[26] "Italian Supreme Court: web magazines are not to be held responsible for readers' comments," Law & the Internet (blog), December 14, 2011, http://www.blogstudiolegalefinocchiaro.com/wordpress/?p=279.
[27] M. Del Vecchio, "Espressione digitale, libero bavaglio", Punto Informatico July 9, 2013Il senatore Torrisi (PdL) http://punto-informatico.it/3845739/PI/News/espressione-digitale-libero-bavaglio.aspx.
[28] This is related to a video posted by a user that showed a mentally disabled child being bullied by his classmates, although Google removed the video as soon as it was notified. The appeal decision for the "Vivi Down" case, as it was known, was expected at the end of December 2012, but as of early 2013, there had been no update. See Cristina Sciannamblo "Caso

content hosts are not responsible for prescreening content. For example, in July 2011, a Rome court specializing in intellectual property overturned a lower court's decision and found that Yahoo was not liable to punishment for listing search results that allowed users to access websites that may violate copyright."[29] Similarly, in March 2013, the Courthouse of Milan ruled that phrases stemming from Google's "Autocomplete"' or "Related Searches" features could not be seen as defamatory, since results were based on software calculations and did not represent the views of the search engine company.[30]

In April 2012, the Supreme Court imposed an obligation on publishers to update their online archives to ensure that outdated facts do not inadvertently damage an individual's reputation. The case involved a story about the 1993 arrest of a politician on corruption charges in northern Italy. Although the man was ultimately acquitted, news of his arrest continued to appear in search results. Following the European Union (EU) principle of "the right to oblivion" (or "the right to be forgotten"), the Supreme Court ordered the outlet to update the story to indicate the new facts. However, it also found that there were no grounds for libel since the events recounted in the article were true, even if they were incomplete or outdated.[31]

In a case from January 2013, a court in Milan ordered the blocking of 10 online platforms that index links to the online streaming of sports events.[32] In 2011, RTI, a subsidiary of the Berlusconi-owned Mediaset media conglomerate, had sued Google for allowing users, via its blog-hosting platform "Blogger," to stream Italian soccer matches. In December of that year, a Rome court ruled that web platforms were not in breach of the law so long as users removed streamed copyrighted materials upon being notified.[33] However, in the more recent case from 2013, the Milan court ruled that, even if the soccer game itself was not protectable, distributers could seek copyright protection over its broadcast.[34]

Vividown, aspettando la sentenza d'Appello", December 7, 2012, http://punto-informatico.it/3666664/PI/News/caso-vividown-aspettando-sentenza-appello.aspx.

[29] Giulio Coraggio, "Yahoo! Liable for Searchable Contents!" *IPT Italy Blog*, April 3, 2011, http://blog.dlapiper.com/IPTitaly/entry/yahoo_liable_for_searchable_contents; "PFA vs Yahoo: la decisione del Tribunale di Roma riapre il dibattito sulla responsabilità degli ISP nei casi di violazione del diritto d'autore" [PFA vs Yahoo: the decision of the Court of Rome reopens the debate on ISP liability in cases of violation of copyright], Key4biz, July 14 2011, http://www.key4biz.it/News/2011/07/14/Policy/About_Elly_yahoo_pfa_film_internet_service_provider_isp_diritto_d_autore_204511.html.

[30] Mauro Vecchio, "Google completa senza pensare", Punto Informatico, March 20, 2013, http://punto-informatico.it/3754530/PI/News/google-completa-senza-pensare.aspx.

[31] "Italian Supreme Court: the right to oblivion to be protected with newspaper archive updates," Law & the Internet (blog), April 23, 2012, http://www.blogstudiolegalefinocchiaro.com/wordpress/?p=360. See also, Morena Ragone, "Il diritto alla memoria, tra privacy e oblio" [The right to memory, including privacy and oblivion], LeggiOggi.it, April 10, 2012, http://www.leggioggi.it/2012/04/10/il-diritto-alla-memoria-tra-privacy-e-oblio/.

[32] Mauro Vecchio, "Mediaset, sequestro per lo streaming pallonaro" [Mediaset, seizure for soccer streaming], January 16, 2013, http://punto-informatico.it/3691462/PI/News/mediaset-sequestro-streaming-pallonaro.aspx.

[33] Guido Scorza, "Mediaset e Google: tra copyright e libertà" [Mediaset and Google: between copyright and freedom], Punto Informatico, December 16, 2011, http://punto-informatico.it/3368416/PI/Commenti/mediaset-google-copyright-liberta.aspx; http://www.telecompaper.com/news/google-not-responsible-for-streaming-football-from-mediaset; "Court of Rome: not to precautionary controls of online content by intermediaries," Law & the Internet (blog), January 17, 2012, http://www.blogstudiolegalefinocchiaro.com/wordpress/?tag=rti.

[34] Mauro Vecchio "Mediaset, sequestro per lo streaming pallonaro", January 16, 2013, http://punto-informatico.it/3691462/PI/News/mediaset-sequestro-streaming-pallonaro.aspx.

While intermediaries are not liable to prosecution for hosting content, they must remove illegal content upon receiving notice from a judicial authority in line with provisions laid out in the EU E-Commerce Directive.[35] For example, Google received 27 requests in the period of July to December 2012, two more with respect to the previous six-month reporting period.[36] The vast majority of all court orders involved material that was broadly interpreted as defamatory.

Decisions related to the blocking of illegal websites are made by the Postal and Communications Police,[37] which falls under the Ministry of Interior, and intervenes in areas of cyberterrorism, copyright, hacking, protection of critical infrastructure, online banking, forensics, and online gambling.[38] Sites can also be shut down and their data seized by the Financial Police (GdF), a division of the Ministry of Economy and Finance, which combats cybercrime, fraud, and a range of other illegal activities.[39] Beginning in December 2010, AGCOM has continually sought new powers to conduct administrative filtering in a bid to combat online copyright infringement.[40] Under the proposal, the agency could block websites hosted outside of the country and remove content on Italian servers through an internal five-day review without any degree of judicial oversight. The move was criticized by the European Parliament and by internet freedom advocates.[41] As of late April 2013, AGCOM stated that it had still not yet taken a final decision on the matter, which has been delayed several times.[42]

Even in the absence of legal requirements, ISPs tend to exercise some informal self-censorship, declining to host content that may prove controversial or that could create friction with powerful entities or individuals. Online writers also exercise caution to avoid libel suits by public officials, whose litigation—even when unsuccessful—often takes a significant financial toll on defendants in the traditional media. The Italian government does not proactively manipulate news websites. However, coverage in traditional media does affect what is published on news websites, giving the outlets controlled by former Prime Minister Berlusconi an indirect influence over online reporting.

Some restrictions on internet content uncommon in other Western European countries remain in place in Italy. Drawing on a 1948 law against the "clandestine press," a regulation issued in 2001 holds that anyone providing a news service, including on the internet, must be a "chartered" journalist within the Communication Workers' Registry (ROC) and hold membership in the

[35] Martine Wubben, "Court of Appeal Rome: no monitoring requirement for hosting provider Yahoo," Future of Copyright, July 16, 2011, http://www.futureofcopyright.com/home/blog-post/2011/07/16/court-of-appeal-rome-no-monitoring-requirement-for-hosting-provider-yahoo.html.
[36] Google Transparency Report, "Italy," Google, accessed August 6, 2013, http://www.google.com/transparencyreport/removals/government/IT/ .
[37] Polizia postale e delle comunicazioni, http://www.poliziadistato.it/articolo/23393/.
[38] "Attività ed organizzazione," Polizia di Stato, accessed August 7, 2013, http://www.poliziadistato.it/articolo/view/23395/.
[39] Guardia di Finanza, http://www.gdf.it/GdF/it/Home/index.html.
[40] "Subject: Internet censorship in Italy—via administrative procedure," European Parliament, July 13, 2011, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2011-006948+0+DOC+XML+V0//EN accessed February 2, 2013.
[41] "Italian Agency to Review Internet Filtering Project," Reporters Without Borders, July 7, 2011, http://en.rsf.org/italy-italian-agency-poised-to-assume-05-07-2011,40595.html; "Internet Blocking Stopped in Italy (for Now), Digital Civil Rights in Europe, July 13, 2011, http://www.edri.org/edrigram/number9.14/internet-blocking-agcom-italy.
[42] "Italian regulator says still no decision on online copyright," Telecompaper, April 24, 2013, http://www.telecompaper.com/news/italian-regulator-says-still-no-decision-on-online-copyright--939469.

national journalists' association.[43] The law led to many users, including those conducting scholarly research, to collaborate with registered journalists in order to protect themselves from legal action. However, in a September 2012 ruling by the Court of Cassation, it was clarified that blogs cannot be considered clandestine press.[44] The decision came after an appeal from the Sicilian blogger Carlo Ruta, who had been ordered to pay a fine of €150 ($200) for defamatory remarks made on his blog "accadeinsicilia.net" back in 2008. In any case, these rules were not generally applied to bloggers and, in practice, millions of blogs are published in Italy without repercussions.

Most policymakers, popular journalists, and figures in the entertainment industry have their own blogs, as do many ordinary citizens. Social-networking sites, especially Facebook and Twitter, have emerged as crucial tools for organizing protests and other mass gatherings, such as concerts, parties, or political rallies. However, at times, some content on social-networking platforms has been aggressive enough to potentially incite violence.[45] Although blogging is very popular in Italy, television remains by far the leading medium for obtaining news.

The widespread use of social media and the web in the February 2013 general elections represented a major shift in political strategy. Online tools were central, not only as a communication medium, but also as a measure of political allegiances through Facebook "likes" and Twitter hashtags related to the many political players.[46] Indeed, even Mario Monti seemed to utilize new media more readily than Silvio Berlusconi, who preferred to rely on his traditional outlets to convey his political message. Furthermore, the Five Star Movement (M5S), co-founded by comedian Beppe Grillo, based its political campaign almost exclusively on the internet and declined to take part in political talk shows or television interviews.[47]

After taking office, the Five Star Movement has used the web both to strengthen its political base as well as to conduct surveys. For example, the party used blogs and social media to select its candidate to run in Italy's presidential elections,[48] to vote on the expulsion of members who did not conform to the movement's rules and internal decisions, and to provide an outlet for statements by Grillo who, due to M5S rules, cannot stand for public office due to past criminal convictions.[49]

---

[43] Law No. 62, March 7, 2001, "Nuove norme sull'editoria e sui prodotti editoriali" [New Rules on Publishing and Publishing Products], InterLex, accessed August 21, 2012, http://www.interlex.it/testi/l01_62.htm.

[44] Mauro Vecchio, "Cassazione: il giornale telematico non è stampa" [Supreme Court: the electronic journal is not a press], September 17, 2012, http://punto-informatico.it/3606488/PI/News/cassazione-giornale-telematico-non-stampa.aspx.

[45] For example, in 2009, fan pages for imprisoned Mafia bosses emerged, as did a Facebook group called "Let's Kill Berlusconi." See Eric Sylvers, "Facebook to Monitor Berlusconi Content," The New York Times, December 15, 2009, http://www.nytimes.com/2009/12/16/technology/internet/16iht-face.html.

[46] Luca Annunziata, "Chi vince le elezioni su Internet?", *Punto Informatico*, February 8, 2013, http://punto-informatico.it/3713780/PI/News/chi-vince-elezioni-internet.aspx.

[47] Stephan Faris and Marina di Bibbona, "Italy's Beppe Grillo: Meet the Rogue Comedian Turned Kingmaker," Time, March 7, 2013, http://world.time.com/2013/03/07/italys-beppe-grillo-meet-the-rogue-comedian-turned-kingmaker/.

[48] The first candidate was Milena Gaibanelli, a journalist, who delcined then follone by Stefano Rodotà, former leader of the Privacy authority. In the end the incumbent president, Giorgio Napolitano, was re-elected.

[49] See Grilloì's blog at http://www.beppegrillo.it/. Grillo was criticized even on his blog for the advertisements revenues from his blog.

VIOLATIONS OF USER RIGHTS

As a signatory to the European Convention on Human Rights, freedoms of speech and the press, as well as the confidentiality of correspondence, are constitutionally guaranteed in Italy.[50] Nonetheless, the courts often issue conflicting decisions when passing judgments on similar cases related to internet freedom, particularly when related to intermediary liability. For this reason, online freedom of expression advocates have focused their efforts on proposing legal amendments to improve protections and prevent censorship rather than engaging in public interest litigation.[51] Though criminal provisions are rarely applied, civil libel suits against journalists, including by public officials and politicians, are a common occurrence, and the financial burden of lengthy legal proceedings may have a chilling effect on journalists and their editors.

Defamation is a criminal offense in Italy, punishable by prison terms ranging from six months to three years and a minimum fine of €516 ($670). In cases of libel through the press, television, or other public means, there is no prescribed maximum fine.[52] Public debate on libel was renewed during the high profile case of Alessandro Sallusti, director of *Il Giornale* newspaper, which has dragged on for years.[53] Many observers have criticized the libel law that can still send a journalist to prison. Worryingly, when the parliament took up proposals for a bill that was meant to decriminalize libel for journalists, the final draft actually led to a worsening of penalties.[54] Discussions were left unfinished after the fall of the Monti government. Nevertheless, the lack of legal clarity continues to threaten freedom of expression for online journalists.

Furthermore, there are growing concerns over the enforcement of defamation law on Facebook. For example, a young woman who posted negative and racist remarks about her former employer on the social network was found guilty of libel and made to pay a fine of €1,000 ($1,330) by a court in Livorno.[55] In that case, citing Article 595 of the penal code, the court found that a Facebook post could be interpreted as an "other means of publicity." Given this, the judge ruled that a more aggravated form of defamation had occurred—defamation by means of the press—and was able to order the defendant to pay a higher sum than in a standard defamation case unrelated to the press.

---

[50] An English copy of the constitution is available at, http://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf. See especially Articles 15 and 21.
[51] Andrea Monti (lawyer specialized on Internet freedom and activist), interview with author, February 20, 2012.
[52] Organization for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, *Libel and Insult Laws: A Matrix on Where We Stand and What We Would Like to Achieve* (Vienna: OSCE, 2005), 79, http://www.osce.org/fom/41958.
[53] Sallusti was found guilty of libel over an anonymous op-ed that had appeared in 2007 in the newspaper *Libero*, of which he was director at the time. Following a number of legal mishaps in the appeal, he was given a prison sentence of more than one year due to the Italian law on libel. The sentence was later confirmed by a higher court until, in 2012, the sentence was converted into a house arrest. For more information in Italian, please see http://www.ilgiornale.it/speciali/caso-sallusti.html.
[54] Ordine dei Giornalisti "Diffamazione a mezzo stampa", December 7, 2012, http://www.odg.it/content/diffamazione-mezzo-stampa and Francesco Maitoni "Ddl Salva Sallusti, il colpo di coda della democrazia di plastica", LeggiOggi.it, http://www.leggioggi.it/2012/10/25/legge-bavaglio-il-colpo-di-coda-della-democrazia-di-plastica/
[55] Adriana Apicella, "Diffamazione a mezzo stampa, è reato anche su Facebook" [Defamation by medium of the press, also on Facebook?], Justicetv.it, January 17, 2013, http://www.justicetv.it/index.php/news/2992-diffamazione-a-mezzo-stampa-e-reato-anche-su-facebook and also, Mauro Vecchio, "Diffamazione, stampa e social pari sono?" [Defamation, are press and social equal?], Punto Informatico, January 15, 2013, http://punto-informatico.it/3690966/PI/News/diffamazione-stampa-social-pari-sono.aspx.

The ruling could open the door to similar judgments, in which victims of defamation over social networks could seek high amounts of compensation.

The monitoring of personal communications is permissible only if a judicial warrant has been issued, and widespread technical surveillance is not a concern in Italy. Nevertheless, the country's authorities are known for engaging in extensive wiretapping.[56] According to 2006 figures from the Max Planck Institute, a German think-tank, Italy led the world in terms of wiretaps, with 76 intercepts per 100,000 people.[57] Data from 2010 shows that the authorities bug the communication lines of roughly one in every 470 adults.[58] Wiretapping is generally restricted to cases involving ongoing legal proceedings and terrorism investigations. Since 2001, "pre-emptive wiretapping" may occur even if no formal prosecutorial investigation has been initiated. More lenient procedures are also in place for Mafia-related investigations.[59]

The past year witnessed the failure of a draft wiretap bill ("DDL intercettazioni") that aimed to address concerns over the right to privacy, particularly as information obtained from wiretaps is regularly leaked to the media. The bill, promoted by Berlusconi's PdL over the past few years, has been criticized by the Organization for Security and Co-operation in Europe Representative on Freedom of the Media and the United Nations Special Rapporteur on Freedom of Expression.[60] Indeed, several provisions appeared to threaten media freedom and the right of the public to access independent information. These included high fines and jail sentences for filming an individual without permission and obligations for websites and blogs to issue corrections within 48 hours of receiving notice of an alleged error.[61] The bill was subsequently put on hold in late 2010 but revived in October 2011 after incriminating and embarrassing wiretaps of Berlusconi's conversations related to a sex scandal were published in newspaper and online.[62] Although not a priority for the Monti government, the issue of wiretapping remains on the agenda of current Prime Minister Enrico Letta due to continued pressure from Berlusconi's PdL.[63]

---

[56] See for example Cristina Bassi, "Intercettazioni, quante sono e quanto costano" [Interceptions, How Many and How Much They Cost], *Sky TG24*, June 13, 2010, http://tg24.sky.it/tg24/cronaca/2010/06/12/intercettazioni_quante_sono_e_quanto_costano.html.

[57] Duncan Kennedy, "Italian bill to limit wiretaps draws fire," BBC, June 11, 2010, http://www.bbc.co.uk/news/10279312 and "Intercettazioni: dati ufficiali" [Interceptions: official data], Il Chiodo (blog), June 19, 2010, http://ilchiodo.blogspot.it/2010/06/intercettazioni-dati-ufficiali.html.

[58] Doug Longhini, "We'll be listening: Amanda Knox case reveals extent of Italian wiretapping," CBS News, November 23, 2011, http://www.cbsnews.com/8301-504083_162-57329774-504083/well-be-listening-amanda-knox-case-reveals-extent-of-italian-wiretapping/.

[59] Privacy International, "Italy: Privacy Profile," in *European Privacy and Human Rights 2010* (London: Privacy International, 2010), https://www.privacyinternational.org/article/italy-privacy-profile.

[60] "OSCE media freedom representative urges Italy to amend bill on electronic surveillance," OSCE Representative on Freedom of the Media, June 15, 2010, http://www.osce.org/fom/69428.

[61] Nadine de Ninno, "Italian Wikipedia Shuts Down Prompted by New Wiretap Act," International Business Times, October 4, 2011, http://www.ibtimes.com/italian-wikipedia-shuts-down-prompted-new-wiretap-act-321225

[62] Tom Kington, "Berlusconi wiretaps reveal suspected pimp had visa to join him in China," The Guardian, September 18, 2011, http://www.guardian.co.uk/world/2011/sep/18/berlusconi-pimp-china-visa-wiretaps; Jeffery Kofman, "Silvio Berlusconi Wiretaps: 'Only Prime Minister in His Spare Time,'" ABC News, September 18, 2011, http://abcnews.go.com/International/silvio-berlusconi-wiretaps-prime-minister-spare-time/story?id=14546921; John Hooper, "Silvio Berlusconi faces fresh claims over parties, prostitutes and pay-outs," The Guardian, September 15, 2011, http://www.guardian.co.uk/world/2011/sep/15/silvio-berlusconi-claims-prostitutes-wiretap.

[63] "Intercettazioni, ritorna il ddl Alfano: è polemica" [Interceptions, the Alfano draft law returns], Tgcom24, May 15, 2013, http://www.tgcom24.mediaset.it/politica/articoli/1095305/intercettazioni-ritorna-il-ddl-alfano-e-polemica.shtml.

In March 2008, Parliament approved a law (No. 48 of 2008) that ratified the Council of Europe's Convention on Cybercrime, which established the period in which internet-related communication data should be retained.[64] This matter was further refined with the inclusion in the Italian legislative system of the 2006 EU Data Retention Directive two months later.[65] Under the current legal framework, ISPs must keep users' traffic records—though not the content of communications—for 12 months. This includes broadband internet data, internet telephony, internet use via mobile phone, and e-mail activity.[66] The records can only be disclosed in response to a request from a public prosecutor (a judge) or a defendant's lawyer, and, like their counterparts elsewhere in Europe, Italy's law enforcement agencies may ask ISPs to make such information readily available in the course of criminal investigations. Given the technical burden of this directive, most ISPs now use a third-party service that offers the necessary security guarantees for encryption and data storage.

As Italy moves towards greater e-governance, some concerns have been raised over the protection of user data in the hands of public agencies. "Certified Electronic Mail" (PEC), an initiative of the national postal service *Poste Italiane*, was named the public agency most damaging to individual privacy at the annual "Big Brother Awards" 2011. The shaming "prize" was given to PEC for its gross mishandling of private information kept by the government's "Registro delle Opposizioni," a register of people who wish to keep their contact information hidden from advertisement companies.[67] Nevertheless, in November 2011, it became mandatory for all businesses to use the PEC service in their communications with the public administration to cut costs and reduce paperwork.[68]

Reports of extrajudicial intimidation or physical violence in response to online activity are rare, although individuals who expose the activities of organized crime may be at risk of reprisals in certain areas of the country. According to intelligence reports, there are increasing fears that the country's economic crisis may push extremist groups to adopt cybercrimes as a form of protest or terrorism.[69] A special branch within the Postal and Communications Police, the National Center for Infrastructure Protection (CNAIPIC), is tasked with the protection of the country's critical infrastructure.[70] More common is the defacement or launching of denial-of-service (DoS) attacks against banks, business websites, and government institutions. In October 2012, Italian members of

[64] For a useful timetable of the required retention periods, see Gloria Marcoccio, "Convention on cybercrime: novità per la conservazione dei dati" [Convention on Cybercrime: News on Data Retention], InterLex, April 10, 2008, http://www.interlex.it/675/marcoccio7.htm. See also Andrea Monti, "Data Retention in Italy. The State of the Art," Digital Thought (blog), May 30, 2008, http://blog.andreamonti.eu/?p=74.
[65] Legislative Decree No. 109, May 30, 2008.
[66] Privacy International, "Italy: Privacy Profile."
[67] Cristina Sciannamblo "Big Brother Awards Italia: tutti i vincitori," Punto Informatico, June 6, 2011, http://punto-informatico.it/3182022/PI/News/big-brother-awards-italia-tutti-vincitori.aspx.
[68] "Ulteriore Deroga fino a fine giugno 2012 per la casella PEC aziendale," IlSoftware.it, accessed July 24, 2012, http://www.i-node.it/2012/05/ulteriore-deroga-fino-fine-giugno-2012-la-casella-pec-aziendale/.
[69] Il Corriere della sera, "Servizi: crisi alimenta tensione sociale", February 28, 2013, http://www.corriere.it/cronache/13_febbraio_28/crisi-terrorismo-rapporto-servizi_4d7f35e8-8178-11e2-aa9e-df4f9e5f1fe2.shtml.
[70] Critical infrastructure includes telecommunications networks, energy and water distribution systems, banking networks, and transportation and emergency services.

the hacktivist group Anonymous leaked 1.35 GB of data it had received in an attack on the Italian State Police. The information included details of existing wiretaps, interception techniques, and personal information on police officers.[71] In February 2013, the websites of the police of the Campania region, the Courthouse of Milan, and the Department of Penitentiary Administration were hacked. The homepages of those sites were replaced with an image of the Anonymous emblem and a declaration of a "digital revolution" of young Italians against "government delinquents."[72] Nevertheless, Italy does not rank highly on the list of countries identified as points of origin for cybercrimes.[73]

[71] Mohit Kumar, "Anonymous Hakcers leaks 1.35GB Italian State Police Data," The Hacker News, October 25, 2012, http://thehackernews.com/2012/10/anonymous-hackers-leaks-135gb-italian.html.

[72] "Gli hacker colpiscono ancora: attaccato sito della polizia campana" Corriere della Sera, February 17, 2013, http://www.corriere.it/cronache/13_febbraio_17/polizia-hacker-anonymous_1727d948-790b-11e2-a28b-a2fa92ae99be.shtml.

[73] "Italy leader in mobile attacks," Global Cyber Security Center (blog), accessed August 21, 2012, http://www.gcsec.org/blog/italy-leader-mobile-attacks. It should be noted, nonetheless, that the Global Cyber Security Center has been established by Poste Italiane. As active stakeholder in the area of cyber security, the agency may have a vested interest in presenting a picture of Italy's cyber security that is not reassuring by stressing weaknesses rather strengths of the Italian information infrastructure system. See, C. Giustozzi, "Italia patria del malware?" Punto Informatico, May 12, 2012 http://punto-informatico.it/3513450/PI/Commenti/italia-patria-del-malware.aspx. The "Symantec Threat report 2011" shows Italy as highly infected only as far as bots are concerned, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf (published April 2012), and the independent report by HostExploit shows Italy scoring well on a "badness" scale (Germany and the Netherlands, for example get a worse score), http://hostexploit.com/downloads/viewdownload/7-public-reports/39-global-security-report-april-2012.html). These results are also graphically visible in here: http://globalsecuritymap.com/#nl.

JAPAN

	2012	2013
INTERNET FREEDOM STATUS	N/A	FREE
Obstacles to Access (0-25)	n/a	4
Limits on Content (0-35)	n/a	7
Violations of User Rights (0-40)	n/a	11
Total (0-100)	n/a	22

* 0=most free, 100=least free

POPULATION: 128 million
INTERNET PENETRATION 2012: 79 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Political speech was constrained online for 12 days before the December 2012 election under a law banning parties from campaigning online (see **LIMITS ON CONTENT**).
- In April 2013, the legislature overturned that law, but kept restrictions on campaign emails (see **VIOLATIONS OF USER RIGHTS**).
- 2012 amendments to the Copyright Law criminalized intentionally downloading pirated content, though lawyers called for civil penalties (see **VIOLATIONS OF USER RIGHTS**).
- Anti-Korean and anti-Chinese hate speech proliferated online amid real-world territorial disputes (see **VIOLATIONS OF USER RIGHTS**).
- A constitutional revision promoted by the newly-elected LDP party threatens to erode freedoms and rights that "violate public order" (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Internet and digital media freedom are generally well established in Japan, where the constitution protects all forms of speech and prohibits censorship. Given this broad lack of restrictions, however, some legislation disproportionately penalizes specific online activities.

Businesses started to recognize the potential of the internet after 1996, when major companies such as Nippon Telegraph and Telephone Corporation (NTT) and Fujitsu offered ISP services. In the early 2000s, providers introduced high-speed broadband. The world's first large-scale mobile internet service, iMode, was pioneered in 1999 by the nation's largest mobile carrier, NTT DoCoMo. Today, the internet is a major part of social infrastructure with 79 percent penetration.

Japan's internet industry is characterized by voluntary self-regulation. The government, especially the Ministry of Internal Affairs and Communications, maintains a hands-off approach when it comes to online content. Law enforcement agencies tend to push for stronger official regulation, and sometimes make arrests based on online activity. Police made a misguided attempt to reign in the chaotic discussion site 2channel in 2012, briefly charging its founder with abetting a drug dealer who had posted a message, but later backed off. Four others, including a student, were detained for several days in July 2012 when police believed them responsible for terror threats sent after malware commandeered their computers.

Japan's lawmakers also struggle to balance freedom with protection online, with mixed success. A revised copyright law in effect since October 2012 criminalized the deliberate download of a single pirated file; an offence now punishable with jail time. The law already threatens uploaders with up to 10 years in jail—making the commercial distribution of illegally copied entertainment in Japan subject to heavier sentences than the commercial distribution of child pornography.[1]

Other developments were more positive, particularly a change to restrictions on political speech on the internet that took place in April 2013. In December 2012, politicians stopped using the web for 12 days prior to the general election, which brought the conservative Liberal Democratic Party to power, following an outdated law against online campaigning. Four months after the social-media savvy Shinzo Abe assumed office as prime minister on December 26, the ban was reversed, though confusing limits remain on campaign emails and advertising.[2]

Troublingly, Abe's social networking expertise shows signs of turning manipulative, and his rhetoric against neighboring South Korea and China is echoed in increasingly xenophobic online discourse, which in turn fuels right-wing demonstrations. At the same time, the LDP is seeking to change the very core of Japan's free speech protections by revising the constitution so that rights

[1] Downloading and viewing child pornography for personal, non-commercial use is legal. A draft law criminalizing possession of child pornography has been in the pipeline since 2009 yet most opposition parties do not support the current language.
[2] Ayako Mie, "Election Campaigning Takes to Net: New law Opens Web to Candidates, Voters Ahead of Upper House Poll," *Japan Times*, April 11, 2013, http://www.japantimes.co.jp/news/2013/04/11/national/election-campaigning-takes-to-net/#.UY8XXqIqzFE.

"shall not violate public interest"—a disturbing change of emphasis. A national referendum must still approve constitutional revisions. So far, however, Abe's nationalism has attracted some popular support, to the possible detriment of the online space.

OBSTACLES TO ACCESS

In general, Japanese people experience few obstacles to internet access, with penetration at 79 percent in 2012.[3] In late 2011, official figures measured household penetration at 86 percent, and 99 percent for businesses with over 100 employees.[4]

Among individuals, figures show that 79 percent used a home computer to access the internet. Another 66 percent used mobile phones, and another 20 percent used smartphones. Game consoles, tablets, and internet-capable TV amounted to less than 10 percent of usage each. Few still use dial-up connections in Japan, since 60 percent have fiber-to-the-home broadband, according to 2013 government figures. [5] Access is high quality with competitive speeds. In April 2013, So-net, an ISP backed by Sony, said it was launching the world's fastest internet service for home use in Japan.[6]

The average cost of internet access is around 5,000 yen ($50) per month,[7] though many providers bundle digital media subscriptions, Voice over IP (VoIP) and e-mail addresses, pushing expenses higher. While this remains within reach of most, declining average incomes make staying connected increasingly costly, especially for the younger generation.[8]

NTT, formerly a state monopoly, was privatized in 1985 and reorganized in 1999 under a law promoting functional separation between the company's mobile, fixed-line, and internet services.[9] Asymmetric regulation, which creates stricter rules for carriers with higher market share, helped diversify the industry, though critics say the expense of switching providers—and the inconvenience of losing an email address and other services—ties customers to the dominant players and creates a barrier for new entrants.[10] While the telecommunications market looks open,

[3] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[4] Ministry of Internal Affairs and Communications, "Communication Service Use Trend, 2011" [in Japanese], http://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html.
[5] Ministry of Internal Affairs and Communications, "Broadband Subscription Trend, 2013" [in Japanese], http://www.soumu.go.jp/johotsusintokei/field/data/gt010103.xls.
[6] Jay Alabaster, "Sony ISP Launches World's Fastest Home Internet, 2Gbps," *PC World,* April 15, 2013, http://www.pcworld.com/article/2034643/sony-isp-launches-worlds-fastest-home-internet-2gbps.html.
[7] Informal Freedom House survey of providers' costs, 2013.
[8] The average monthly income for working households in 2010 was 700 yen (US$7) less than it was in 1990. See, Ministry of Internal Affairs and Communications, "Average Monthly Income and Expenditure per Household (Workers) 1955-2010," Statistics Bureau, http://www.stat.go.jp/data/chouki/zuhyou/20-06.xls.
[9] "Law Concerning Nippon Telegraph and Telephone Corporation, Etc.," 1984, amended 2005, available on the Ministry of Internal Affairs and Communications website, http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/NTTLaw.htm.
[10] Toshiya Jitsuzumi, "An Analysis of Prerequisites for Japan's Approach to Network Neutrality," paper submitted to the Proceedings of the Telecommunincations Policy Research Conference 2012, http://bit.ly/1dPQDcb.

therefore, with hundreds of providers offering FTTH, DSL, CATV, FWA, and BWA services, the NTT group remains dominant in practice.[11]No major foreign operators have successfully penetrated the telecommunications market, with the exception of smartphone devices manufactured by Apple and Samsung, though many invest in, or partner with local providers.

Mobile penetration reached 109 percent in 2012.[12] Almost every mobile phone uses packet-based Internet services which helped mobile internet use became popular in Japan even before the introduction of the smartphones, though increasing smartphone use has made the market more competitive. The three major carriers are KDDI Au, NTT DoCoMo and Softbank. According to data published in 2013, the average household in Japan spends around 6,714 yen ($67) for mobile service. [13]

The vulnerability of Japan's communication network became apparent in March 2011, when an earthquake and tsunami hit Japan's east coast and caused a nuclear disaster. Infrastructure was severely damaged, leaving many people without service for periods from a few days to one month, and restricting relief efforts. Mobile phone usage dropped by almost half in the affected areas.[14]

Network congestion and server outages—the result of increasing smartphone traffic due in part to many applications sending automatic signals every minute—also frequently affect mobile use. KDDI, one of three major mobile carriers, reported large scale disruptions in December 2012, and January and April 2013. NTT DoCoMo also dealt with four interruptions in July and August in 2012 alone.

There is no independent regulatory commission in Japan, though observers believe that the industry has generally improved in the past twelve years under the Ministry of Internal Affairs and Communications (MIC), which regulates the telecommunications, internet, and broadcast sectors.[15] Non-governmental, non-profit organizations supported by the relevant companies in the sector have been formed to self-regulate the industry. These include the television Broadcasting Ethics & Program Improvement Organization, the Content Evaluation and Monitoring Association for mobile platforms, and the Internet Content Safety Association, which manages blocking of child pornography online.[16]

---

[11] Minoru Sugaya, "Regulation and Competition in the JP Broadband Market," presentation, Pacific Telecommunications Council, January 15, 2012, http://bit.ly/16U0HvB.
[12] International Telecommunication Union, "Mobile-cellular Telephone Subscriptions, 2000-2012."
[13] Ministry of Internal Affairs and Communications, "White Paper Information and Communications in Japan 2012" [in Japanese], http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc245340.html.
[14] Izumi Aizu, "The Role of ICTs During the Disaster," *Global Information Society Watch Report (*Association for Progressive Communications: 2011) http://www.ispp.jp/ispp-wp/wp-content/uploads/2011/09/EarthquakeICT0825.pdf.
[15] Before 2001, regulation was managed by the now-defunct Ministry of Post and Telecommunications, and before that, the Diet.
[16] Broadcasting Ethics & Program Improvement Organization, "About BPO," http://www.bpo.gr.jp/?page_id=1092; Content Evaluation and Monitoring Association, "About EMA," http://www.ema.or.jp/en/index.html; Internet Content Safety Association, "About the Organization," http://www.netsafety.or.jp/.

LIMITS ON CONTENT

Restrictions that undermined internet freedom for 12 days before December 2012 election were lifted the following April. Abe and his supporters were particularly active on digital platforms. Unfortunately, nationalistic discourse lead to vitriolic hate speech directed at South Korean and Chinese communities in some internet forums. The 2011 earthquake continued to cast a long shadow online, as internet journalists not affiliated with traditional media outlets struggled to gain recognition allowing them to cover the aftermath of the nuclear disaster and related protests.

No direct political censorship has been documented in Japan. However, political speech was constrained online in the days preceding the December 2012 election under a law banning parties from using the internet in the run-up to polling. Although the law dated from 1950, it was used to stop politicians from blogging and tweeting during designated campaign periods.[17] In 2012, many retroactively deleted content posted before the campaign formally commenced on December 3rd.[18] Occasional violations led to a warning from the MIC, but no penalties or administrative deletions were reported as a result of the ban, and other candidates flouted or creatively avoided it without repercussions.[19] In April 2013, the restriction was lifted across digital platforms—though some limits on email and advertising remain—in part because Prime Minister Abe has hundreds of thousands of followers on Facebook, Twitter and local network LINE.[20] Conservative politicians had previously resisted such a revision in the past for fear it would empower their opponents.

ISPs voluntarily filter child pornography, and many offer parents the option to filter other immoral content to protect young internet users.[21] Depictions of genitalia are pixelated to obscure them for internet users based on a common—though poorly-articulated—interpretation of article 175 of the penal code, which governs obscenity.[22] Otherwise, individuals or police instruct ISPs to administratively delete contested or illegal content. A police Internet Hotline Center which cooperates with ISPs to solicit reports of illegal or harmful content from the public said it received 196,474 calls in 2012. Among them, 20 percent involved illegal content and 75 percent involved obscene material.[23] Providers are not obliged to comply but most cooperate. A few, like 2channel, notoriously refuse.

---

[17] Lower house campaigns last 12 days; upper house campaigns last 17. See, Ayako Mie, "Election Campaigning Takes to Net: New Law Opens Web to Candidates, Voters Ahead of Upper House Poll," *Japan Times*, April 11, 2013, http://www.japantimes.co.jp/news/2013/04/11/national/election-campaigning-takes-to-net/#.UY8XXqIqzFE

[18] Alexander Martin and Yoree Koh, "Before Japan Votes, Mum's the Word, Twitterwise," *Wall Street Journal,* December 13, 2012, http://online.wsj.com/article/SB10001424127887323981504578177040874830524.html.

[19] "Conservatives Dominate Japan Social Media Ahead of Poll," Reuters, December 5, 2012, http://reut.rs/WKKLqg.

[20] Arianna Huffington, "Postcard From Japan."

[21] "Japan Internet Providers Block Child Porn," Agence France-Presse, April 21, 2011, http://www.google.com/hostednews/afp/article/ALeqM5jQdti3UuXNuAqabydVSloqy5rRcA?docId=CNG.40acf6c3c3e92addbe546909e145276a.191; Electronic Network Consortium, "Development and Operation of the Next-Generation Rating/Filtering System on the Internet," press release, via New Media Development Association, April 30, 1999, http://www.nmda.or.jp/enc/rating2nd-en.html.

[22] Amanda Dobbins, "Obscenity In Japan: Moral Guidance Without Legal Guidance," 2009, Available at Selected Works, http://works.bepress.com/amanda_dobbins/1.

[23] Internet Hotline Center Japan, "Statistical Data," http://www.internethotline.jp/statistics/index_en.html.

The 2001 Provider Liability Limitation Act directed ISPs to establish a self-regulatory framework to govern take-down requests involving illegal or objectionable content, defamation, privacy violations and copyright infringement.[24] In 2002, industry associations produced guidelines designed to protect ISPs from legal liability within the jurisdiction of the Japanese courts. Under the guidelines, anyone can report material that infringes directly on their personal rights to the service provider, either to have it removed or to find out who posted it. No third party can do so. The provider notifies the individual who posted the content, and either fulfills the request with their permission or removes the content without the authors' approval if they fail to respond within two weeks. If the poster refuses permission, the service provider is authorized to assess the complaint for themselves, and comply if they believe it is legitimate. In this scenario, an ISP could give the complainant information to identify the poster—such as their name or IP address—without that person's consent, leading to privacy concerns. This process is voluntary, but by complying, service providers protect themselves from civil liability.[25] In practice, many citizens say service providers have failed to remove libelous content.

Police sometimes intervene more directly, and their emphasis on security over transparency occasionally threatens internet freedom.[26] In April 2013, they recommended ISPs and website administrators cooperate to block IP addresses used by Tor—which allows internet users to disguise their location by connecting through a network of other computers—in order to prevent criminals from abusing the service, which also has many legitimate applications.[27]

The threat of official content restrictions looms periodically during public debates about child safety, though carriers and content producers have successfully resisted intrusive regulation. In 2007, the MIC ordered mobile operators to install filtering software enabling parents to control content seen by their children. A coalition of groups, including the Japan Internet Providers Association and the user rights organization Movement of Internet Active Users lobbied against the mandate, and mobile users can now select voluntary filters. [28] Complaints to the official Consumer Affairs Agency about quasi-gambling functions in games played by children on mobile devices shot up in 2011, along with calls for government regulation.[29] In 2012, game developers Gree and DeNA Mobage voluntarily adopted caps on purchases of virtual items by minors instead.[30] Games integrated with social networks have also been criticized for their potential for abuse by sexual predators.

---

[24] "Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders," November 30, 2001, available at UNESCO, http://www.unesco.org/culture/pdf/anti-piracy/Japan/Jp_%20LimitLiability_Telecom_en.

[25] Business Software Alliance, "Country Report: Japan, 2012," http://cloudscorecard.bsa.org/2012/assets/pdfs/country_reports/Country_Report_Japan.pdf.

[26] charles, "Japan: Police Remove Messages from Cell Phone Social Networking Sites," OpenNet Initiative, https://opennet.net/blog/2009/04/japan-police-remove-messages-cell-phone-social-networking-sites.

[27] Phil Muncaster, "Japanese Feds Urge ISPs to Support Tor Ban Plan," *The Register,* April 22, 2013, http://www.theregister.co.uk/2013/04/22/tor_japan_police_ban/.

[28] Izumi Aizu, "Country Report: Japan, 2009," Global Information Society Watch, http://bit.ly/16AioGr.

[29] Ishaan, "Japanese Social Games Risk Seeing Crackdown," *siliconera,* May 7, 2012, http://www.siliconera.com/2012/05/07/japanese-social-games-risk-seeing-crackdown/.

[30] Dr Serkan Toto, "Self-Regulation: Dena Introduces Payment Caps For Minors On Mobage [Social Games]," Japan Mobile And Social Games Consulting, April 24, 2012, http://www.serkantoto.com/2012/04/24/dena-mobage-payment-caps/.

Private interests also pressure ISPs to restrict content. In June 2012, a coalition of music rights advocates were reportedly offering to sell service providers a tool to detect whether material being uploaded to the internet is subject to copyright, and sever connections of users violating Japan's strict copyright laws.[31] None are known to have purchased it.

Japanese citizens exercise some self-censorship online, often on historical and social issues. The society at large prefers "harmony," and people avoid criticizing the role of Japan's Emperor, especially when connected with historic issues like World War II. Individuals and public figures who break this code risk censure and even attacks from right-wing fanatics, who notoriously tried to assassinate the Nagasaki mayor on these grounds in the 1990s. Though exceptional, incidents like this still exert a chilling effect on Japanese expression.

There are few known cases of the government or powerful groups proactively manipulating online news or other content. In a significant exception, officials and the Tokyo Electric Power Company withheld data about pollution after a nuclear power plant in Fukushima prefecture was severely damaged by the 2011 earthquake and tsunami, and citizens unwittingly exposed themselves to radiation. The MIC requested that four industry associations monitor false or unsubstantiated content circulating about the disaster online, including on social networks. Some observers said this was a measure to control public discourse, though deletions were not widespread. Service providers removed content, which included images of corpses, in at least 13 cases,[32] though the national police agency reported 41 items for review.[33]

The disaster also had an impact on social media use. YouTube, Twitter, and international blog-hosting services are freely available, as are popular domestic platforms like Nico Nico Douga, a video-sharing site, and LINE, a chat application launched in 2011. Facebook recently overtook domestic rival Mixi, more than doubling its Japanese customer base between May 2011 and May 2012, as many users sought to connect with loved ones and exchange news on a single platform.[34] The earthquake also spurred cloud funding of civic causes,[35] and the launch of Twitter's Lifeline feature, which lists government accounts providing public information in emergencies, in September 2012.[36]

---

[31] Enigmax, "Jail For File-Sharing Not Enough, Labels Want ISP-Level Spying Regime," *TorrentFreak,* June 24, 2012, https://torrentfreak.com/jail-for-file-sharing-not-enough-labels-want-isp-level-spying-regime-120624/.

[32] Madeline Earp, "Freelance, Online Reporting Discouraged on Nuclear Threat," *CPJ Blog,* April 14, 2011, http://www.cpj.org/blog/2011/04/japan-discourages-freelance-online-reporting-on-nu.php; Ministry of Internal Affairs and Communications, "Demand for Telecommunications Carriers Associations Regarding the Appropriate Response to False Rumors on the Internet Related to the Great East Japan Earthquake," press release, April 6, 2011, http://www.soumu.go.jp/menu_news/s-news/01kiban08_01000023.html;

[33] National Police Agency, "For Police Responding to False Rumors on the Internet," June 21, 2011, http://www.npa.go.jp/archive/keibi/biki/cyber/0621ryuugenhigo.pdf.

[34] Rob Gilhooly, "Why Japan finally fell for Facebook," July 25, 2012, *New Scientist,* http://www.newscientist.com/article/mg21528756.400-why-japan-finally-fell-for-facebook.html#.Uh45IBukpTY.

[35] Examples include Just Giving, http://justgiving.jp, Give One, http://www.giveone.net, and Ready For https://readyfor.jp.

[36] Akky Akimoto, "2012 Has Been a Big Year on the Japanese Social-Media Scene," *Japan Times,* December 19, 2012, http://www.japantimes.co.jp/life/2012/12/19/digital/2012-has-been-a-big-year-on-the-japanese-social-media-scene/#.Uh46JRukpTY.

Though slowed by the aforementioned online campaigning restriction, many politicians are embracing digital tools. Toru Hashimoto, the governor of Osaka, has more than one million followers on his Twitter account @t_ishin, while the governor of Tokyo, Naose Inoki's account @inosenaoki has over 300,000. Both are popular for calling out their critics by name, including reporters and politicians. However, some news reports from the past year expressed concern about manipulated online discourse. In December 2012, the prime minister's secretary invited his Facebook supporters to bombard a public broadcaster with messages of support in advance of a scheduled panel appearance she assured them would include "Abe-bashing;" Abe subsequently updated the account himself to belittle his opponents on the panel.[37]

These interventions are more significant in the context of escalating online hate speech targeting South Koreans and Chinese communities amid territorial disputes between Japan and their respective governments. Abe's stance on these active rivalries, as well as historic ones, does nothing to calm the situation. In December 2012, he said he was reconsidering apologies Japan had made for acts of wartime aggression, including one for forcing Asian and European women to work in army brothels, which he denied was coerced. While he later retracted this position,[38] an advertisement with a government seal that appeared to support such a revisionist history was widely circulated on social media in early 2013, though it turned out to be fake.[39] The incitements to violence directed at South Korean and Chinese people—and unpatriotic activity in general—which flourished on websites like 2channel in the past year, were far more extreme, but they were arguably routed in the same nationalist discourse, which threatens to undermine the diversity of voices being heard in Japanese cyberspace.[40]

Blogs have a significant impact on public opinion, and several independent journalists are becoming influential through personal or commercial websites and social media accounts. Yet most online media remain small and community-based, with no major national successes, and the mainstream media's habit of compliance and restraint may be standing in the way of the combative online news culture flourishing elsewhere in Asia.[41] Kisha clubs, formal organizations only open to traditional media companies, and an advertising market that favors established players, may be preventing digital media from gaining a foothold in the market. Kisha clubs provide essential access to officials in Japan, but discriminate against new media practitioners. At least one online journalist was denied access to one of their Tokyo locations in October 2012.[42] The previous May, the only two freelancers permitted to join an official group of 40 reporters on a tour of the nuclear disaster site

[37] Tessa Morris-Suzuki, "Freedom of Hate Speech; Abe Shinzo and Japan's Public Sphere," *Asia-Pacific Journal 11*, 8, no. 1, (February 2013), http://www.japanfocus.org/-Tessa-Morris_Suzuki/3902#sthash.s1dMNVPK.dpuf.
[38] "Abe: No Review of Kono Statement Apologizing to 'Comfort Women,'" *Asahi Shimbun,* February 1, 2013, http://ajw.asahi.com/article/behind_news/politics/AJ201302010077.
[39] Keiko Tanaka, "No More Apologies – Japan's Facebook Users Share 'Fake' Propaganda," April 19, 2013, *Global Voices,* http://globalvoicesonline.org/2013/04/19/no-more-apologies-japans-facebook-users-share-fake-propaganda/.
[40] Tessa Morris-Suzuki, "Freedom of Hate Speech."
[41] Roger Pulvers, "Danger Lurks When Self-restraint Segues into Media Self-censorship," *Japan Times,* January 10, 2010, http://www.japantimes.co.jp/opinion/2010/01/10/commentary/danger-lurks-when-self-restraint-segues-into-media-self-censorship/#.Uh9hEhukpTY.
[42] Keiko Tanaka, "Online Journalist Barred from Japan's Diet Press Hall," *Global Voices,* October 12, 2012, http://globalvoicesonline.org/2012/10/12/online-journalist-barred-from-japans-diet-press-hall/.

were forbidden from taking equipment.[43] In the meantime, independent online news outlets have struggled to sustain themselves financially. *OhmyNews,* a South Korean platform, established a Japanese operation in 2006, but closed in 2008. The US-based *Huffington Post* digital media website launched a Japanese-language version in May 2013.[44]

A number of civil liberty groups are actively engaged in the online space. Movements for the Internet Active Users, founded by activist Daisuke Tsuda and 11 colleagues in 2007, is one example, a user rights group that contests excessive content regulation and advocates for free speech.[45]

VIOLATIONS OF USER RIGHTS

The strong protections in Japan's constitution were potentially put in jeopardy in 2012, after the now-incumbent LDP party proposed making them subject to limits to protect public order. While their reversal of a ban on internet campaigning was positive, the law retained disproportionate penalties for violating email restrictions to solicit political support, including possible jail terms. An already-strict copyright law was also strengthened during the coverage period to criminalize downloading illegal material. Public trust in the police implementing these laws was undermined when they charged an online entrepreneur for abetting a criminal, saying the bulletin board he founded failed to delete a post offering drugs for sale, and jailed four people for nearly a month on charge of sending threatening messages, though all proved to be innocent.

Article 21 of Japan's constitution prohibits censorship and protects freedom of "speech, press and all other forms of expression," as well as the "secrecy of any means of communication." [46] In general, individuals and media can exercise this in practice, though social and legal constraints exist.

In May 2012, the LDP, then in the opposition, proposed revising the constitution.[47] In December, the party gained a landslide electoral victory in the Diet, the lower house; they went on to win the senate in July 2013.[48] Critics say their draft promotes conservative nationalism, replacing the subject of the constitution—currently the people of Japan—with the nation state.[49] While it would not affect the protections outlined above, it does add that "freedoms and rights come with

[43] Reporters Without Borders, "Freelance Journalists Face Discrimination On Fukushima Plant Visit," May 23, 2012, http://en.rsf.org/japan-freelance-journalists-face-23-05-2012,42669.html.
[44] Arianna Huffington, "Postcard From Japan: Talking Zen, Abenomics, Social Networking and the Constitution With Prime Minister Shinzo Abe," *Huffington Post,* May 9, 2013, http://www.huffingtonpost.com/arianna-huffington/shinzo-abe-arianna-huffington_b_3245338.html.
[45] Movements for the Internet Active Users, "Our History," http://miau.jp/index.phtml?genre=English.
[46] "Constitution of Japan November 3, 1946," available at Prime Minister of Japan and his Cabinet, http://www.kantei.go.jp/foreign/constitution_and_government_of_japan/constitution_e.html.
[47] Liberal Democratic Party of Japan, "LDP Announces a New Draft Constitution for Japan," May 7, 2012 http://www.jimin.jp/english/news/117099.html. Japanese text available at Liberal Democratic Party of Japan: http://www.jimin.jp/policy/policy_topics/pdf/seisaku-109.pdf.
[48] "Japanese Prime Minister's Party Scores Win in Senate Elections," Agencia EFE, July 21, 2013, http://www.globalpost.com/dispatch/news/agencia-efe/130721/japanese-prime-ministers-party-scores-win-senate-elections.
[49] Michael Hoffman, "Constitutional Revision May Bring Less Freedom," *Japan Times,* February 3, 2013, http://www.japantimes.co.jp/news/2013/02/03/national/constitutional-revision-may-bring-less-freedom/#.Uh5iBBukpTY.

responsibilities and duties, and shall not violate public interest and public order." A national referendum must still approve the revision, which would also lower the bar for making future constitutional changes.

A more positive LDP initiative undid long-standing restrictions on use of the internet for election campaigns for the first time in 2013, and a revision of Public Offices Election Act passed the Upper House on April 19. Limits remained on paid online advertising and campaign emails, which could only be sent directly by a party or candidate—not a supporter—in a measure designed to prevent fraud, though members of the electorate can freely solicit support on social media.[50] While these provisions were contested and revisions are still planned, [51] news reports during the coverage period said politicians violating these restrictions face a potential 300,000 yen ($3,060) fine or one year in prison; imprisonment would strip them of political rights to vote or run for office. Voters found improperly soliciting support for a candidate via e-mail could be fined 500,000 yen ($5,100) or jailed for two years, which would also deprive them of political rights.[52]

Another legal revision passed during the coverage period of this report introduced potentially disproportionate sentences for copyright violators—including any internet user downloading content they know has been illegally copied, as opposed to those engaged in piracy for commercial gain. [53] While both uploading and downloading pirated material was already illegal under the copyright law, with uploaders subject to 10 years imprisonment or fines up to 10 million yen ($102,000), the version in effect since October 1, 2012 added two years in jail or fines up to two million yen ($20,500) for downloading a single file.[54] The Japanese Bar Association said that downloading, as an essentially insignificant personal act, should be regulated by civil, instead of criminal laws.[55] Police launched a nationwide antipiracy crackdown, searching 124 different locations and arresting 27 people under the law in in February 2013.[56]

The sentences for copyright and e-mail fraud seem particularly harsh in light of Japan's lack of restrictions on child pornography and hate speech online, which are acceptable to limit under international law.[57] Laws passed in 1999 and 2003 outlawed the production, distribution and sale of

---

[50] "Editorial: Internet Election Campaigns can Change Japan's Politics," *Asahi Shimbun,* April 20, 2013, http://ajw.asahi.com/article/views/editorial/AJ201304200031.

[51] Ida Torres, "Japan's Internet Election Campaigning Ban One Step Closer to Being Lifted," *Japan Daily Press,* April 4, 2013, http://japandailypress.com/japans-internet-election-campaigning-ban-one-step-closer-to-being-lifted-0426427/.

[52] Ayako Mie, "Election Campaigning Takes to Net;" "Japanese Parliament Permit Use of Internet Campaigning During Elections," TJC Global, April 20, 2013, http://tjcglobal.wordpress.com/tag/public-offices-election-law/.

[53] Daniel Feit, "Japan Passes Jail-for-Downloaders Anti-Piracy Law," *Wired,* June 21, 2012, http://www.wired.com/gamelife/2012/06/japan-download-copyright-law/.

[54] Maira Sutton, "Japan's Copyright Problems: National Policies, ACTA, and TPP in the Horizon," Electronic Frontier Foundation, August 21, 2012, https://www.eff.org/deeplinks/2012/08/copyright-japan.

[55] "Japan Introduces Piracy Penalties for Illegal Downloads," BBC, September 30, 2012, http://www.bbc.co.uk/news/technology-19767970.

[56] Some had uploaded TV and music. See, "27 People Arrested in Simultaneous Crackdown of Copyright Violations Across Country," JWSSN News, February 23, 2013, http://blog.livedoor.jp/misutiru7878/archives/24818756.html; Bryan Bishop, "Japanese Authorities Arrest 27 in Nationwide File-Sharing Crackdown," *The Verge,* March 3, 2013, http://www.theverge.com/2013/3/3/4059720/japanese-authorities-arrest-27-in-nationwide-file-sharing-crackdown.

[57] United Nations Human Rights, "Freedom of Expression Everywhere, Including in Cyberspace," November 4, 2011, http://www.ohchr.org/EN/NewsEvents/Pages/Freedomofexpressioneverywhere.aspx.

hardcore child pornography, including electronically,[58] but possessing it for non-commercial use remains legal except in Kyoto prefecture, central Japan, where police arrested three people for purchasing child pornography online for the first time in September 2012 under an ordinance in effect since the previous January.[59] Although nationalistic hate speech and incitement to racially-motivated violence is proliferating online, the government has taken no action to curb it on grounds it is already criminalized under the penal code; yet police in 2012 were more likely to use the relevant clauses to prosecute antinuclear demonstrators than groups whose on and offline slogans included exhortations to "kill Koreans."[60]

Article 175 of the Japanese penal code bans the sale or distribution of broader categories of obscene material, and while it dates from over 100 years ago, it is considered to apply online. [61] However, it does not define what constitutes obscenity, leading to concerns that it may infringe on artistic expression and LGBT rights.[62]

No citizens have faced politically motivated arrest or prosecution for content they have published online, though observers believe that police sometimes overstep during cybercrime investigations. Four people, including a student, were detained for nearly a month in July 2012 for sending electronic terrorism threats that had actually been triggered without their knowledge, by malware.[63] In November 2012, police charged 2channel founder Hiroyuki Nishimura with abetting the drug trade, saying he failed to delete a post from someone trading amphetamines on the rambunctious bulletin board; the allegation was complicated by the fact that Nishimura no longer manages the site,[64] and was dropped without explanation in March.[65] Police were less diligent in another case, however. On November 6, 2012, a woman in Kanagawa prefecture was stabbed and killed by a stalker police had refused to investigate in March, when she reported him for sending over 1000 threatening emails in 20 days—in part because the law governing stalking does not explicitly ban harassment via email.[66] A bill to establish an independent human rights commission

[58] William Sparrow, "Japan's Lolita Merchants Feel the Heat," *Asia Times Online,* February 23, 2008, http://www.atimes.com/atimes/Front_Page/JB23Aa02.html.
[59] Tomasz Janowski and Teppei Kasai, "Pressure on Japan for Stronger Laws on Child Pornography," Reuters, September 19, 2012, http://uk.reuters.com/article/2012/09/19/us-japan-pornography-idUKBRE88I07H20120919.
[60] Tessa Morris-Suzuki, "Freedom of Hate Speech."
[61] James R. Alexander, "Obscenity, Pornography, and the Law in Japan," *Asian-Pacific Law and Policy Journal* 4, no.1 (February 2003), available at University of Pittsburgh Johnstown, http://faculty.upj.pitt.edu/jalexander/Research%20archive/Japanese%20obscenity%20law/Oshima%20article.pdf; "Penal Code, Act No. 45 of April 24, 1907," available at Japanese Law Translation, http://www.japaneselawtranslation.go.jp/law/detail/?ft=2&re=02&dn=1&yo=penal+code&x=0&y=0&ky=&page=1.
[62] Keiko Tanaka, "Japan's Porn Law is Strangling Artists," February 18, 2013, http://globalvoicesonline.org/2013/02/18/japans-porn-law-is-strangling-artists/.
[63] "Police Release Suspects, say Virus Likely Used to Threaten Mass Murder," *Asahi Shimbun,* October 8, 2012, http://ajw.asahi.com/article/behind_news/social_affairs/AJ201210080093. "Police Arrest Tokyo Man in Malicious Computer Hacking Case," *Asahi Shimbun,* February 10, 2013, http://ajw.asahi.com/article/behind_news/social_affairs/AJ201302100067.
[64] "Prosecution of 2channel Founder Draws Flak," *Japan Times,* November 26, 2012, http://www.japantimes.co.jp/news/2012/12/26/national/prosecution-of-2channel-founder-draws-flak/#.UiC26jakpTZ.
[65] "Charges Dropped Against 2ch Founder Hiroyuki Nishimura," *Anime News Network,* March 19, 2013, http://www.animenewsnetwork.com/news/2013-03-19/charges-dropped-against-2ch-founder-hiroyuki-nishimura.
[66] Keiko Tanaka, "Standing Up for Stalking Victims in Japan," *Global Voices,* December 11, 2012, http://globalvoicesonline.org/2012/12/11/standing-up-for-stalking-victims-in-japan/.

which may address online abuses like cyberbullying was announced in September 2012, but the details and possible timeframe involved remain unclear.[67]

Japan's Supreme Court protects privacy through its interpretation of Article 13 of the constitution, which provides for the right to life and liberty,[68] while 2003 laws specifically protect personal data amounting to more than 5,000 records collected electronically by both the private and the public sector.[69] Law enforcement requests for this data should be supported by a warrant, though some cooperate without one.[70] Individuals may be afforded less due process. In November 2012, police raided the home of Yuzuru Kaneko, who documented antinuclear protests on YouTube, seizing his footage and equipment in an attempt to prove wrongdoing by one of the protesters.[71]

Under voluntary guidelines drafted by four ISPs in 2005, service providers automatically inform police of internet users identified on pro-suicide websites, and comply with law enforcement requests for information related to acts of self-harm.[72]

Through the Resident Basic Register Network System in effect for over a decade, Japanese citizens' unique ID numbers are stored in a national *juki-net* computer network which critics say is vulnerable to cyberattacks, although this risk is partially offset by the fact that it has no centralized database.[73] Some individuals and municipalities have refused to participate in the database.[74] A "My Number Bill" proposed by the cabinet in 2012 would potentially increase the kinds of personal data government agencies would collect and share electronically, a measure the Japanese Bar Association and other groups oppose for threatening privacy.[75]

"Secrecy of communication" is protected under telecommunications laws,[76] and there are no restrictions on anonymous online speech except in internet cafes, where users are required to produce formal ID such as a driver's license and register their name and address. Police can request these details, along with usage logs, if they detect illegal online activity. A law enacted in 2003 and

[67] Keiko Tanaka, "Japan: Anxiety Over Human Rights Commission Bill," *Global Voices,* September 25, 2012, http://globalvoicesonline.org/2012/09/25/japan-anxiety-over-human-rights-commission-bill/.
[68] Privacy International, "Chapter i: Legal Framework," in *Japan*, December 12, 2006, https://www.privacyinternational.org/reports/japan/i-legal-framework.
[69] Business Software Alliance, "Country Report: Japan."
[70] Privacy International, "Chapter iii: Privacy Issues," in Japan, December 12, 2006, https://www.privacyinternational.org/reports/japan/iii-privacy-issues.
[71] Keiko Tanaka, "Police Raid Video Blogger's Home in Japan," November 15, 2012, http://globalvoicesonline.org/2012/11/15/police-raid-video-bloggers-home-in-japan/.
[72] Carolina A. Klein, "Live Deaths Online: Internet Suicide and Lethality," *American Academy of Psychiatry and the Law* 40 no. 4 (December 2012) 530-536, http://www.jaapl.org/content/40/4/530.full.
[73] Rebecca Bowe, "In Japan, National ID Proposal Spurs Privacy Concerns," Electronic Frontier Foundation, June 13, 2012, https://www.eff.org/deeplinks/2012/06/japan-national-id-proposal-spurs-privacy-concerns.
[74] Privacy International, "Chapter iii: Privacy Issues."
[75] Japanese Bar Association, "Statement Submitted to Parliament and the Cabinet Regarding the 'Social Security and Tax Number System' Bill," February 15, 2012, http://www.nichibenren.or.jp/activity/document/statement/year/2012/120215_6.html.
[76] Ministry of Internal Affairs and Communications, "Telecommunications Business Act," December 25, 1984, http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_2.pdf.

revised in 2008 prohibits electronic communications encouraging sexual activity with minors.[77] Under the law, all online dating services must register with police, verify their customers' ages with a driver's license or credit card, and delete or block content that appears to involve someone under 18; most services voluntarily monitor messages in real time to ensure compliance.

Under a wiretap law enacted in 1999, law enforcement agents may seek a court order to conduct electronic surveillance in criminal investigations involving drugs, firearms, human trafficking, or organized murders, an exception to articles of other laws that explicitly forbid wiretapping.[78] The law obliges agents to notify targets of wiretaps after investigations are concluded and inform the Diet about the number they implement annually. While the law was extremely controversial when it passed, in part due to the authorities' politicized abuse of surveillance in the recent past,[79] lawmakers were seeking to expand it in December 2012.[80] Critics say the law does not prevent the systematic storage of intercepted communications or protect innocent parties.[81] Security agents and the military have been accused of implementing surveillance in cases involving national security.[82]

No physical violence has been reported against bloggers or internet users in relation to their online activity. While distributed denial-of-service (DDoS) attacks were part of the arsenal used by nationalists in Japan, China and South Korea to target perceived opponents in other countries, and cyberattacks have been reported against commercial and government targets,[83] they are not known to have been used to systematically target individuals or civil society groups. In acts of protest against the copyright law, hackers briefly targeted websites of several political parties and institutions in October 2012.[84]

---

[77] Akira Saka, "Regulation for Online Dating in Japan," presentation Keio University, 2008, http://saka.jp/lecture/ChildProtenctionbyRetulationOnlineDatingSites2.pdf.
[78] Privacy International, "Chapter ii: Surveillance," in *Japan*, December 12, 2006, https://www.privacyinternational.org/reports/japan/ii-surveillance-policy.
[79] In 1997, a court ordered the government to pay a senior member of the Japanese Communist Party 4 million yen [US$35,500] in damages for illegally wiretapping his residence in the 1980s. See, "Tokyo, Kanagawa Bow to Wiretap Ruling," *Japan Times,* July 7, 1997, http://www.japantimes.co.jp/news/1997/07/10/national/tokyo-kanagawa-bow-to-wiretap-ruling/#.Uh-8fRukpTY.
[80] Tsuyoshi Tamura, "Legal Panel to Discuss Wiretapping for Wider Range of Crimes," *Asahi Shimbun,* December 25, 2012, http://ajw.asahi.com/article/behind_news/social_affairs/AJ201212250065.
[81] Privacy International, "Chapter ii: Surveillance."
[82] "Japan's Military Watched Citizens: Communist Party," Reuters, via *bdnews24*, June 6, 2007, http://bdnews24.com/world/2007/06/06/japan-s-military-watched-citizens-communist-party.
[83] "Over 1,000 targeted cyber-attacks hit Japanese entities in 2012," *Japan Times,* March 1, 2013, http://www.japantimes.co.jp/news/2013/03/01/national/over-1000-targeted-cyber-attacks-hit-japanese-entities-in-2012/#.Uh-e2RukpTY.
[84] Stacey Leasca, "Japan introduces strict anti-piracy laws," *Global Post,* October 1, 2012, http://www.globalpost.com/dispatch/news/regions/asia-pacific/japan/121001/japan-introduces-strict-anti-piracy-laws.

JORDAN

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	13	13
Limits on Content (0-35)	12	13
Violations of User Rights (0-40)	20	20
Total (0-100)	45	46

* 0=most free, 100=least free

POPULATION: 6.3 million
INTERNET PENETRATION 2012: 41 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Amendments to the Press and Publications Law were passed in September 2012, requiring news websites to obtain licenses in order to continue to operate in the country (see **LIMITS ON CONTENT**).
- Online editors and site owners are now officially liable for comments posted by other users on their platforms, increasing the need for pre-censorship (see **LIMITS ON CONTENT**).
- The offices of the online media company Watan were ransacked in July 2012 and several news websites were the victims of cyberattacks over the past year (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

This report covers events between May 1, 2012 and April 30, 2013. On June 2, 2013, the Telecommunication Regulatory Commission instructed internet service providers to block over 200 websites. The sites had failed to obtain a license from the Department of Press and Publications after the expiration of a nine-month grace period granted by authorities. These actions have their foundations in amendments to the Press and Publications Law passed in September 2012. The law imposes disproportionately-heavy burdens on intermediaries and unnecessary obstacles to registration. The editors-in-chief of all news websites must be members of the Jordan Press Association for a prior period of at least four years. On July 2, authorities revealed that 254 news sites had been blocked, while 111 have been licensed. Previously, only one news website was known to be blocked in Jordan. The recent moves signal a drastic shift in the country's attitude towards online censorship and mounting fears over the power of the internet in the face of increasing discontent in the traditionally stable kingdom.

INTRODUCTION

Jordan, a small kingdom of about six million people, has prided itself as being an example of stability and incremental political reform. The Jordanian government's response to relatively low-level public protests in 2011 was mild compared to neighboring countries and other monarchies in the Gulf. Working with parliament, the king passed a set of constitutional amendments to improve protections on freedom of expression and strengthen the independence of the judiciary. Protests returned, however, in November 2012, when thousands of protestors took to the streets of Amman and other major cities to protest a rise in fuel prices.[1] Hundreds of protesters were arrested by security forces in the ensuing chaos. Parliamentary elections in January 2013 resulted in limited political developments, with supporters of the king maintaining a strong majority in the lower house of parliament (members of the upper house are appointed by the king himself).[2] The elections do not seem to have quelled repeated calls for greater political reform and were boycotted by opposition parties including the Islamic Action Front, the political arm of Jordan's Muslim Brotherhood.[3]

Internet access was first provided to Jordanians in 1995, the same year the Telecommunications Regulatory Commission (TRC) was established to regulate the country's information and communication technology (ICT) sector.[4] Recognizing the economic potential of the internet,

[1] Aalektisadia (2012, November 13) Demonstrations, roads blocking and confrontations in Jordan after rise in Fuel prices. Accessed June 26, 2013. http://www.alegt.com/2012/11/13/article_709448.html
[2] Tucker, Joshua(2013, January 25) 2013 Jordan Post-Elections Report: And the winner is …the King. Accessed June 27,2013. http://themonkeycage.org/2013/01/25/2013-jordan-post-election-report-and-the-winner-isthe-king/
[3] "Jordan election: Voting ends as Islamists allege fraud," BBC News, January 23, 2013, http://www.bbc.co.uk/news/world-middle-east-21158713.
[4] The TRC was established as a financially and administratively independent jurisdictional body through the Telecommunications Law (No. 13 of 1995) and a subsequent amendment (Law No. 8 of 2002).

authorities actively promoted ICT development in the kingdom.[5] Once seen as a means of trivial entertainment and the exchange of scandalous or banned information, the internet has grown into a vital instrument for business and an important forum for public discussion. Likewise, as the number of users began to increase dramatically, the government drew up legal methods for maintaining control over online content and monitoring users.

In this regard, restrictions on internet freedom have increased since the regional uprisings of 2011. News websites, a vital source of information in a country where traditional media freedom is limited, often face pressure from state actors to delete politically-sensitive articles. In August 2012, around 1,000 websites temporarily went offline to protest proposed amendments to the 1998 Press & Publications Law.[6] The amendments impose a variety of burdensome requirements to operate online news portals, limiting freedom of expression and placing heavy liabilities on intermediaries. Despite the opposition campaign, the new amendments were passed on September 19, 2012.[7] While censorship is due to increase, prosecutions and extralegal attacks on users appears to have declined in severity over the past year. Nonetheless, during the coverage period, the offices of an online media company were raided and several news sites suffered cyberattacks by unidentified perpetrators.

OBSTACLES TO ACCESS

According to the International Telecommunication Union (ITU), a total of 41 percent of the Jordanian population accessed the internet in 2012.[8] National figures from the TRC estimated the number of users to be much higher in the first quarter of 2013, at 69 percent, or 4.45 million users.[9] Given the large number of people accessing the internet at cybercafes and offices, most users have access to broadband rather than dial-up connections.[10] Furthermore, most internet users are young people ranging from ages 15 to 24.[11]

Mobile phone use has also expanded rapidly and by the end of 2012, the number of subscriptions was over 9 million, representing a penetration rate of 139.1 percent.[12] 3G services were first launched by Zain and Jordan Telecom (Orange) in mid-2010 and increased in 2012 upon implementation of a tax exemption for the purchase of smartphones and the launch of mobile

[5] Privacy International, "Jordan," *Silenced: An International Report on Censorship and Control of the Internet*, 2003, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-103564.
[6] The blackout was called by a group of internet users called 7uryanet (freedom for the internet)
[7] http://www.lob.gov.jo/ui/laws/all_modified_law.jsp?no=32&year=2012&law_no=8&law_year=1998. Accessed April, 30, 2013.
[8] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2012, accessed July 5, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[9] Telecommunications Regulatory Commission of Jordan's official website [in English], accessed June 26, 2013. http://www.trc.gov.jo/index.php?option=com_content&task=view&id=2603&Itemid=1&lang=english.
[10] Telecommunications Regulatory Commission of Jordan's official website.
[11] Mohammad Ghazal, "News websites most popular destination for Jordanian Internet users—study," The Jordan Times, March 22, 2012, http://jordantimes.com/news-websites-most-popular-destination-for-jordanian-internet-users----study.
[12] International Telecommunication Union (ITU), "Fixed (wired)-broadband subscriptions," 2000-2012, accessed July 5, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

broadband by another provider, Umniah.[13] A call from the TRC to introduce a fourth mobile operator in December 2012, however, was rejected by Zain and Jordan Telecom.[14] No new providers have been introduced since then and the three companies have a similar share of the market. [15]

The expansion of fixed-line internet access has been hampered by the relatively high costs of computers and connectivity. Indeed, fixed broadband subscriptions have decreased since 2009, with only 3 subscriptions per 100 inhabitants.[16] On the other hand, mobile broadband use has soared to over 812,000 subscribers, or 73 percent of all internet subscriptions.[17]

For several years, internet connection fees were considered high relative to neighboring countries and the cost of living. Prices have decreased, reportedly upon direct orders from the king, but complaints about the quality of service persist. Monthly fixed-line subscription prices currently range from JOD 13 ($18) for speeds of 128 Kbps and an allowance of 10 Gigabytes (GB), to JOD 65 ($92) for speeds of up to 24 Mbps and a 65 GB allowance. Postpaid monthly plans for Evolved High-Speed Packet Access (HSPA+) range from JOD 5 ($7) to JOD 49 ($69) per month, depending on speeds and data allowances.[18] By comparison, gross national income per capita is $6,130, or only $511 per month.[19] Meanwhile, internet access in remote areas remains poor, as almost all companies concentrate their operations and promotions in major cities, particularly the capital Amman.

The ICT sector is regulated under Law No. 13 of 1995 and its amendment, Law No. 8 of 2002. The law endorses free-market policies and governs licensing and quality assurance.[20] Citizens and businesses can obtain internet access through privately owned service providers without state approval or registration. As of November 2011, there were 16 active internet service providers (ISPs) in Jordan, though licenses have been granted to over 20 companies.[21] The market is dominated by Umniah (a subsidiary of Batelco Bahrain), Zain, and Jordan Telecom, the local affiliate of France Telecom's Orange brand. The formerly state-owned Jordan Telecom controls the fixed-line network and provides access to all other ISPs, thereby centralizing most of the

[13] ITU, "Smartphone tax exemption drives 3G growth (Jordan)," news release, January 19, 2012, http://www.itu.int/ITU-D/ict/newslog/Smartphone+Tax+Exemption+Drives+3G+Growth+Jordan.aspx.
[14] Ghazzal, Mohammad "Orange Jordan Opposes TRC Plan," Jordan Times, December 15, 2012. http://jordantimes.com/orange-jordan-opposes-trc-plan, accessed April 30, 2013.
[15] Mai Barakat, "Jordan will be challenging, but a fourth operator might find elbow room as a mobile broadband provider," Informa, February 21, 2013, http://blogs.informatandm.com/9181/jordan-will-be-challenging-but-a-fourth-operator-might-find-elbow-room-as-a-mobile-broadband-provider/.
[16] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2000-2012, accessed July 5, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[17] "Telecommunications Indicators (Q1-2013)," Telecommunications Regulatory Commission – Jordan, 2013, accessed July 5, 2013, http://www.trc.gov.jo/index.php?option=com_content&task=view&id=2603&Itemid=1&lang=english.
[18] "Broadband," Zain, accessed July 5, 2013, http://www.jo.zain.com/english/consumer/broadband/Pages/default.aspx.
[19] "GNI per capita, PPP" World Bank Databank, 2008-2012, accessed July 5, 2013, http://data.worldbank.org/indicator/NY.GNP.PCAP.PP.CD.
[20] "Jordan," *One Social Network With A Rebellious Message,* Arabic Network for Human Rights Information, 2009, http://www.openarab.net/en/node/1618.
[21] ITU, *ICT adoption and prospects in the Arab region,* Connect Arab Summit 2012, pg. 57, http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-AR-2012-PDF-E.pdf.

connection to the international internet. All traffic must flow through a government-controlled telecommunications hub.

The TRC is the independent agency responsible for regulating the ICT sector. It is governed by the Telecommunications Law and defined as a "financially and administratively independent juridical personality."[22] Nonetheless, it is accountable to the Ministry of Information and Communication Technology (MoICT), which in turn was created in April 2002 to drive the country's ICT development.[23] The TRC's Board of Commissioners and its chairman, currently Mohammad al-Taani,[24] are appointed by a resolution from the Council of Ministers based on a nomination from the prime minister.[25] The government retains a degree of control over the country's internet backbone and traffic must flow through a government-controlled telecommunications hub. Nonetheless, the TRC is generally seen as independent and fair in its decision making, though it does coordinate policy with the government.

LIMITS ON CONTENT

Although the Jordanian government did not engage in extensive blocking of websites from May 2012 to April 2013, changes to the PPL have drastically altered the country's legal framework, opening the door to censorship of any website not in compliance with the law. Intermediaries face increasing liability for content posted to their sites and new restrictions laid the groundwork for the widespread blocking of internet news sites. On a positive note, Jordan witnessed several notable online campaigns over the past year, indicating users' growing interest in utilizing online tools for activism. YouTube, Facebook, Twitter, and international blog-hosting services are freely available and very popular in the country. Crucially, however, social media activity and numerous protests over amendments to the press law failed to halt the bill from being passed in September 2012. Furthermore, a nine-month grace period in which websites must register with authorities was set to expire in June 2013.

The amended PPL places restrictions on online news editors and requires news websites to register with the government. According to Article 49(A), any electronic publication which publishes domestic or international news, press releases, or comments is required to register with the Ministry of Commerce and Industry and acquire a license from the Department of Press and Publications (DPP).[26] For many observers, the law's broad definition of a news website could have included almost all Jordanian and international websites, blogs, portals, and social networks. Articles 48 and 49 enable the Director of the DPP to block any website for failing to obtain a

[22] The Telecommunications Regulatory Commission of Jordan, *Chapter III*, http://www.trc.gov.jo/index.php?option=com_content&task=view&id=20&lang=english.
[23] "Jordan ICT Sector Profile," Information & Communications Technology Association – Jordan, Slide 10, accessed July 5, 2013, http://intaj.net/sites/default/files/jordan_ict_sector_profile.pdf.
[24] Telecommunications Regulatory Commission of Jordan, *Mohammad Al Taani, Chairman of the Board of Commissioners/CEO*, http://www.trc.gov.jo/index.php?option=com_content&task=view&id=126&Itemid=1079&lang=english.
[25] Telecommunication Regulatory Commission Jordan. Telecommunication Law No. (13) of 1995, p. 18, accessed June 26,2013. http://www.trc.gov.jo/images/stories/pdf/telecomunication%20law.pdf?lang=english.
[26] Law number (32) 2012. Amendments to The Press and Publications law for the Year 1998 (8).

license or, more broadly, for violating Jordanian law. In addition to facing blocking, unlicensed websites also face a potential fine of JOD 1,000–5,000 ($1,500–7,500) according to Article 48(B). The law also requires that editors-in-chief of online outlets must have been prior members of the Jordan Press Association (JPA) for a period of at least four years. The Director of the DPP estimated that Jordan contains some 400 news websites.[27]

Jordan does not have a history of extensive web filtering and, for a number of years, the only blocked website was the U.S.-based *Arab Times*, which often takes a critical tone toward Arab regimes.[28] In the past, however, authorities have attempted to introduce greater restrictions. In 2008, authorities blocked access to about 600 websites on internal government networks, claiming such measures were necessary to prevent public service employees from wasting time online. The inclusion of key Jordanian news websites among those blocked raised concerns that the purpose was also to limit government employees' access to independent information.[29] Marouf al-Bakhit, the prime minister at the time, reversed this policy in 2011. More recently, rumors resurfaced that the MoICT was seeking to block access to pornographic sites. On numerous occasions, internet freedom activists have criticized reports that the ministry has instructed ISPs to block explicit content.[30] On the other hand, some groups have staged small protests and even launched a Facebook campaign to push the MoICT to block pornography sites, most recently in July 2012.[31] According to one official, authorities may instead insist that ISPs offer a voluntary service to block these sites for subscribers.[32]

In a more subtle censorship dynamic, website owners have occasionally acted to remove online content after receiving informal complaints from government officials, members of the security services, party leaders, lawmakers, journalists, and even ordinary users. Websites that have refused such requests have faced reprisals. For example, in February 2011, one of the country's most popular news websites, *Ammon News*, was hacked and temporarily disabled after its editors refused to comply with security agents' demands to remove a statement by 36 prominent Jordanian tribesmen, in which they called for democratic and economic reforms. Among other actions, the hackers deleted the joint statement, which represented a politically-sensitive development given such groups' historic support for the monarchy.[33] In another incident from March 2012, the Jordanian Royal Court pressured the website of the *al-Arab al-Yawm* newspaper to delete an article

[27] BBC Arabic (2013, June) The Blocking of 290 websites in Jordan. Accessed June 26, 2013. http://www.bbc.co.uk/arabic/middleeast/2013/06/130603_jordan_electronic_sites_closed.shtml. AlBawaba.Com (2013, June 5) Jordan: Lifting up the Block only on a few websites. accessed June 26, 2013.
[28] A test by Freedom House in February 2012 confirmed that the website remains inaccessible. See also, "Jordan," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/jordan.
[29] Arab Archives Institute, "Fear of Freedoms: King Insists on Freedoms, Government Resists," news release, December 6, 2008, http://www.ifex.org/jordan/2008/12/09/capsule_report_despite_advances/; "Public Employees Wasting Time on the Internet," The Jordan Times, August 5, 2010, http://www.jordantimes.com/index.php?news=28938.
[30] "Internet freedom activists slam ministry's call to block porn sites," Ammon News, August 1, 2012, http://en.ammonnews.net/article.aspx?articleno=17418#.UdsThPm1EwA.
[31] "Protest calls on Gov't to block Porno sites," Ammon News, July 16, 2012, http://en.ammonnews.net/article.aspx?articleno=17418#.UdsThPm1EwA.
[32] Majed Al Dabbas, "Govt will not block porn sites," Ammon News, April 27, 2013, http://en.ammonnews.net/article.aspx?articleno=20775#.UdsS7Pm1EwA.
[33] "In Jordan, website hacked after running sensitive statement," Committee to Protect Journalists, February 9, 2011, http://cpj.org/2011/02/in-jordan-website-hacked-after-running-sensitive-s.php.

titled, "We will not live in a stupid man's robe," which criticized the government's handling of corruption and protests in the city of al-Tafila.[34] In other cases, news websites that tackle sensitive issues must deal with waves of angry comments from conservative readers.

The 2012 amendments of the PPL treat readers' comments under the same restrictions as normal news content. Clause 3 of Article 49 states that both the editors-in-chief and owners of online publications are legally responsible for all content posted to the site, including user comments.[35] Moreover, websites must keep a record of all comments for six months after initial publication and refrain from publishing any "untruthful" or "irrelevant" comments.[36] Journalists in Jordan stated that the new changes in the law aim at increasing self-censorship and instigating fear among journalists.[37]

The amended law also affects the financial viability of online news websites. The amended PPL prohibits foreign investment in newspapers, a provision that could now apply to online news outlets as well. Meanwhile, in mid-2012, unconfirmed reports emerged of government agencies pressuring advertisers to avoid certain news websites in an effort to limit the sites' income.[38] There have also been some initial reports of security or government officials offering encouragement—and possibly material support—to journalists to establish news websites favorable to the government that would compete with the increasingly influential, and often critical, existing online outlets.[39]

The threat presented by restrictive laws and financial penalties in the PPL, combined with an awareness of extensive content monitoring, has a chilling effect on online speech. Bloggers and news website owners often complain about their inability to post news freely due to monitoring. Many practice self-censorship and rarely cross the standard red lines, particularly concerning material that could be perceived as harmful to national security, national unity, the country's economy, or the royal family. Traditional journalists often start their own blogs in order to be free from editorial censorship. Since 2011, blogs have regained their importance as an avenue for debate on political and social issues. A growing number of blogs are also written in Arabic, a shift from several years ago when most were in English or bilingual.

Nonetheless, the country's hundreds of news websites are an increasingly important source of information and analysis for many Jordanians. Many feel that online sources discuss a wide range of

[34] International Freedom of Expression Exchange (IFEX), "Royal Court orders newspaper to remove critical article from website," news release, March 26, 2012, http://www.ifex.org/jordan/2012/03/26/article_censored/.
[35] Law number (32) 2012. Amendments to The Press and Publications law for the Year 1998 (8).
[36] Law number (32) 2012. Amendments to The Press and Publications law for the Year 1998 (8).
[37] Tarawnah, Naseem "Jordan Internet Goes Dark" Foreign Policy. August 31, 2012. http://mideast.foreignpolicy.com/posts/2012/08/31/jordans_internet_goes_dark. Accessed April 30, 2013. And Sweis, Rana "Jordan Limits Protests, and Internet as Tensions Simmer" New York Times. September 19, 2012. http://www.nytimes.com/2012/09/20/world/middleeast/jordan-limits-protests-and-internet-as-tensions-simmer.html?pagewanted=all&_r=1&. Accessed April 30, 2013.
[38] "Campaign on websites and the government refuses to license" [in Arabic], Allofjo, May 30, 2012, http://www.allofjo.net/index.php?page=article&id=29643.
[39] "Liberal Press: government seeks to break the power forward positions" [in Arabic], JO24, May 29, 2012, http://www.jo24.net/index.php?page=article&id=5179.

topics typically avoided by traditional media outlets. A study released by the market research firm Ipsos in March 2012 found that around 70 percent of internet users accessed news websites, making it the most popular area of online interest, surpassing music and sports.[40] Seven news websites—*Jfranews, Garaanews, Sarayanews*, *Tasweernews, Alwakeelnews Sameerbook*, and *Khaberni*—were among the top 20 most visited websites in the country in mid-2013, up from only three news sites in March 2012.[41]

Web 2.0 applications such as Facebook, the micro-blogging service Twitter, and the video-sharing site YouTube are very popular, particularly among younger Jordanians. There are over two million Facebook users in Jordan, representing over one-third of the country's population.[42] Twitter has garnered a much smaller following of around 60,000 users.[43] Several local social media tools, such as the Jordanian microblogging site WatWet, have shutdown in recent years over an inability to compete.[44] Several state officials, including Queen Rania and the Minister of Information, have established Facebook and Twitter accounts to communicate with the public.

These online tools, in addition to news websites, have played an important role in mobilizing public protests to oppose restrictions on free expression, to call for broader political reforms, and to protest government policies. Over 500 websites went offline on August 29, 2012 in a coordinated protest to the changes in the PPL.[45] The home pages to these sites displayed a black screen with text reading, "You may be deprived of the content of this site under the amendments of the Jordanian Press and Publications Law and the governmental internet censorship."[46] Facebook played a particularly important role in 2012, when activists used it to mobilize against a rise in fuel prices in November of that year. The *Habbet Teshreen* ("November Demonstration") hashtag was trending for almost a week on Twitter. Demonstrations have continued throughout the year, with online media playing a central role in keeping the public informed of recent events. Social media has also been critical in documenting attacks against demonstrators by police, *darak* (special riot police known as "riders"), government loyalists, and other actors.

---

[40] "News websites most popular destination for Jordanian Internet Users," Zawya.com, accessed September 18, 2012, http://www.zawya.com/story.cfm/sidZAWYA20120323115500/News_websites_most_popular_destination_for_Jordanian_Internet_users (subscription required).
[41] "Top Sites in Jordan," Alexa Web Information Company, accessed July 8, 2013 and March 27, 2012, http://www.alexa.com/topsites/countries/JO.
[42] "Jordan Facebook Statistics," Social Bakers, accessed March 28, 2012, http://www.socialbakers.com/facebook-statistics/jordan.
[43] Salem, Fadi., & Murtada, Racha (2012, July) Arab Social Media Report. Vol.2, No.1. Dubai School of Government. Dubai, UAE. Pp.10,12,15, Accessed June 26, 2013. http://www.dsg.ae/en/Publication/Pdf_En/826201211212209347849.pdf.
[44] "On Shutting Down WatWet," Tootcorp.com, July 2011, http://tootcorp.com/2011/07/on-shutting-down-watwet/ (site discontinued).
[45] Ruth Michaelson, "Jordan blocks over 200 'unlicensed' websites," Index on Censorship, June 3, 2013, http://www.indexoncensorship.org/2013/06/jordan-blocks-over-200-unlicensed-websites/.
[46] 7oryanet.com "Ammendemnts to the Press and Publications Law," September 20, 2012. http://7oryanet.com/, accessed April 30, 2013.

VIOLATIONS OF USER RIGHTS

While the country appears on a trend toward greater restrictions of online content, prosecutions and extralegal attacks on web users have decreased in severity over the past year. Nonetheless, strict penalties for criminal defamation against public authorities remain a concern. Amendments to the press law, discussed in detail above, also restrict internet freedom through the mandatory registration of news websites and their staff.

In October 2011, responding to public discontent, constitutional amendments were introduced to strengthen checks and balances and ensure greater protections for human rights.[47] The measures resulted in the creation of a constitutional court (Article 58-61), an explicit prohibition on torture (Article 8), and the restriction of the State Security Court's jurisdiction to crimes of treason, espionage, and terrorism (Article 110).[48] The Constitutional Court's nine members were named by King Abdullah II in October 2012.[49] Earlier that year, the king issued two royal decrees completing the necessary processes for the Constitutional Court and the Political Parties Laws to be enacted. [50] Several amendments touched directly or indirectly on internet freedom. Specifically, terms such as "mass media" and "other means of communication," which likely encompass online media, were added to provisions that protect freedom of expression and concomitantly allow for its limitation during states of emergency (Article 15). With regard to the right to privacy, judicial approval was added as a precondition for censorship or confiscation of private communications (Article 18).[51]

Despite constitutional protections, several laws that hinder freedom of expression and access to information remain on the books. These include the 1959 Contempt of Court Law, the 1960 penal code, the 1971 Protection of State Secrets and Classified Documents Law, the 1992 Defense Law, the 1998 Jordan Press Association Law, and the 1999 Press and Publications Law. Despite the passage of an Access to Information Law in 2007, a number of restrictions remain on requesting socially- and religiously-sensitive content.[52] In September 2011, the lower house of parliament passed an amendment to the country's Anti-Corruption Law, which would have penalized the publication or dissemination of allegations of corruption without proof with fines ranging from

[47] Law Library of Congress (2012, December 3) Jordan: Constitutional Law Court Newly Established in Jordan. Accessed June 26, 2013. http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403416_text

[48] Ali al-Rawashdah, "Jordan approves constitutional amendments," Al-Shorfa, October 5, 2011, http://al-shorfa.com/cocoon/meii/xhtml/en_GB/features/meii/features/main/2011/10/05/feature-01.

[49] Daily Star (2012, October 7) Jordan's King Abdulla Sets up a Constitutional Court. Accessed June 26, 2013. http://www.dailystar.com.lb/News/Middle-East/2012/Oct-07/190450-jordans-king-abdullah-sets-up-constitutional-court.ashx#axzz2XGFGrzWz

[50] King Abdulla II website (2013, June 6) Jordan Enacts New Political Parties, Constitutional Court Laws. accessed June 26, 2013. http://www.kingabdullah.jo/index.php/en_US/news/view/id/10139/videoDisplay/1.html.

[51] Constitution of Jordan, 1952, http://www.mpil.de/shared/data/pdf/overview_amendments.pdf; "Jordan," Max Planck Institute for Comparative Public Law and International Law, last updated May 4, 2012, http://www.mpil.de/ww/en/pub/research/details/know_transfer/constitutional_reform_in_arab_/jordanien.cfm.

[52] For example, the law bars public requests for information involving religious, racial, ethnic, or gender discrimination (Article 10), and allows officials to withhold all types of classified information, a very broad category (Article 13) Arab Archives Institute, "Summary of the Study on Access to Information Law in Jordan," June 2005, http://www.alarcheef.com/reports/englishFiles/accessToInformation.pdf.

JOD 30,000 to JOD 60,000 ($42,000 to $84,000).[53] However, in January 2012, the upper house of parliament rejected the controversial article following advocacy efforts by civil society groups and threats by the board of the Jordan Press Association to resign.[54]

The 2010 cybercrime law proscribes penalties for hacking and online identity theft, though it also contains several provisions that could be easily used to suppress online expression. For example, the new law prohibits posting any information concerning national security, foreign affairs, the national economy, and public safety that is not already available to the general public. Nevertheless, following protests by civil society, several more egregious provisions related to defamation and warrantless police searches were removed by royal decree in September 2010, one month after the law was passed.[55]

Defamation remains a criminal offense under the penal code. Amendments to the press law enacted in 2010 abolished prison sentences for libeling private citizens. However, the same bill increased fines and jail sentences for defaming government officials to up to JOD 10,000 ($14,000) and three to twelve months imprisonment.[56] On April 25, 2013, Mohammad Asha al-Dawaymeh, a parliamentarian from the Islamist Centrist Party, filed a suit against the website *Ammon News* for publishing news about a visit to Israel he made earlier this year.[57] He was later expelled from his political party over the visit, during which he reportedly attended a reception with Israeli President Shimon Peres to celebrate Israel's Independence Day.[58]

For the most part, Jordanian authorities have not made use of these laws to severely punish domestic political opponents, though some online commentators have faced legal harassment.[59] In the past, several online journalists were brought before the military-dominated State Security Court (SSC) on charges related to their writings. In July 2011, Jordanian journalist Alaa' Fazzaa' was arrested for "working to change the constitution by unlawful means" after he reported about a Facebook group supporting reinstatement of Prince Hamza, King Abdullah's half-brother, as crown

[53] Yahya Shakir, "Article 23 of the Anti-Corruption Law aimed at burying the opposing views in the bud" [in Arabic], Alarabalyawm, http://alarabalyawm.batelco.jo/pages.php?articles_id=17077;
[54] "Jordan journalists protest anti-corruption bill," Khaleej Times, September 28, 2011, http://www.khaleejtimes.com/darticlen.asp?xfile=data/middleeast/2011/September/middleeast_September568.xml&section=middleeast; Wael Jaraysheh, "Senate Returns Controversial Anti-Corruption Law, Dodging Deliberations Again," Ammon News, December 8, 2011, http://en.ammonnews.net/article.aspx?articleNO=14876; "Jordanian Senate Rejects Article 23 of the Anti-Corruption Law," SKeyes News, January 16, 2012, http://www.skeyesmedia.org/en/News/Jordan/Jordanian-Senate-Rejects-Article-23-of-the-Anti-Corruption-Law.
[55] International Freedom of Expression Exchange (IFEX), "Government yields to protests, modifies cyber crimes law," news release, September 3, 2010, http://ifex.org/jordan/2010/09/03/cyber_crimes_law/; Official Website of the Prime Ministry of the Hashemite Kingdom of Jordan [in Arabic], http://www.pm.gov.jo/arabic/index.php?page_type=gov_paper&part=3&id=5056.
[56] IREX, "Introduction to News Media Law and Policy in Jordan," May 2011, pg 38, http://www.irex.org/sites/default/files/Media%20Law%20and%20Policy%20Primer%20(English).pdf.
[57] Saraha News (2013, April 26) After heis secret was revealed by Ammon News AlAsha goes to defame the website. accessed June 26, 2013 http://www.sarahanews.com/?p=33472
[58] "Jordanian MP expelled for Israel visit," UPI, April 22, 2013, http://www.upi.com/Top_News/World-News/2013/04/22/Jordanian-MP-expelled-for-Israel-visit/UPI-45941366623316/.
[59] Oula Farawati, "Jordan's News Websites Running for Legal Cover," Menassat, March 11, 2009, http://www.menassat.com/?q=ar/comment/reply/6143.

prince.[60] He was released several days later. That same year, Fazzaa' also faced prosecution for an article he authored on the news website *Khabarjo* in which he accused senior officials of inappropriately allowing convicted business tycoon Khalid Shahin to leave the country.[61] The charges against Fazzaa' were later dropped as part of a general amnesty.[62]

Jordanians are careful when talking on mobile phones or at public meetings. This attitude has passed naturally to the internet, where it is believed that security services closely monitor online comments, cataloging them by date, internet-protocol (IP) address, and location. In a 2010 case that strengthened these suspicions, Jordanian college student Imad al-Ash was sentenced to two years in prison after security forces accused him of insulting the king in an instant message to a friend and posting "controversial religious opinions" in public online forums.[63] He was subsequently released after a royal pardon.

Cybercafes, where users might otherwise write with relative anonymity, have been subjected to a growing set of regulations in recent years. Since mid-2010, operators have been obliged to install security cameras to monitor customers, who in turn must supply personal identification information before they use the internet. Cafe owners are required to retain the browsing history of users for at least six months.[64] Authorities claim these restrictions are needed for security reasons. Although enforcement is somewhat lax, the once thriving cybercafe business is now in decline due in part to the restrictions, as well as increased access to personal internet connections.

Over the past year, incidents of physical harassment and cyberattacks against bloggers and staff of online news websites have continued, though they have decreased in severity since last year. Jordanian policemen targeted journalists with teargas during protests in Amman in November 2012.[65] Unknown perpetrators raided the offices of the online news site *Watan* on July 17, 2012, stealing documents and damaging equipment.[66] The webpage of the news sites *Khaberni* and *Al Ain* were hacked in March and October 2012 respectively, while the site of the Jordanian rap group *Ahat* was also hacked on September 15, 2012.[67]

---

[60] James M. Dorsey, "Assad Criticism Isolates Iran, Fails to Tackle Key Issues," MidEast Posts, September 8, 2011, http://mideastposts.com/2011/08/09/assad-criticism-isolates-iran-fails-to-address-key-issues/.
[61] AFP, "Jordan frees journalist held for 'undermining throne," Google News, http://www.google.com/hostednews/afp/article/ALeqM5gqpn0B98i6cWhwxx2TJvrRGILmFg?docId=CNG.7e8c9b730d578a188e3f19c677e0e598.131.
[62] James M. Dorsey, "Assad Criticism Isolates Iran, Fails to Tackle Key Issues," MidEast Posts, September 8, 2011, http://mideastposts.com/2011/08/09/assad-criticism-isolates-iran-fails-to-address-key-issues/.
[63] Ahmad Al-Shagra, "Jordanian Student Sentenced to 2 Years Over IM," The Next Web, July 19, 2010, http://thenextweb.com/me/2010/07/19/royal-ash-jordanian-student-sentenced-to-jail-for-2-years-over-im/.
[64] International Freedom of Expression Exchange (IFEX), "Cyber crime law attacks free expression; Internet cafés monitored," News Release, August 18, 2010, http://www.ifex.org/jordan/2010/08/18/cyber_cafe/; "Interior requires internet cafes to install surveillance cameras and keep internet visits for months" [in Arabic], Saraya News, June 3, 2010, http://www.sarayanews.com/object-article/view/id/23211.
[65] Talhouk (2012).
[66] "Report: increasing attacks on journalists in Jordan, mostly from the security," [translated] Satel News, July 8, 2012, see http://bit.ly/15WAUGB.
[67] "Press and Cultural Freedom in Lebanon, Syria, Jordan and Palestine – Annual Report 2012," SKeyes Center for Media and Cultural Freedom, 2013, http://foundationforfuture.org/en/Portals/0/Grantees%20Publications/SKeyes%202012%20Annual%20Report%20EN.pdf.

KAZAKHSTAN

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	15	15
Limits on Content (0-35)	23	23
Violations of User Rights (0-40)	20	21
Total (0-100)	**58**	**59**

* 0=most free, 100=least free

POPULATION: 16.8 million
INTERNET PENETRATION 2012: 53 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- In December 2012, a court order banned four of the main opposition media outlets and any websites that reproduced their content (see **LIMITS ON CONTENT**).
- The effective use of online tools to mobilize support for political and social campaigns in response to government policies continued to grow (see **LIMITS ON CONTENT**).
- The first case of libel charges being brought to court for material posted online occurred in January 2013 (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

For the past few years, Kazakhstan's government has been steadily declaring information and communication technologies (ICTs) a developmental priority. In 2012, however, the relevant state bodies were comparatively quiet regarding this issue, partly because the most dynamic period of the "boom" is already over, and partly because of the authorities' heightened cautiousness regarding the potential "evils and virtues" that online opportunities bear in the autocratic society.

The Ministry of Transport and Communications continues its efforts to promote the introduction of more advanced ICTs and the improvement of e-government services. Other state entities have enhanced their websites, including the official website of the president of Kazakhstan, which was redesigned in the summer of 2012 to include official YouTube, Facebook, and Twitter accounts.[1] The national telecommunications operator, Kazakhtelecom, and its business rivals are fiercely competing for new subscribers to their internet services, modestly improving their access speeds and providing some additional services.

In February 2013, the minister of culture and information, Mukhtar Kul-Mukhammed, stated that future government procurement contracts in the media sphere would be redistributed to favor more web-based publications.[2] At approximately the same time, State Secretary Marat Tazhin, while criticizing the work of state-owned traditional media, expressed the need for a new information policy that would create a database of popular domestic and foreign analysts, bloggers, and moderators of social network communities.[3] It remains unclear if the official's demands were met or not, and the first posts about his comments were deleted from the news wires.

The authorities clearly fear the internet's democratizing potential and, in addition to the legally endorsed practice of blocking certain websites over the past few years, the authorities have passed additional terrorism-related legislation to acquire broader control over the media, a continuation of the previous year's national security amendments that solidified state control over information distributed via both traditional and online media. The trend stemmed from a number of bombings attributed to religious extremists in 2011[4] and a state of emergency declared after violent clashes between oil strikers and police in the town of Zhanaozen (western Kazakhstan) in December 2011.[5]

The most visible and worrying development in the sphere of stifling internet and media freedom is also related to the Zhanaozen events—particularly, the controversial trial of the riot's alleged

[1] Official Site of the President of the Republic of Kazakhstan, accessed July 2, 2013, http://www.akorda.kz/en/mainpage
[2] "Распределение государственного информационного заказа будет жестко привязано к рейтингу средств массовой информации" ["Distribution of state information procurement contracts will be strictly tied to the rating of media outlets"], Kazinform, February 25, 2013, http://inform.kz/rus/article/2537802.
[3] Makpal Mukankyzy, "Блогеры придумали словосочетание «список Тажина»" ["Bloggers invented the term - "Tazhin's list""], February 27, 2013, Azattyq.org, http://rus.azattyq.org/content/blogery-kritikuyut-initsiativu-marata-tazhina/24913675.html.
[4] Joanna Lillis, "Kazakhstan: Astana Jolted by Terror Incidents," EurasiaNet, November 16, 2011, http://www.eurasianet.org/node/64529.
[5] "Kazakh authorities censor news on deadly clashes," Committee to Protect Journalists, December 20, 2011, http://cpj.org/2011/12/kazakh-authorities-censor-news-on-deadly-clashes.php.

instigators[6] that included activists from the unregistered opposition party, and a court decision to ban the print and online media outlets associated with the opposition newspaper *Respublika*.[7] In another case, a major independent online publication, *Guljan.org*, faced a wave of civil and administrative suits, including charges resulting in huge moral damage claims, and was eventually banned by an obscure court decision following a prosecutor's demand.[8]

OBSTACLES TO ACCESS

Internet access has grown exponentially in Kazakhstan, increasing from a 4 percent penetration rate in 2007 to 53.3 percent in 2012, according to the International Telecommunication Union.[9] Official government statistics cite a penetration rate of nearly 60 percent as of May 2012,[10] although experts have consistently questioned these official statistics over the past few years, citing a lack of clarity in the methodology.[11] The independent think tank Profit Online argues that the penetration level could be up to 70 percent, if one counts the number of devices that connect to the internet in a one month period, due to the rapid surge in usage of affordable internet-enabled mobile gadgets. However, the number of "real users" would be much lower, around 50 percent (monthly internet users), while the core usage (users accessing internet at least several days a week) would be formed by a pool of 2.5 million Kazakhstanis (around 16 percent of the total population).[12]

Despite these discrepancies in statistics, the access trends clearly indicate a steady escalation in internet use. A growing number of people prefer to go online from home, alongside widening access at educational institutions, libraries, workplaces and public places (malls, restaurants, and so forth). Internet speeds offered by the state-run operator Kazakhtelecom and private internet service providers (ISPs) have increased at a slow but steady pace. Prices remain relatively high for the majority of the population, but both Kazakhtelecom and the Ministry of Transport and Communication continue working together to decrease connection and usage fees, including prices on wholesale web traffic for other ISPs, thus boosting competition on the market.[13]

---

[6] "Kazakhstan opposition leader jailed," BBC, October 8, 2012, http://www.bbc.co.uk/news/world-asia-19873237.
[7] "Almaty Court Backs Closure Of Opposition Newspaper, Websites", RFE/RL, December 25, 2012, http://www.rferl.org/content/almaty-court-backs-media-closures/24808018.html.
[8] "Court has made rule to suspend website www.guljan.org on three months by unknown reasons," Adil Soz, December 5, 2012, http://bit.ly/1bRAVyU.
[9] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, " 2006 & 2012, accessed July 7, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
[10] "Number of Kazakhstan's internet users grew," [In Russian] Meta.kz, May 4, 2012, http://meta.kz/other/708136-v-kazahstane-vyroslo-kolichestvo-polzovateley-interneta.html.
[11] "Недостаточно высокий уровень проникновения Интернета...," [Insufficient level of Internet penetration...] Zakon, May 8, 2010, http://www.zakon.kz/171765-nedostatochno-vysokijj-uroven.html.
[12] "Проникновение интернета в Казахстане достигло 70%" [Internet penetration rate in Kazakhstan reaches 70 percent], February 29, 2012, http://www.profit.kz/news/8307-Proniknovenie-interneta-v-Kazahstane-dostiglo-70-procentov/#.UQokXx002wR.
[13] "Price of internet access to be decreased from January 1," [In Russian] Forbes.kz, December 28, 2012, http://forbes.kz/process/technologies/tsenyi_na_dostup_v_internet_snizyat_s_1_yanvarya.

Unlimited broadband subscriptions currently cost $25 to $30 per month (basic tariffs offer 3Gb to 10Gb of traffic for a fee of $12 to $20), compared to the average monthly income of approximately $660 as of October 2012.[14] Internet packages for most fixed-line subscribers in Kazakhstan are broken into a two-tiered system: access to information hosted inside the country is unlimited, but for content hosted outside of the country, contracts usually have a quota on traffic. If the quota is exceeded, the connection speed slows down; normally no extra fee is charged.

Mobile phone penetration is significantly higher than internet usage, with a penetration rate of 159 percent in 2012 (an increase of 30 percent since 2010), with 40 percent of those subscribers accessing the internet from their phone.[15] Mobile telecom operators increasingly compete on the market of internet access both with each other and with other ISPs since the launch of 3G in late-2010. A growing number of people are accessing the internet on their mobile phones, tablet computers, or regular computers with USB modems. In January 2013, ALTEL, a Kazakhtelecom subsidiary, launched a 4G LTE network that is currently available in Astana and Almaty.[16]

Since 2009, WiMAX networks have also become available in Kazakhstan, mostly enjoying corporate clientele. The number of free Wi-Fi hotspots in public places has been growing, mostly in the larger cities, while internet cafes still enjoy a stable customer base, especially when they are part of a chain with computer gaming as a primary source of business. Following government instructions, Kazakhtelecom has set up public hotspots and terminals within government agencies for public access free of charge, but the stations only provide access to e-government services and websites.

Kazakhstan's ".kz" top-level domain was introduced in 1994. Currently there are more than 71,000 domains registered in the Kazakhstani segment of the internet, dubbed KazNet, but only about 25 percent of them are active,[17] and even fewer receive at least 100 visitors per day.[18] The government has initiated several programs to stimulate internet use, lower the digital divide, improve websites of state-owned and state-funded institutions, and expand e-government functions.[19]

Social-networking platforms and other Web 2.0 applications are increasingly popular in Kazakhstan. The government has invested substantial funding into creating local websites and online services, including a national social network, although this site failed to generate any worthwhile user basis. The most accessed online resources from Kazakhstan remain foreign ones, especially Russian-based social-networking sites like Mail.ru, Vkontakte.ru and Odnoklassniki.ru, multiservice portals like Google and Yandex, and YouTube. Facebook, Wikipedia, and Twitter are

[14] "Средние заработные платы" [Average Monthly Income], Mojazarplata.kz, accessed January 31, 2013, http://mojazarplata.kz/main/srednie-zarabotnye-platy.
[15] "Number of cellphone users in Kazakhstan grew by 30 percent," [In Russian] June 25, 2012, http://www.profit.kz/news/8692-Kolichestvo-abonentov-sotovoj-svyazi-v-Kazahstane-uvelichilos-na-30/#.UQoxZB002wQ.
[16] "Altel launches commercial use of 4G," [In Russian] Iport.kz, December 25, 2012, http://iport.kz/blog/kaznet/3256.html.
[17] Beknur Kissikov, "Не казахстанский Казнет" [Non-Kazakhstani KazNet], Vlast.kz, may 11, 2012, http://vlast.kz/?art=407
[18] Chulpan Gumarova, "Количество – не значит качество" [Quantity does not mean quality], Kapital newspaper, January 18, 2012, http://www.kapital.kz/gazeta/biznes/4293-2012-01-18-16-50-32.html.
[19] Программа по развитию информационных и коммуникационных технологий в Республике Казахстан на 2010 – 2014 годы, [Program on Development of Information and Communication Technologies in the Republic of Kazakhstan for 2010-2014], September 29, 2010, http://www.mtk.gov.kz/images/stories/contents/otr_prog_834_20072011.doc

also growing in popularity. The most visited Kazakh site (or site with a ".kz" domain) as of January 2013 was the automobile-related classified ads site Kolesa.kz, followed by the multifunctional portal Nur.Kz, which were ranked at 12th and 14th place, respectively, out of all sites accessed within the country.[20]

In December 2011, two days before the Zhanaozen riots, the parliament adopted amendments and addendums to the Law of National Security, which reserve the government's right to forcibly suspend communications services during counter-terrorist operations or the suppression of mass riots (Article 23.4).[21] The amendments came into force in January 2012. That same month, the president signed amendments and addendums in the legislation governing intellectual property rights that criminalizes the illegal use of copyrighted material (punishable by one year in prison) and the organized distribution of such material through a file-sharing hub (punishable by five years in prison).[22] Critics argue that the law's formulations are vague and its punishments harsh, leaving room for selective and arbitrary enforcement, including against civil society groups or opponents of the government. When they came into effect in January 2012, these amendments forced all major peer-to-peer file exchange services (torrent trackers) to shut down and re-register URLs outside of the ".kz" domain zone.[23]

The state owns 51 percent of Kazakhtelecom, the largest ISP, which holds a 70 percent share in the internet access market.[24] Another five operators are licensed to connect to the international internet, but they are required to channel at least part of their traffic through Kazakhtelecom's backbone network facilities infrastructure.[25] Over 100 other ISPs operate in Kazakhstan, but have to purchase traffic via the above-mentioned six main providers. Kazakhtelecom's dominance over market and data transfer routes creates conditions for systemic content filtering. In addition, the law requires all ISPs to implement blocking of specific web content if a court finds the content illegal.

As of April 2013, there were four mobile telephone providers in Kazakhstan, three of which use the GSM standard (GSM Kazakhstan, Beeline, and TELE2) and one that uses CDMA/4G (ALTEL). Currently, all GSM operators are owned privately, with large foreign participation in ownership. Kazakhtelecom holds 100 percent of the shares of ALTEL, the first mobile operator in Kazakhstan. It was established in 1994 as a joint venture with British partners and has repeatedly changed

[20] "Top Sites in Kazakhstan," Alexa, accessed January 31, 2013, http://www.alexa.com/topsites/countries/KZ.
[21] "Республики Казахстан О национальной безопасности Республики Казахстан" [The Law on National Security], Zakon.kz, July 10, 2012, http://online.zakon.kz/Document/?doc_id=31106860&mode=all.
[22] See full text of the law published by the Kazakhstanskaya Pravda newspaper's website on January 12, 2012, http://kazpravda.kz/_pdf/jan12/200112law.pdf, accessed January 24, 2012; Nate Schenkkan, "Kazakhstan: Could Copyright Crackdown Be Next Frontier in Curbing Dissent?" Eurasianet.org, February 14, 2012, http://www.eurasianet.org/node/64998.
[23] "В Казахстане закрылись три торрент-трекера" [Three torrent-trackers closed in Kazakhstan], February 1, 2012, http://www.today.kz/ru/news/science/2012-02-01/58802
[24] Kazakhstan Stock Exchange, http://www.kase.kz/ru/emitters/show/KZTK; Kazakhtelecom presentation, "Kazakhtelecom JSC – national operator of telecommunications in Kazakhstan," 2011, pg. 22, accessed on January 24, 2012, http://www.telecom.kz/download/Presentacia1.pdf.
[25] OpenNet Initiative, "Country Profile: Kazakhstan," *Access Controlled*, accessed September 23, 2010, http://www.access-controlled.net/wp-content/PDFs/part2/007_Kazakhstan.pdf.

ownership since then, but was fully taken over by the national telecom operator when they purchased a stake for the remaining 50 percent in 2006.

Several bodies regulate the ICT sector, with the main regulators being periodically reorganized. The most recent shift in January 2012 gave the responsibility for the technology infrastructure sector to the Ministry of Transport and Communications, while entrusting regulation of information-related issues to the Ministry of Culture and Information. Until that point, both functions were filled by the reorganized Ministry of Communications and Information, whose head became the minister for transport and communications and remained such as of January 2013.

The ".kz" top-level domain name is managed by a registry, the Kazakhstani Network Information Center (KazNIC), and the Kazakhstani Association of IT Companies. Both were created in 2004–2005 as formally nongovernmental organizations, but in practice, they are believed to be under close control of the authorities and have been known to make politicized decisions on registration and deregistration of the domain names.[26] The government demands that any website with a ".kz" country domain must physically host its servers within the territory of Kazakhstan. Such regulations were introduced in April 2005, but the authorities undertook steps to fully enforce the regulation only in September 2010. The move prompted several controversies, the most prominent of which took place in June 2011, when Google chose to redirect all of the traffic from its localized Google.kz page to Google.com rather than comply with the demand to move its servers in-country, which it said would contribute to a "fractured internet" and ultimately harm Kazakhstani users.[27] Shortly after the dispute became public, the government retreated and the Kazakhstani Association of IT Companies explained that the rule applies only to domain names registered after September 7, 2010.[28]

LIMITS ON CONTENT

In the past, the Kazakhstani government's online censorship practices were mostly secretive, as well as selective, sporadic, and inconsistent. From 2009 through early 2013, however, these practices became more institutionalized, particularly through the enactment of legislation. In addition, filtering practices expanded from Kazakhtelecom to other ISPs, and the authorities sought to undermine the effectiveness of circumvention tools. The courts also started issuing decisions to block websites in a frequent and dense manner, banning dozens of websites at a time, mostly on the grounds of religious extremism.

The most recent country report on Kazakhstan by the OpenNet Initiative (ONI) in December 2010 stated that access was blocked to some "opposition…websites, regional media sites that carry

[26] OpenNet Initiative, "Country Profile: Kazakhstan."
[27] "Changes to the open Internet in Kazakhstan," Official Google Blog, June 7, 2011, http://googleblog.blogspot.com/2011/06/changes-to-open-internet-in-kazakhstan.html.
[28] "Google.kz вернулся в Казахстан" [Google.kz returrned to Kazkahstan], Tengrinews.kz, June 15, 2011, http://tengrinews.kz/internet/190571/.

political content…selected social networking sites, [and] a number of proxy sites."[29] Reporters Without Borders' monitoring results, published in 2012, indicated that a handful of websites deemed "extremist" were blocked despite the fact that much of the content found on these sites had nothing to do with terrorism or religious extremism.[30] International news sites such as the BBC, the *New York Times*, RFE/RL (including "Azattyq," its Kazakhstan subsidiary), and websites of international organizations such as Human Rights Watch and Freedom House are available.

Web 2.0 applications have been periodically blocked in Kazakhstan in recent years, though the government has not always admitted their intent behind the restrictions. The international blog-hosting platform LiveJournal was blocked for over two years from October 2008 to November 2010 by the two largest ISPs, the state-owned Kazakhtelecom, and Nursat.[31] The impetus for the block was ostensibly to restrict access to politically sensitive content related to President Nazarbayev's former son-in-law, Rakhat Aliyev.[32] The platform was unblocked after the disputed blog was frozen by LiveJournal administrators,[33] yet blocked again in August 2011, under claims that some accounts contained religious extremism.[34] A LiveJournal spokesperson stated that the company had never received any official notice from the Kazakhstan government identifying certain accounts as extremist and requesting their removal, an action the blog-hosting provider claimed it would take if the concerns were found to be legitimate.[35] The site remained inaccessible from Kazakhstan as of January 2013.

In February 2011, a district court in Astana banned two Wordpress-based blogs for disseminating content related to religious extremism, but this resulted in the blocking of the entire platform.[36] It is not fully clear when the access was restored; the disputed blogs are no longer available. Currently, Kazakhstani users can access Wordpress.com, but certain blogs hosted by it are inaccessible. Individual user pages on Blogspot.com could be accessed at the time of preparing this report.

---

[29] OpenNet Initiative, "Country Profile: Kazakhstan."
[30] "Kazakhstan country profile," Reporters Without Borders, March 12, 2012, http://en.rsf.org/kazakhstan-kazakhstan-12-03-2012,42073.html
[31] Karim Toktabayev, "1000 and 1 nights without LiveJournal" [in Russian], Profit.kz, October 9, 2012, http://www.profit.kz/articles/1856-1000-i-1-noch-bez-Zhivogo-Zhurnala/#.UZpwPMo1r31
[32] Rakhat Aliyev, Nazarbayev's former son-in-law, had served in top positions in the country's secret services and diplomatic service. He had large business and media holdings before definitively falling out of favor with the president and his family in 2008 after he had faced multiple charges of abduction, financial crimes and a coup attempt. Having fled abroad, Aliyev began airing inside information and allegations, in the traditional media and online, in an effort to discredit the president. Materials related to Aliyev have been systematically filtered, and republication of excerpts from his book "Godfather-in-law" is officially banned. Many observers believe that Nazarbayev's conflict with Aliyev was the primary reason for the first blockage of LiveJournal in Kazakhstan, and also accelerated adoption of the internet-related legal amendments in 2009.
[33] Adil Nurmakov, "Kazakhstan: Livejournal Unblocked After 2 Years of Filtering," Global Voices Online, November 17, 2010, http://globalvoicesonline.org/2010/11/17/kazakhstan-livejournal-unblocked-after-2-years-of-filtering/.
[34] "Kazakhstan blocks websites to battle religious extremism," Neweurasia.net, September 9, 2011, http://www.neweurasia.net/media-and-internet/kazakhstan-blocks-websites-to-battle-religious-extremism/.
[35] "LiveJournal portal, several blogs suspended," IFEX, September 2, 2012, http://www.ifex.org/kazakhstan/2011/09/02/livejournal_suspended/.
[36] Svetlana Glushkova, "Портал Вордпресс заблокировали из-за двух блогов" [Wordpress portal was closed because of two blogs], Azattyq.org, July 12, 2011, http://rus.azattyq.org/content/worldpress_kazakhtelecom_blocking_blog_/24262786.html.

On December 14, 2012, internet users complained about having trouble accessing Facebook from approximately 3:00 p.m. to 6:00 p.m. Reportedly, the problem was present with various ISPs, but even subscribers of the same provider reported having unequal access to the site. Kazakhtelecom and Beeline denied any involvement.[37] Coincidentally, though, Mukhtar Ablyazov, a former owner of a major bank and sponsor of a number of opposition organizations and media outlets, and who is currently being prosecuted internationally for gross financial fraud, had announced earlier that he would hold an online "Q&A session" on Facebook at exactly 3:00 p.m. that day.[38]

In 2011–2012 Kazakhtelecom users had persistently reported difficulties in accessing some of Google's services, including the ability to download attachments sent in Gmail, the Picasa image bank, Google Translate's URL translation function, and others.[39] The cause of the problem was unclear and was never specifically explained by Kazakhtelecom officials, although the problem ceased to exist in September 2012, reportedly after Google started using local servers to cache webpages and thus enhance its search services.[40] In the spring of 2012, users periodically reported the inaccessibility of several web-based live video broadcasting sites, particularly Ustream.tv and Bambuser.com.[41] The latter site remained blocked as of January 2013.

A package of legislative amendments adopted in July 2009, which received significant domestic and international criticism, granted the state broad authority to block access to foreign online resources whose content is deemed to run counter to national laws. The amendments declared that the internet and all websites—referred to as "internet resources"—were to be considered media outlets, without differentiating between news sites, blogs, chat rooms, and so forth. The amendments also granted the state the power to suspend or shut down websites hosted within Kazakhstan, including any website with content deemed harmful to the interests of the public and the state. Foreign websites can be shut down by a court decision made in absentia of the website representative and does not require further notification—to the public or the website owner—about why the website is blocked.

Under these amendments, all ISPs are required to ensure blockage of banned websites, and the owners of "internet resources" are responsible for any content, posted either by themselves or other users, that is deemed illegal under Kazakhstan's civil, criminal, or administrative laws.[42] The law stipulates that filtering of websites could be applied only with a court decision, though this requirement is not always observed in practice. The amendments have resulted in tighter

[37] "Казахстанцы не могли зайти на Facebook" [Kazakhstans couldn't access Facebook], December 14, 2012, http://tengrinews.kz/internet/kazahstantsyi-ne-mogli-zayti-na-Facebook-225220/
[38] See Facebook post https://www.facebook.com/mukhtar.ablyazov/posts/217723715028863
[39] See Google Help forum thread (in Russian) at https://groups.google.com/a/googleproductforums.com/forum/#!category-topic/gmail-ru/?????-???????/dJV0yhvaG08, accessed January 31, 2013.
[40] "Разблокировка сервисов Google (обновление)" [Unblocking the Google services (update)], September 2, 2012, http://www.fateyev.com/ru/blog/2012/google_services_unlock_update
[41] "Kazakhstan - Another regime blocks Bambuser", April 19, 2012, http://blog.bambuser.com/2012/04/kazakhstan-another-regime-blocks.html
[42] "Парламент принял закон, усиливающий контроль над интернет-ресурсами в Казахстане" [Parliament adopted law to increase control over internet resources in Kazakhstan], Zakon.kz, June 24, 2009, http://www.zakon.kz/141606-parlament-prinjal-zakon-usilivajushhijj.html.

censorship, ending the phenomenon whereby users could still access pages blocked by Kazakhtelecom via alternative operators.

For some time, the 2009 legal amendments stood unimplemented, but after a series of suicide bombings in 2011, several court decisions were issued ordering the blocking of websites for reasons of "religious extremism." In August 2011, a court decision blocked access to LiveJournal and 11 other websites based on claims that the websites or certain webpages were disseminating content with signs of religious extremism.[43] In 2011, access to 125 websites was blocked in Kazakhstan for carrying content related to religious extremism.[44] In November 2012, the National Security Committee stated that courts in Kazakhstan had banned access to nearly 950 websites in 2011–2012 for propaganda relating to terrorism, violence, and extremism, and over 150 more websites were undergoing court examinations.[45]

Despite these legal precedents, the filtering of websites without court decisions continues. In March 2010, the Computer Emergency Response Team (CERT) was established in Kazakhstan and operates as a governmental body under the Ministry of Communications. In contrast to many of its foreign counterparts, whose mandate is restricted to address only technical incidents, Kazakhstan's CERT also aspires to fight "destructive content" and "political extremism" by blacklisting and banning certain sites.[46] In March 2010, when probed about the transparency of their work, a CERT spokesperson said that the team's activities, including its criteria for blacklisting and the lists of blocked websites, is considered secret.[47]

According to Google's 2012 global report on government-initiated content removal requests, Kazakhstan made two requests in the first half of 2012 regarding the removal of 17 elements from Blogger.com and Youtube.com on the grounds that the material contained threats to national security, in one case, and unacceptable levels of violence in the other. In both cases the requests arrived from the law enforcement bodies without a court decision.[48]

One of the most notable cases of blocking over the past few years has been the restrictions placed on the main website of *Respublika*, an opposition weekly paper that, as both an online and print publication, faced repeated charges and pressures throughout the last decade. In 2012, after the trials over the alleged organizers of riots in Zhanaozen concluded with either a conviction or an admission of guilt, the media outlets close to the Alga Party (financed by the exiled oligarch,

[43] "Kazakhstan blocks websites to battle religious extremism," Neweurasia.net, September 9, 2011, http://www.neweurasia.net/media-and-internet/kazakhstan-blocks-websites-to-battle-religious-extremism/.
[44] "В Казахстане закрыли доступ к 125 сайтам" [Kazakhstan closed access to 125 websites], Tengrinews.kz. October 1, 2011, http://tengrinews.kz/kazakhstan_news/198106/.
[45] "КНБ Казахстана через МИД решает вопрос закрытия экстремистских сайтов" [Kazakshstan's NSC resolves the issue of extremist websites ban through the MFA], Tengrinews.kz, November 14, 2012, http://tengrinews.kz/kazakhstan_news/knb-kazahstana-cherez-mid-reshaet-vopros-zakryitiya-ekstremistskih-saytov-223419/
[46] "В Казахстане начались проверки "неправильных" сайтов" [Checks of 'undue' websites started in Kazkahstan], Nur.kz, March 1, 2010, http://news.nur.kz/144920.html.
[47] "Служба реагирования на компьютерные инциденты рассказала о своей работе" [Computer emergency response team told about its work], Zakon.kz, March 25, 2010, http://www.profit.kz/articles/001196/.
[48] Google Transparency Report: Kazakhstan. http://www.google.com/transparencyreport/removals/government/KZ/?metric=compliance&by=product

Mukhtar Ablyazov) were charged with deliberate fomentation of the riots and were shut down in an unprecedented move. In November 2012, the Almaty city prosecutor's office filed four suits, asking the court to ban *Respublika*, the newspaper *Vzglyad,* the satellite TV channel *K+*, and the *Stan TV* video news site (the latter two are entities registered in Russia and Kyrgyzstan, respectively).[49] Three of the suits included the request to ban both the publication and the "resources that duplicate it," meaning the outlet's websites and accounts in blogging or social networking sites.[50] The fourth suit targeted *Respublika*, and considered 8 print publications and 23 websites as the "single media outlet titled *Respublika*." Prosecutors alleged that the "analysis revealed presence of propaganda of violent overthrow of government and undermining of state security" in their content.[51] No journalist or editor was convicted, but the court forbade the editorial collectives to reunite in any new media outlet.

The court ordered the suspension of the distribution of the *Respublika* newspaper on the same day that the suit was filed.[52] According to a *Respublika* representative, the Almaty prosecutor's office also listed Google, Facebook, Twitter, and LiveJournal as defendants.[53] A spokesman from the office of the general prosecutor refuted this claim and stated that those sites were mentioned "only in relation to certain pages and blogs mirroring *Respublika* and *Vzglyad*," while the administrators of Facebook and other sites would be "requested to delete or block the appropriate pages, while access to Facebook itself would not be blocked."[54] By the end of 2012 the courts had finished considering the cases and ruled to fully satisfy the prosecutor's suits by banning the media outlets,[55] causing a tide of condemnation from international rights watchdogs, domestic journalists, and media defenders.

In addition, the online newspaper and investigatory whistleblower Guljan.org, which is sympathetic to the country's opposition, has repeatedly been charged with libel by state officials. In February 2012, the wife of Kazakhstan's financial police chief won a case seeking KZT 5 million ($33,300) in moral damages for alleged defamation. The court ruling threatened to jeopardize the website with bankruptcy, but by the end of the year the fine was repaid.[56] However, on December 4, 2012, the Bostandyk district court in Almaty considered the prosecutor's request to suspend Guljan.org and agreed to ban it for three months. The court hearing was conducted without the participation of the defendants or their representatives, and both the prosecutor's request and the judge's ruling did not

[49] "Main opposition media silenced in space of a month," Reporters Without Borders, December 28, 2012, http://en.rsf.org/kazakhstan-main-opposition-media-silenced-in-28-12-2012,43751.html
[50] "Прокуратора Алматы подала иски в суд в отношении ряда казахстанских и зарубежных СМИ" [Almaty Prosecutors Bring Charges against several Kazakhstani and foreign media], Gazeta.kz, November 21, 2012, gazeta.kz/art.asp?aid=373227
[51] "Прокуратура Алматы просит суд закрыть ряд оппозиционных СМИ" ["Prosecutors ask court to ban several opposition media outlets"], Tengrinews.kz, November 21, 2012, http://m.tengrinews.kz/ru/kazakhstan_news/223826
[52] "Суд в Алматы приостановил распространение газеты Республика" [Almaty court suspends distribution of Respublika newspaper], November 23, 2012, http://news.gazeta.kz/art.asp?aid=373369
[53] "Almaty prosecutors filed lawsuits against Google, Facebook and Twitter", November 23, 2012, http://en.tengrinews.kz/crime/Almaty-prosecutors-filed-lawsuits-against-Google-Facebook-and-Twitter-14715/
[54] "Kazakhstan General Prosecutor's office denies filing lawsuits against Google, Facebook and Twitter", November 23, 2012, http://en.tengrinews.kz/internet/Kazakhstan-General-Prosecutors-office-denies-filing-lawsuits-against-Google-14731/
[55] "«Республику» велено закрыть. Что дальше?" [Respublika is to be closed. What's next?], December 25, 2012, http://rus.azattyq.org/content/respublika-oppositional-press-trial-verdict/24808192.html
[56] Interview with Mr. Ayan Sharipbayev, journalist of the Guljan.org website, Almaty, January 2013.

specify the grounds for the suspension.[57] Moreover, the court that considered the case did not have jurisdiction over it.

A second trial was held in the proper court, the Medeu district court of Almaty, and upheld the ban, adding that any URL containing the term "Guljan" (the first name of the site's editor-in-chief, Guljan Yergaliyeva) should be subject to immediate blocking, thus outlawing the mirror site "guljan.info" that the editorial staff had hastily registered by then. The second court hearing clarified that the formal reason for the shutdown was the website's participation in a campaign to encourage citizens to participate in an unsanctioned rally in January 2012.[58] No legal action or investigation was known by the journalists or public to be held against Guljan.org during the ten months between when the alleged offence was committed and the court ruling. The journalists' team launched a new site, Nuradam.kz, in February 2013, which fell victim to distributed denial-of-service (DDoS) attacks on several occasions. Its domain name was subsequently closed on charges that the website was based on foreign servers, which is a violation of domestic regulations; however, the content continues to be available through the use of mirror websites.

Since early 2009, there has also been an increase in self-censorship and content removal implemented by companies hosting online information.[59] With the 2009 internet-related amendments coming into force, most online content providers intensified their moderating practices in order to censor content that could expose them to legal repercussions. The self-censorship environment was further solidified following the July 2010 adoption of a law granting President Nazarbayev the status of "Leader of the Nation," which essentially places any criticism of him and his family under the umbrella of threats to national security or reputation. In 2012, the owners of independent political websites have reportedly received "friendly warnings," urging them to remove sensitive (usually, president-related) material. These warnings came from their hosting providers, who, in their turn, were approached by the special services.

From 2012–2013, no new methods were used by the government or non-state actors to proactively manipulate the content and online news landscape, although the presence of government-paid commentators continued to be observed during this period.

The 2008 blocking of LiveJournal, at the time the most popular blogging platform in Kazakhstan, combined with unstable access to Wordpress and Blogspot, have generated significant changes to the country's blogosphere.[60] At that time, there were no major local blogging sites. Since then, Yvision.kz has become the most popular Kazakhstan-based blog-hosting platform, with over 80,000

[57] "Гульжан Ергалиева: Я еще не знаю, в чем меня обвиняют" [Guljan Yergaliyeva: I don't know what are the charges they bring against me], December 5, 2012, http://forbes.kz/massmedia/guljan_ergalieva_ya_esche_ne_znayu_v_chem_menya_obvinyayut

[58] "Суд приостановил guljan.org из-за январских призывов к митингам" ["Court suspended guljan.org for the January 2012 calls for participation in an unsanctioned rally"], KazTAG report republished by Headline.kz news aggregator http://news.headline.kz/chto_v_strane/sud_priostanovil_guljanorg_iz-za_yanvarskih_prizyivov_k_mitingam.html

[59] Carl Schreck, "Kazakhstan Puts Pressure on Bloggers," The National, August 25, 2009, http://www.thenational.ae/apps/pbcs.dll/article?AID=/20090825/FOREIGN/708249847/1140.

[60] SUP Media, "LiveJournal in Figures. Autumn 2007," presentation, November 30, 2007, http://www.sup.com/stat_autumn07.pdf.

users as of January 2013, most of them blogging in Russian. A number of other blogging projects (both mass market and niche) are emerging, testing new formats of user-generated content (UGC) and services in commercial and non-commercial fields. Many users have migrated to Twitter and Facebook, which appear to be popular choices for new users as well.

The Kazakhstani blogosphere is dominated by the younger generation, but recent years have shown broader engagement on the part of professionals, journalists, academics, members of parliament, and other public figures, particularly on social networks. In 2012, as political activists continued to vigorously use social media to spread their message, the authorities kept recruiting popular, yet relatively loyal, bloggers to engage in "special coverage" propaganda campaigns, inviting them on "blogger tours," starting with the visit to oilfields and the Cosmodrome space launch facility, but then recruiting bloggers to report from the trials that followed the clashes in Zhanaozen.[61] Their coverage was heavily in line with the prosecutor's position. Both the government and bloggers deny having any financial ties to one another.

In an effort to demonstrate a willingness to engage with citizens online, officials and government institutions continue setting up and maintaining blogs on popular social-networking platforms. The website of every government body and local administration is required to have a blog. In November 2012, Bolat Kalyanbekov, the chairman of the Committee for Information and Archives at the Ministry of Culture and Information, recommended that all government press secretaries have their own Twitter accounts "to regularly monitor and participate in discussions, and resolve issues right where they occur."[62] In another instance, the deputy chief of the Presidential Administration, the country's main policy-making body, acknowledged that his staff is keeping an eye on online debates.[63]

Several grassroots campaigns have been actively employing social media to reach out to potential supporters and to coordinate activities. The most notable examples include the environmentalist group "Protect Kok-Zhailyau!," which opposes plans of large-scale construction on the territory of a nature reserve near Almaty, and BlogBasta.kz, a non-partisan initiative that supports the political mobilization of creative urban youth. Additionally, a movement to oppose budget cuts to maternity benefits and an increase in the retirement age, which also used Facebook to organize supporters, was able to develop suggestions to improve legislation and was invited by the government to deliver their report to members of parliament. These cases have shown serious self-organizing potential that was not previously present in the online sphere in Kazakhstan.

[61] "Усилились постжанаозенские баталии блогеров" ["Post-Zhanaozen battles between bloggers have intensified"], Azattyq.org, August 20, 2012, http://rus.azattyq.org/content/twitter-bloggers-battle-about-zhanaozen-trial/24680408.html
[62] "МКИ Казахстана рекомендует пресс-секретарям госорганов «переехать» в Твиттер" [MCI of Kazakhstan suggests press secretaries of state bodies "moving" to Twitter], November 23, 2012, http://www.inform.kz/rus/article/2512711
[63] "Замглавы Администрации Президента прокомментировал критику алматинцев в адрес Есимова" [Deputy chief of presidential administration commented upon the critic of Almaty residents towards Yesimov], December 21, 2012, http://tengrinews.kz/kazakhstan_news/zamglavyi-administratsii-prezidenta-prokommentiroval-kritiku-almatintsev-adres-225559/

VIOLATIONS OF USER RIGHTS

The government of Kazakhstan continued to use legal and extralegal mechanisms to control the activities of internet users in 2012–2013. Restrictions on the use of anonymizing tools remain in place, and in March 2012 the Tor Project found evidence that deep packet inspection (DPI) was being used by at least one telecommunications service provider. Additionally, in 2013 two individuals were sentenced to one year "restraint of freedom" for posting an anonymous comment about corruption on the blog of a tax committee chairman.

The constitution of Kazakhstan guarantees freedom of the press, but the criminal code also provides special protection for state officials, members of parliament, and in particular, the president. In practice, the authorities use various legislative and administrative tactics to control the media and limit free expression. There are additional restrictions applied during elections and the coverage of court trials.

In 2010, the parliament passed a law granting President Nazarbayev the status of "Leader of the Nation," which attached criminal responsibility to any damage done to his image, including public insults or distortion of his private biographical facts, among other provisions. More broadly, defamation remains a criminal offense and Kazakhstani officials have a track record of using libel to punish critical reporting.

While no bloggers were legally prosecuted from late 2012 to early 2013, in April 2012, Lukpan Akhmedyarov, a journalist of the independent weekly *Uralskaya Nedelya*, was violently beaten near his home by unidentified attackers.[64] Akhmedyarov had repeatedly reported on high-level corruption in the western province of Uralsk, appeared in defamation cases before the court, co-organized political rallies, and ran a personal blog on the official website of his newspaper.[65] The case was investigated and, in December 2012, police arrested four suspects, declaring the crime cleared,[66] although there still has been no information about the instigators of the crime or their potential motives.[67]

In late January 2013, the media reported the first case in Kazakhstan of online libel to reach the courts. Two officers of the Almaty tax department published an anonymous post on the official blog of the chairman of the tax committee, claiming that their supervisor was implicated in crimes of corruption. The police inquired into the crime and six months later the offenders appeared in court after a series of investigatory activities that included internet protocol (IP) analysis, retrieval of video recordings from cameras installed inside the cybercafe from which the comments had been

[64] "Совершено покушение на Лукпана Ахмедьярова" [Attempt on Lukpan Akhmedyarov's life], April 20, 2012, http://rus.azattyq.org/content/lukpan_ahmediyarov_attacked_uralksaya_nedelya/24554128.html

[65] See the page of Lukpan Akhmedyarov's personal blog on the website of "Uralskaya Nedelya" (Uralsk Week) newspaper http://bit.ly/19Kts03.

[66] "Нападение на Лукпана Ахмедьярова раскрыто" [Attack on Lukpan Akhmedyarov cleared], December 28, 2012, http://newskaz.ru/society/20121228/4533449.html

[67] "За жизнь Лукпана Ахмедьярова исполнителям обещали $10 тыс" [$10,000 was promised to the attackers for life of Lukpan Akhmedyarov], January 8, 2013, http://www.zakon.kz/4534211-za-zhizn-lukpana-akhmedjarova.html

posted, and the cybercafe's server data regarding online activities from certain PCs. The defendants maintained their innocence; however, the court sentenced both to one year of restraint of freedom, which requires notifying the police prior to leaving one's place of residence, education, or work.[68]

Beginning in early 2011, anonymizing tools, including proxy websites and specific circumvention software, were increasingly being blocked in Kazakhstan, though no court decision had been issued against them. Many users wishing to circumvent censorship instead switched to browsers designed by the Opera Corporation,[69] whose traffic compression feature was initially meant to facilitate browsing with slow connections but also enables users to access blocked websites. On April 21, 2012, Kazakhstani users reported problems with Opera browsers, particularly the inability to access websites outside of the ".kz" country code zone.[70] The problem was resolved on the same day; however, no explanations were provided.[71] In March 2012, the Tor Project announced that the service provider KazTransCom JSC had started using deep packet inspection (DPI) to censor and monitor the internet, particularly SSL-based encryption protocols.[72] At approximately the same time, users were no longer able to download Tor software from Kazakhstan (at the time of the report's update in May 2013, however, the download was possible).

It is difficult to track or verify efforts by the National Security Committee (KNB) or other agencies to monitor internet and mobile phone communications. However, a series of regulations approved in 2004 and updated in 2009 oblige telecom operators (both ISPs and mobile phone providers) to retain records of users' online activities, including phone numbers, billing details, IP addresses, browsing history, protocols of data transmission, and other data, via the installation of special software and hardware when necessary.[73] Providers must store user data for two years and grant access to "operative-investigatory bodies" when sanctioned by a prosecutor.[74] Furthermore, SIM card registration is required for mobile phone users at the point of purchase under the civil code; however, the requirement is not tightly enforced, and SIM card vendors view the registration as optional.[75]

The new amendments to the law on countering terrorism, which were signed by the president on January 8, 2013 and became effective on January 18, 2013,[76] granted extra powers to the security

[68] "Клевета в Интернете" [Libel on the internet], January 29, 2013, http://www.nomad.su/?a=13-201301300007
[69] "Web browser that bypasses big brother a Kazakh hit," Reuters, April 13, 2010, http://www.reuters.com/article/2010/04/13/us-kazakhstan-internet-browser-idUSTRE63C37N20100413.
[70] "Казахстанские интернет-пользователи испытывают трудности с браузером Opera" [Kazakhstani users experience problems with Opera browser], April 21, 2012, http://tengrinews.kz/internet/kazahstanskie-internet-polzovateli-ispyityivayut-trudnosti-s-brauzerom-Opera-212610/
[71] See http://my.opera.com/community/forums/topic.dml?id=1369952
[72] "Updates on Kazakhstan Internet Censorship", March 2, 2012, http://bit.ly/yhkSVQ.
[73] Ksenia Bondal, "Следи за базаром - нас слушают" [Watch out, we are watched], *Respublika*, republished by Zakon.kz, November 5, 2009, http://www.zakon.kz/top_news/152528-objazyvaet-li-ais-i-knb-sotovykh.html.
[74] See, "Rules of rendering internet access services," adopted by the governmental decree #1718 on December 30, 2011, and the Law on operative-investigatory activities, dated September 15, 1994, http://www.minjust.kz/ru/node/10182.
[75] "Сотовая связь: абонент не определен и опасен" [Cellular: caller is uncertain and dangerous], Ipr.kz, June 21, 2011, http://www.ipr.kz/kipr/3/1/51#.T7t40tx1BLc.
[76] Law of the Republic of Kazakhstan on amendments and addenda into several legislative acts of the Republic of Kazakhstan regarding counteraction to terrorism [In Russian], January 8, 2013, http://online.zakon.kz/Document/?doc_id=31318154

bodies,[77] reiterated a vague term of "fomenting social discord," and obliged all mass media (thereby including online resources and citizen journalists) to "assist" the state bodies involved in counter terrorism. The exact mechanisms of assistance are not specified.

On December 30, 2011, the government issued a decree tightening surveillance in cybercafes. Under the decree, cybercafe owners are obliged to gather the personal information of customers and retain data about their online activities and browsing history. This information is to be retained for no less than six months and can be accessed by "operative-investigatory bodies."[78] The decree also banned the use of circumvention tools in cybercafes. Beginning in early 2012, parts of the decree came into force, including the requirement to install video surveillance equipment and filtering software.[79] As of early 2013, none of the cybercafes specifically reviewed for this report required an identification card or passport before granting access to internet. It is still unclear how these regulations might apply to public Wi-Fi access points.

The administrators of several opposition-related or independent news websites such as *Respublika,* Zonakz.net and Guljan.org have reported suffering sporadic DDoS cyberattacks since 2009.[80] Although many suspect that regime actors were behind the attacks, their origin has been neither independently confirmed nor investigated by the police or the Computer Emergency Response Team (CERT),[81] whose responsibility is to address such incidents.

[77] Alexandr Gribanov, "Закон особого назначения" ["Law of special task"], Vecherniy Almaty newspaper, January 31, 2013, http://www.vecher.kz/node/18716

[78] See, "Rules of rendering internet access services," adopted by the governmental decree #1718 on December 30, 2011, http://medialawca.org/old/document/-11242.

[79] "В интернет-клубы теперь будут пускать только с удостоверением личности" [Internet clubs will demand IDs], Zakon.kz, January 25, 2012, http://www.zakon.kz/kazakhstan/4469529-takie-pravila-okazanija-uslug-dostupa-k.html.

[80] "Интернет-СМИ «Фергана.Ру», Zona.kz и «Республика» были атакованы неизвестными хакерами почти одновременно" [Internet Media 'Fergana.ru,' Zona.kz and 'Respublika' Are Attacked by Unknown Hackers Almost Simultaneously], Fergana.ru, February 20, 2009, http://www.ferghana.ru/news.php?id=11348.

[81] Computer Emergency Response Team (CERT), accessed July 1, 2013, http://kz-cert.kz/en/

KENYA

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	10	9
Limits on Content (0-35)	7	7
Violations of User Rights (0-40)	12	12
Total (0-100)	29	28

* 0=most free, 100=least free

POPULATION: 43 million
INTERNET PENETRATION 2012: 32 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Kenya's first general election, under the new 2010 constitution was held on March 4, 2013, which saw citizens and politicians alike using ICTs to disseminate information and prevent electoral violence (see **LIMITS ON CONTENT**).
- Fearful of election-related unrest, the government blocked thousands of allegedly inflammatory text messages, mandated bulk texts be pre-screened, and hired a team to proactively monitor social media for inciting language (see **LIMITS ON CONTENT**).
- Service providers were required to install internet traffic monitoring equipment known as the Network Early Warning System (NEWS) by December 2012 to detect cyber threats, such as online hate speech (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Over the past decade, Kenya has made notable strides in the field of information and communication technologies (ICTs), spurred by the government's commitment to economic development and an engaged civil society. Among several success stories are the start of construction for the Konza Techno City, dubbed "Africa's Silicon Savannah," in January 2013,[1] the launch of the National ICT Master Plan 2017,[2] and an impressive rise in both internet and mobile usage. The large-scale adoption of the M-Pesa mobile money platform, both domestically and regionally, has made the country a global leader in mobile money transfer services.[3] Additionally, two SMS-based applications that have become internationally known–Ushahidi and Frontline SMS–are based in Nairobi and paving the way for the integration of mobile and internet content development.[4] Together with Nigeria and Morocco, Kenya has risen to become one of Africa's major tech hubs.

Kenya held its first general election on March 4, 2013 under the new 2010 constitution. As a result of the political violence that ensued after the last general election in 2007, there were many concerns that ICTs would be used to propagate hate speech in the lead-up to the polls. The electioneering period saw the spread of political propaganda and incendiary speech through social media,[5] leading to ramped up efforts to limit speech and content that could incite violence. In September 2012, for example, the Communications Commission of Kenya (CCK) issued guidelines which mandated the pre-screening and approval of bulk messages containing political content before transmission.[6]

While there were no known incidents of government filtering or interference with online content in the past year, the Blue Coat PacketShaper appliance—a device that can help control undesirable traffic by filtering application traffic by content category—was discovered in Kenya alongside 18 other countries around the world, including China, Bahrain, and Russia in January 2013, though it

---

[1] "Kenya Begins Construction of 'Silicon' City Konza," BBC News, January 23, 2013, http://www.bbc.co.uk/news/world-africa-21158928?print=true.

[2] Joseph McOluch (ed.), *Connected Kenya 2017, National ICT Master Plan* (Kenya: ICT Board, 2012), http://www.ict.go.ke/docs/MasterPlan2017.pdf.

[3] Wolfgang Fengler, "How Kenya Became a World Leader for Mobile Money," *Africa Can…End Poverty* (blog), World Bank, July 16, 2012, http://blogs.worldbank.org//africacan/how-kenya-became-a-world-leader-for-mobile-money.

[4] David Souter and Monica Kerretts-Makau, "Internet Governance in Kenya -- An Assessment for the Internet Society," ICT Development Associates Ltd, September 2012, 32, http://www.internetsociety.org/sites/default/files/ISOC%20study%20of%20IG%20in%20Kenya%20-%20D%20Souter%20%26%20M%20Kerretts-Makau%20-%20final.pdf.

[5] A report by the Kenya Human Rights commission pointed out that "Kenyans on Twitter and Facebook, ran amok with all manner of accusations and counter-accusations mainly laced on choice epithets betraying raw ethnic chauvinism or blind political party loyalty." See, "Report: Election Propaganda Widespread in Social Media," *African Seer,* March 28, 2013, http://www.africanseer.com/news/african-news/265133-report-election-propaganda-widespread-in-social-media.html.

[6] According to article 9.4, "Political Messages shall not contain inciting, threatening or discriminatory language that may or is intended to expose an individual or group of individuals to violence, hatred, hostility, discrimination or ridicule on the basis of ethnicity, tribe, race, colour, religion, gender, disability or otherwise." See: "Guidelines for the Prevention of Transmission of Undesirable Bulk Political Content/Messages via Electronic Communications Networks," CCK, September 2012, http://www.cck.go.ke/regulations/downloads/Guidelines_for_the_prevention_of_transmission_of_undesirable_bulk_political_content_via_sms.pdf.

is uncertain whether the device has been implemented. Meanwhile, over 300,000 text messages were reportedly blocked a day during the March 2013 elections for allegedly containing speech that had the potential to incite violence. Precautionary surveillance measures were also implemented to curb the spread of provocative and inflammatory speech, which involved a requirement announced by the CCK in March 2012 for service providers to install the internet traffic monitoring equipment known as the Network Early Warning System (NEWS) by December 2012, citing a rise in cyber threats.[7]

Citizen and civil society efforts to monitor electoral activities and outcomes through innovative ICT tools played an instrumental role during the elections period. The Uchaguzi crowd-sourcing platform, for example, monitored trends as they were reported in real-time by citizens via SMS, and highlighted instances of political violence and electoral malpractice.[8]

OBSTACLES TO ACCESS

The spread and use of ICTs is increasing in Kenya, in no small part due to the government's commitment to developing the country's ICT infrastructure as a tool for economic growth. According to the latest CCK data from the last quarter of 2012, the percentage of the population with access to the internet stood at over 41 percent, increasing from 28 percent in 2011, though the International Telecommunications Union (ITU) estimated a 2012 rate of 32 percent.[9] Meanwhile, Kenya's mobile data and internet subscriptions stood at 8.5 million as of December 2012, with an estimated 17.4 million users,[10] while 34 percent of the population accessed the internet via mobile phones.[11] Mobile phone subscribers stood at over 30 million,[12] with a 78 percent penetration rate (72 percent according to ITU data[13]), though many people have more than one subscription to take advantage of lower prices or expand their geographic coverage, putting the actual number of users much lower. Nevertheless, the growth in mobile subscribers can be attributed to the popularity of mobile handsets as a medium of communication and the increasing availability of value-added mobile services such as internet, entertainment, and mobile money transfer.

[7] Okutttah Mark, "CCK Sparks Row with Fresh Bid to Spy on Internet Users," *Business Daily Africa*, March 20, 2012, http://www.businessdailyafrica.com/Corporate-News/CCK-sparks-row-with-fresh-bid-to-spy-on-Internet-users-/-/539550/1370218/-/item/0/-/edcfmsz/-/index.html.

[8] Juliana Rotich, "Uchaguzi Overview Report for March 4, 2013," Uchaguzi, March 4, 2013, http://sitroom.uchaguzi.co.ke/2013/03/04/uchaguzi-overview-report-for-march-4-2013/.

[9] Communications Commission of Kenya, "Quarterly Sector Statistics Report, Second Quarter of the Financial Year 2012/13 (Oct-Dec 2012)," , 21, http://www.cck.go.ke/resc/downloads/Sector_statistics_for_Quarter_2_-_2012-2013.pdf; International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[10] "Kenya ICT Board launches Julisha ICT Survey report 2013," *Humanipo,* February 19, 2013, http://www.humanipo.com/news/4084/Kenya-ICT-Board-launches-Julisha-ICT-Survey-report-2013.

[11] Communications Commission of Kenya, "Mobile Penetration in the Country Continues to Increase," , January 21, 2013, http://www.cck.go.ke/mobile/news/index.html?nws=/news/2013/Mobile_penetration.html.

[12] Communications Commission of Kenya, "Mobile Penetration.

[13] International Telecommunication Union,"Mobile-cellular Telephone Subscriptions, 2000-2012."

Kenya is also said to have comparatively low-priced mobile service for Africa, with monthly costs averaging KES161 ($1.90) for 30 calls and 100 SMS test messages.[14] These relatively affordable costs are largely the result of strong regulatory interventions that have led to the implementation of the lowest mobile termination rates across the continent.[15] In November 2012, the CCK slashed the mobile termination rate from Sh2.21 to Sh1.44 per minute, which drove down prices for mobile phone users.[16] Nevertheless, the CCK also initiated a crackdown against the use and sale of counterfeit mobile devices in 2012, setting a deadline of September 30 for users to verify the authenticity of their handsets through a database of IMEI numbers created in collaboration with device manufacturers.[17] Millions of unverified handsets were deactivated from networks on October 1, 2012.[18]

Data bundles are now available for prepaid mobile customers, while mobile broadband subscriptions on GPRS/EDGE and 3G networks have continued to increase as well. By the last quarter of 2012, broadband subscriptions stood at over one million users, representing approximately 12 percent of total mobile internet subscriptions.[19] By contrast, the number of fixed broadband subscriptions numbered less than 43,000 at the end of 2012, for a penetration rate of 0.1 percent, according to ITU data.[20] The growth in mobile internet subscriptions can be attributed to competitive mobile internet tariffs, special offers and promotions, and the rising use of social media, particularly among the youth population.

While internet penetration continues to increase across the country, there is still a large disparity in access between rural and urban areas. A 2012 study by the Internet Society noted that internet use in Kenya is largely concentrated in Nairobi and that significant action is still needed to address issues of access outside of the capital.[21] Further, the cost of mobile devices and internet subscriptions remains a stumbling block for many impoverished Kenyans to access the web.[22] For example, the average user pays about $36 per month for 1-2 Mbps of unlimited data services and $37 for unlimited internet through a USB dongle (3G modem),[23] while the average monthly wage of an unskilled employee is about KES 4,258 ($53).[24]

---

[14] Frankline Sunday, "Lack of Expertise Slows Down ICT Growth," *Standard Digital*, December 22, 2012, http://www.standardmedia.co.ke/?articleID=2000073463&story_title=lack-of-expertise-slows-down-ict-growth.

[15] Mobile termination rates are a measure of the costs that mobile operators charge each other for terminating inter-network calls.

[16] Sunday, "Lack of Expertise Slows Down ICT Growth."

[17] The International Mobile Equipment Identifier (IMEI) of counterfeit phones is either duplicated in many other phones or does not conform to the recognized GSMA structure. IMEI is a 15-digit number that is unique to each mobile handset. See, Communications Commission of Kenya, "Counterfeit Mobile Phones," http://www.cck.go.ke/counterfeit-campaign/.

[18] Muthoki Mumo, "Booming Business for Shops as CCK Shuts Fake Phones," *Daily Nation*, October 1, 2012, http://www.nation.co.ke/business/news/Fake-phones-shut/-/1006/1522804/-/bbovmqz/-/index.html.

[19] Communications Commission of Kenya, "Quarterly Sector Statistics Report, Second Quarter of the Financial Year 2012/13 (Oct-Dec 2012).".

[20] International Telecommunication Union, "Fixed (Wired)-broadband Subscriptions, 2000-2012."

[21] David Souter and Monica Kerretts-Makau, "Internet Governance in Kenya -- An Assessment for the Internet Society," ICT Development Associates Ltd, September 2012, 28.

[22] "Costly Smart Devices and Internet Keep Users Away," *Daily Nation*, February 19, 2013, http://bit.ly/XrYk0o.

[23] Orange, "Orange Launches Unlimited Internet Bundles," press release, January 18, 2011, http://oran.ge/1bWXy5i.

[24] "Minimum Wage Rates in Kenya," *Wage Indicator*, as of June 2012, accessed June 22, 2013, http://www.wageindicator.org/main/minimum-wages/kenya.

Both the government and private sector are working to remedy the disparity between rural and urban access through the introduction of digital villages and *Pasha* ("Inform") Centers, which are small public access sites similar to cybercafes.[25] In November 2012, Kenya's ICT board announced that it had set aside 27 million Kenyan shillings to establish an additional 27 digital villages across the country by the end of the year,[26] adding to the 63 centers that have already been built since the initiative's launch in 2009. The board aims to establish centers in 290 constituencies in the long term.[27]

The Konza Techno City is another government initiative that aims to foster the growth of Kenya's ICT industry and place the country on the map as "Africa's Silicon Savannah." Designed to include a central business district, a university campus, urban parks, and housing for up to 185,000 people, the multi-billion dollar project hopes to create nearly 100,000 jobs in the ICT sector by 2030. Construction of the city began in January 2013 on a 5,000-acre plot located some 60 kilometers from Nairobi.[28]

Kenya has four submarine cables that cumulatively provide the country with a capacity of about 8.56 Tbps, and a fifth cable announced in November 2012 will soon double the country's capacity to around 15 Tbps.[29] These infrastructural developments have improved available bandwidth, but unreliable or slow connections in many areas of the country, power outages, and issues of cost remain obstacles to access. Nevertheless, there have been no reports of the government controlling the internet infrastructure to limit connectivity.

Through the country's open market-based licensing process instituted in 2008, competition is present in most segments of the telecommunications market, though Safaricom still dominates the market for mobile phone services with a 63 percent share of all mobile subscriptions.[30] Safaricom also has a dominant position in the ISP market, commanding a 69 percent share of internet subscriptions as of June 2012, though its dominance has decreased over the past year with Airtel, Orange, and Essar gaining market share.[31]

Under the 2009 Communications Amendment Act, the CCK is responsible for regulating both broadcast and online media. Its independence is formally enshrined in the 1998 Kenya Communications Act, and the body has endeavored to work independently even though most of the commissioners remain government appointees and the appointment process is not sufficiently open

[25] "Kenya Investing Ksh 16.3 Billion in Rural ICT," *Information Policy* (blog), July 30, 2009, http://www.ictworks.org/2009/07/29/kenyan-government-investing-ksh163-billion-rural-ict/.
[26] Frederick Obura, "ICT Board to Release Funds for Digital Villages," *Standard Online*, November 1, 2012, http://www.standardmedia.co.ke/?articleID=2000069710&story_title=Kenya-ICT-Board-to-release-funds-for-digital-villages.
[27] Obura, "ICT Board to Release Funds for Digital Villages."
[28] "Kenya Begins Construction of 'Silicon' City Konza."
[29] Muthoki Mumo, "Internet Capacity to Double Soon After Fifth Fibre Optic Cable Lands," *Daily Nation*, November 19, 2012, http://www.nation.co.ke/business/news/Fifth-fibre-optic-cable-lands/-/1006/1624478/-/item/0/-/1uv0vy/-/index.html.
[30] Communications Commission of Kenya, "Quarterly Sector Statistics Report, First Quarter of the Financial Year 2012/13," 15, http://www.cck.go.ke/resc/downloads/SECTOR_STATISTICS_REPORT_Q1_12-13.pdf.
[31] Souter, "Internet Governance in Kenya ,",13.

and transparent.[32] In February 2013, however, the government for the first time publicly advertised the consumer representative position of the CCK board in accordance with Kenya's new 2010 constitution,[33] which states that board positions must be filled competitively.

The proposed Independent Communications Commission of Kenya Bill, 2010 further seeks to expand the independence of the country's ICT regulatory regime by replacing the CCK with the Independent Communications Commission of Kenya, which will be expected to function without any political or commercial interference.[34] Under the new body, all board positions will be publicly advertised, and the four government officials who currently sit on the CCK board will be removed and replaced by seven commissioners appointed by the president,[35] but only on the recommendation of the Public Service Commission.[36] It is expected that the proposed bill will be implemented in 2013 in accordance with the fifth schedule of Kenya's 2010 constitution,[37] which provides for media legislation to be enacted within three years of promulgation.[38]

Meanwhile, service providers have formed organizations such as the Kenyan ISP Association, the Telecommunications Service Providers of Kenya, and the Kenya Cybercafe Owners to lobby the government for better regulations, lower costs, and increased efforts to improve computer literacy.

LIMITS ON CONTENT

The elections period in March 2013 saw the widespread use of ICTs, social media tools, and innovative crowd-sourcing platforms by citizens and politicians alike to disseminate information. Nevertheless, concerns over potential electoral unrest led the government to take various preemptive actions to curb the spread of hate speech via ICTs, mandating the pre-screening and approval of bulk text messages, blocking thousands of other allegedly inflammatory SMS messages, and hiring a team to proactively monitor social media sites for inciting language.

Up until 2013, there were no reports of the Kenyan government employing any form of technical filtering or administrative censorship to restrict access to political or other content. However, in

[32] Open Society Foundations, "Public Broadcasting in Africa Series: Kenya," 2011, 65, http://www.afrimap.org/english/images/report/MAIN%20report%20final%20web%20res.pdf.
[33] Communications Commission of Kenya, "Govt Advertises Consumers Representative Seat on CCK Board," press release, February 14, 2013, http://www.cofek.co.ke/index.php?option=com_content&view=article&id=1362%3Agovt-advertises-consumers-representative-seat-on-cck-board&catid=1%3Alatest-news.
[34] "Independent Communications Commission of Kenya Bill 2010," available at Kenya Correspondents Association, http://www.kca.or.ke/attachments/article/125/INDEPENDENT%20COMMUNICATIONS%20COMMISSION%20OF%20KENYA%20BILL-CN1.pdf.
[35] Article 5 (1), "Independent Communications Commission of Kenya Bill 2010.
[36] This is the body that appoints persons to hold or act in public offices. See, "Public Service Commission of Kenya," Mandate, http://www.publicservice.go.ke/index.php?option=com_content&view=article&id=20&Itemid=61.
[37] "The Constitution of Kenya, Revised Edition 2010," 178, available at Embassy of the Republic of Kenya, http://www.kenyaembassy.com/pdfs/The%20Constitution%20of%20Kenya.pdf.
[38] Article 34 (5) of Kenya's constitution states that Parliament shall enact legislation that provides for the establishment of a body, which shall be independent of control by government, political interests or commercial interests, and set media standards and regulate and monitor compliance with those standards.

January 2013, the Citizen Lab internet research group discovered evidence of the Blue Coat PacketShaper appliance—a device that can help control undesirable traffic by filtering application traffic by content category—in Kenya alongside 18 other countries around the world, including China, Bahrain, and Russia.[39] No further reports or evidence have surfaced to reveal the extent to which the filtering device has been implemented, though its discovery in Kenya is noteworthy given the government's concern over the spread of hate speech and inflammatory content via ICTs in the lead-up to the March 2013 elections.

Intermediaries are responsible for filtering, removing and blocking content considered illegal, such as hate speech via text messages, though they are under no obligation to actively monitor traffic passing through their networks unless they are made aware of illegal content. Otherwise, Kenyans have unrestricted access to social-networking sites such as Facebook, Twitter, YouTube, and the blog-hosting site Blogger, all of which rank among the 10 most popular sites in the country.[40]

As a result of the political crisis that ensued after the 2007 general elections, the government ramped up its efforts to curb the spread of content that could trigger unrest or incite violence prior to March 2013. In September 2012, for example, the CCK issued "Guidelines for the Prevention of Transmission of Undesirable Bulk Content/Messages via Electronic Communications Networks,"[41] rules targeting licensed content service providers seeking to communicate messages to the electorate on behalf of politicians or political parties.[42] Under the guidelines, these providers must submit a request to a mobile network operator that includes the verbatim content of the message and a signed authorization letter from the sponsoring party for approval before a bulk political message can be transmitted.[43] The operator then screens and vets the proposed message for any inflammatory, provoking, or hateful language, and relays its decision within 18 hours. The guidelines also include a complaints handling process for aggrieved parties.[44]

Earlier in June 2012, Safaricom, the dominant mobile phone provider, issued its own guidelines for mobile advertising through its various media services to rein in negative political messages ahead of

[39] Morgan Marquis-Boire et al., "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools," Citizen Lab, Munk School of Global Affairs, University of Toronto, January 15, 2013, https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/#4.
[40] Alexa, "Top Sites in Kenya," http://www.alexa.com/topsites/countries/KE, accessed February 20, 2013.
[41] According to Aarticle 9.4 of the guidelines, "Political Messages shall not contain inciting, threatening or discriminatory language that may or is intended to expose an individual or group of individuals to violence, hatred, hostility, discrimination or ridicule on the basis of ethnicity, tribe, race, colour, religion, gender, disability or otherwise." See: Communications Commission of Kenya, "Guidelines for the Prevention of Transmission of Undesirable Bulk Political Content/Messages via Electronic Communications Networks," September 2012.
[42] "Short Message Service (SMS) & The Kenyan General Elections," *Africa Speaks 4 Africa* (blog), accessed June 22, 2013, http://www.africaspeaks4africa.org/?p=2550.
[43] CSPs are defined in Article 2.1.9 as "a person authorized by the Communications Commission of Kenya to provide content services." See: "Guidelines for the Prevention of Transmission of Undesirable Bulk Political Content/Messages via Electronic Communications Networks," CCK, September 2012; MNOs are defined in Article 2.1.10 as "a person authorized by the Communications Commission of Kenya to build and commercially operate Mobile Telecommunications/Electronic Communications Systems." See: "Guidelines for the Prevention of Transmission of Undesirable Bulk Political Content/Messages via Electronic Communications Networks," CCK, September 2012. "Bulk content" means content that is transmitted on a one-to-many configuration via SMS, MMS and any other similar medium that is capable of providing bulk messaging services.
[44] Article 9.2.

the March 2013 election.[45] Developed in consultation with the CCK and the electoral commission, Safaricom's guidelines indicated that it would suspend or terminate CSP contracts for noncompliance with its bulk message approval process, which is identical to the CCK's process outlined above.

During and after the March 4 elections, the authorities also asked mobile phone providers to block any text messages that could incite violence.[46] To do so, service providers installed a firewall that could detect messages containing particular words, such as "kill," which were automatically flagged for further scrutiny. According to the permanent secretary of the Ministry of Information and Communication, Dr. Bitange Ndemo, mobile phone service providers were blocking more than 300,000 text messages per day during the electioneering period to prevent electoral violence.[47]

Individual internet users are generally comfortable expressing themselves freely online and through mainstream media organizations. Nonetheless, during the March 2013 elections, news outlets admitted to practicing self-censorship as part of a "gentleman's agreement" made by media leaders to withhold from reporting on news that could incite ethnic tensions, according to Kenya's Media Owners Association.[48] The agreement to self-censor raised local debate on the balance between the national interest and the public's right to know.

There are no known state-run, government-influenced, or partisan online news/media outlets to date. Citizens are able to access a wide range of viewpoints, and the websites of the BBC, the CNN, and Kenya's *Daily Nation* newspaper are the most commonly accessed online news outlets.[49] While print outlets, television, and radio continue to be the main sources of news and information for most Kenyans, all major television stations have live-stream features and use YouTube to rebroadcast news clips. They also have accounts on Facebook and Twitter. Notably, there has been an increase in the number of blogs in recent years, with a wide range of topics covered from entertainment, fashion, and photography, to technology and business.[50] The Bloggers Association of Kenya was formed in 2011 to promote the domestic development of online content.[51]

---

[45] "Guidelines for Political Mobile Advertising Safaricom's Premium Rate Messaging Network," Safaricom, http://www.safaricom.co.ke/images/Downloads/Resources_Downloads/POLITICAL_MOBILE_ADVERTISING_NOTICE_FULL_PAGE_2b.pdf.

[46] "Short Message Service (SMS) & The Kenyan General Elections.".

[47] Fred Mukindia, "Phone Firms Block 300,000 Hate Texts Daily, says Ndemo," *Daily Nation*, March 21, 2013, http://www.nation.co.ke/News/Phone-firms-block-300-000-hate-texts-daily-says-Ndemo-/-/1056/1726172/-/ktkiafz/-/index.html.

[48] Jason Straziuso, "Kenya Media Self Censoring to Reduce Vote Tension," Associated Press, March 7, 2013, http://bigstory.ap.org/article/kenya-media-self-censoring-reduce-vote-tension.

[49] Victor Juma, "Mobile Internet on Course to Becoming Top Earner for Firms," *Business Daily Africa*, April 22, 2010, http://www.businessdailyafrica.com/Mobile-internet-on-course-to-becoming-top-earner-for-firms/-/539444/903924/-/5e9tqa/-/index.html.

[50] "The Kenyan Blog Awards 2013 Nominees," BAKE, March 27, 2013, http://bloggers.or.ke/the-kenyan-blog-awards-2013-nominees/.

[51] BAKE is a body that promotes content creation on the web in Kenya and represents a group of content creators who are of Kenyan origin, descent or are based in Kenya and want to syndicate their content, network among other fellow content creators, or get legal and communal representation from the Bloggers Association of Kenya.

Meanwhile, the internet continues to be an important platform for political debate and mobilization around critical issues. For example, in October 2012, hundreds of Kenyans took to Twitter to protest against members of parliament who had voted to award themselves with a substantial send-off bonus, using the hashtag, #KOTAgainstMPsBonus.[52] Their proposal was ultimately tabled, though this was not specifically due to the Twitter campaign, as there were many protests from different groups occurring simultaneously both on and offline.

Digital media has also revolutionized the ways in which human rights and civil society groups in Kenya network and share information.[53] In early 2013, for example, a partnership of civil society organizations launched Uchaguzi,[54] a crowd-sourcing platform designed to help Kenya achieve a free, fair, peaceful, and credible general election by empowering Kenyans with the ability to monitor the voting process and report on significant incidents in real time via SMS. During the election, the platform received over 3,000 messages from ordinary citizens around the country.

VIOLATIONS OF USER RIGHTS

As a result of concerns over increasing cybercrime and potential electoral unrest, service providers were required to install internet traffic monitoring equipment known as NEWS, the Network Early Warning System, by December 2012. Fourteen bloggers were reportedly targeted for posting hate speech during the March 2013 elections period, though no prosecutions were pursued.

Freedom of expression is enshrined in Article 33 of Kenya's constitution and includes the right to seek, receive or impart information and ideas, while Article 31 provides for the right to privacy. These rights, however, do not extend to propaganda, hate speech, incitement to violence, and advocacy of hatred. Criminal defamation laws remain on the books, waiting to be repealed or amended to conform to Kenya's 2010 Constitution. Meanwhile, existing laws that are inconsistent with it are considered unconstitutional.[55]

The 2012 Data Protection Bill is currently being considered in parliament and aims to regulate the collection, processing, storing, use, and disclosure of information relating to individuals that is processed through automated or manual means.[56] Meanwhile, the 2012 Freedom of Information Bill is undergoing stakeholder consultation as of mid-2013.[57] Both bills promise to enhance internet freedom in Kenya, illustrating the country's commitment to the development of its ICT sector and the use of ICTs to enhance public sector accountability.

---

[52] "#KOTAgainst Mps Bonus: Dozens Protest Against Kenyan MPs Vote for $110,000 Bonuses," *Blottr* (blog), October 9, 2012, http://www.blottr.com/breaking-news/kotagainstmpsbonus-dozens-protest-kenyan-mps-vote-110000-bonuses.
[53] Larry Diamond, *In the Spirit of Democracy* (New York: Henry Holt and Company LLC, 2009).
[54] Swahili for elections. https://uchaguzi.co.ke/.
[55] The Constitution of Kenya, Article 4.
[56] Commission for the Implementation of the Constitution "The Data Protection Bill, 2012,", accessed April 16, 2013, http://www.cickenya.org/index.php/legislation/item/174-the-data-protection-bill-2012#.UW10zaJ-bvE.
[57] Commission for the Implementation of the Constitution, "The Freedom of Information Bill, 2012," accessed April 16, 2013, http://www.cickenya.org/index.php/legislation/item/173-the-freedom-of-information-bill-2012#.UW178KJ-be.

Nevertheless, the government appears determined to crack down on cybercrime, which includes the spread of hate speech online,[58] though prosecutions for web activity have not appeared to be politically motivated. During the electioneering period in March 2013, 14 bloggers were reportedly targeted for posting hate speech online, six of whom were investigated.[59] The other eight were not summoned since they had used pseudonyms that made them difficult to identify. No prosecutions were ultimately pursued given a lack of sufficient evidence.[60]

Meanwhile, controversial blogger Robert Alai[61] was arrested in April 2013 for posting an allegedly "offensive tweet" that falsely accused a former gubernatorial candidate of domestic violence against his wife.[62] He was charged under Article 29(b) of the 2009 Kenya Information and Communications Act, which proscribes the transmission of a message that is known "to be false for the purpose of causing annoyance, inconvenience or needless anxiety to another person."[63] He was later acquitted on KES 50,000 ($560) cash bail,[64] though a guilty charge could have yielded a penalty of up to three years in prison and a fine up to 1 million Kenyan Shillings (over $11,500).

While surveillance of the internet and mobile phones was not previously a serious concern in Kenya, worries over increasing cybercrime and potential unrest surrounding the March elections led the government to implement precautionary surveillance measures to curb the spread of hate speech. In March 2012, the CCK announced that telecom service providers needed to install the internet traffic monitoring equipment NEWS, which would help establish early responses to detected cyber threats.[65] A KES32.2 million ($402,500) joint venture between the CCK and the ITU, the system reportedly works by assigning a unique internet protocol (IP) identity to individual gadgets, effectively making any communication traceable to its device of transmission. In their attempts to reassure consumers that the CCK would not proactively spy on internet users, officials noted that the system "does not have to read and disclose people's information" and "will only monitor traffic."[66] In September, service providers were given the deadline of December 2012 to comply with the installation requirement. Providers failing to comply would be cut off by

[58] Muna Wahome, "New Internet Version to Deepen Spying on Users," *Business Daily*, September 2, 2012, http://www.businessdailyafrica.com/New-internet-version-to-deepen-spying-on-users-/-/539546/1493584/-/fc2470z/-/index.html.
[59] Fred Mukinda, "14 bloggers Linked to Hate Messages," *Daily Nation*, March 28, 2013, http://www.nation.co.ke/News/14-bloggers-linked-to-hate-messages/-/1056/1732288/-/cut5kvz/-/index.html.
[60] "Hate Messages 'Still Rampant on Social Sites,'" *Daily Nation*, April 17, 2013, http://www.nation.co.ke/News/Hate-messages-still-rampant-on-social-sites/-/1056/1751340/-/56mc1h/-/index.html.
[61] "Twitter Goes Silent As Robert Alai Is Arrested," *Nairobi Wire*, August 22, 2012, http://www.nairobiwire.com/2012/08/twitter-goes-silent-as-robert-alai-is.html.
[62] "Robert Alai Arrested for Alleged 'Libelous' Twitter Post," *Jambo News Pot*, May 15, 2013, http://www.jambonewspot.com/robert-alai-arrested-for-alleged-libelous-twitter-post/; "Tech Blogger and Twitter Bigwig Robert Alai Arrested Again Over Annoying Tweets," *Vibe Weekly*, May 16, 2013, http://vibeweekly.com/new-vibe/1158-tech-blogger-and-twitter-bigwig-robert-alai-arrested-again-over-annoying-tweets.html.
[63] Communications Commission of Kenya, "The Kenya Information and Communications Act," 2009, http://www.cck.go.ke/regulations/downloads/Kenya-Information-Communications-Act-Final.pdf.
[64] Mukinda, "14 Bloggers Linked to Hate Messages."
[65] Okutttah Mark, "CCK Sparks Row with Fresh Bid to Spy on Internet Users," *Business Daily Africa*, March 20, 2012, http://www.businessdailyafrica.com/Corporate-News/CCK-sparks-row-with-fresh-bid-to-spy-on-Internet-users-/-/539550/1370218/-/item/0/-/edcfmsz/-/index.html.
[66] Lilian Nduati, "We Will Not Spy on Kenyans Online, says Internet Watchdog," *Sunday Nation*, March 22, 2012, http://bit.ly/18Gcsb0.

international backbone operators.[67] As of May 2013, no further information is known about the extent to which service providers have complied with the installation requirement or how the system has been put into practice. Nevertheless, the interception of messages or the disclosure of their content remains a criminal offence.[68]

On February 4, 2013, the National Cohesion and Integration Commission unveiled a toll-free Safaricom number for the reporting of hate speech and announced that it had trained and deployed about 100 hate speech monitors across the country to keep abreast of statements made by politicians or their supporters that could inflame tensions.[69] The government also hired bloggers to monitor websites for inflammatory content, in addition to enlisting the help of the Umati Project—a civic initiative based at Nairobi's iHub research center—and Kenya's National Human Rights Commission to report on online hate speech.[70] Despite the increased monitoring, there were no reported instances of any flagged content being blocked or removed.

In June 2009, the government announced a new SIM card registration requirement in collaboration with service providers, which was followed by various public awareness campaigns aimed at informing consumers of the security imperative behind the new requirement. A final deadline of December 31, 2012 was set for the SIM card registration exercise,[71] after which point 2.4 million unregistered cards were disconnected, including those used in tablets and internet modems.[72] To ensure compliance with the new regulation, the government amended the Kenya Information and Communications Act (KICA) to place the onus on mobile providers to record and maintain an index of all subscribers.[73]

Otherwise, there were no reported cases of government abuse of online surveillance in the past year, nor are there any known requirements for ICT service providers to proactively monitor their users. In addition, netizens did not face any extralegal intimidation or violence, nor were there any politically motivated cases of technical violence against civil society or opposition websites.

---

[67] Muna Wahome, "New Internet Version to Deepen Spying on Users," *Business Daily*, September 2, 2012, http://www.businessdailyafrica.com/New-internet-version-to-deepen-spying-on-users-/-/539546/1493584/-/fc2470z/-/index.html.

[68] Alice Munyua, Grace Githaiga and Victor Kapiyo, "Intermediary Liability in Kenya," Association of Progressive Communications, October 2012, 11, http://www.apc.org/en/pubs/intermediary-liability-kenya.

[69] Roselyn Obala, "NCIC Hires 100 to Monitor Hate Speech," *Standard Online*, February 4, 2013, http://www.standardmedia.co.ke/?articleID=2000076656&story_title=ncic-hires-100-to-monitor-hate-speech.

[70] Drazen Jorgic, "Kenya tracks Facebook, Twitter for Election 'Hate Speech,'" Reuters, February 5, 2013, http://news.yahoo.com/kenya-tracks-facebook-twitter-election-hate-speech-122621161.html.

[71] Communications Commission of Kenya, "No Extension for Sim-registration," December 31, 2012, http://www.cck.go.ke/news/2012/Sim_card_registration_deadline.html.

[72] Communications Commission of Kenya, "More than 2.4m Unregistered Mobile Lines Disconnected," January 11, 2013, http://www.cck.go.ke/mobile/news/index.html?nws=/news/2013/Unregistered_lines.html.

[73] Communications Commission of Kenya, "The Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations, 2012," January 4, 2013, http://bit.ly/1blT2KP.

KYRGYZSTAN

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	13	12
Limits on Content (0-35)	10	10
Violations of User Rights (0-40)	12	13
Total (0-100)	**35**	**35**

* 0=most free, 100=least free

POPULATION: 5.7 million
INTERNET PENETRATION 2012: 22 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Illegally blocked news website *Ferghana News* was officially unblocked by the State Communication Agency in April 2013 (see **LIMITS ON CONTENT**).
- While instances of filtering controversial content continued, including the blocking of videos, there was also an increase in the successful use of online platforms to mobilize against potentially harmful legislation (see **LIMITS ON CONTENT**).
- A journalist was physically assaulted by a member of parliament after posting online comments in defense of another politician (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Shortly before the overthrow of President Kurmanbek Bakiev's regime in 2010, political pressure on the media—both traditional and online—intensified. The video portal Stan.tv was closed as punishment for covering opposition meetings,[1] the country's largest online portal that was serving as the main platform for political discussions was shut down,[2] and all internet service providers (ISPs) were forced to cut off their connections to the international internet in order to prevent information from leaking out.[3]

After Bakiev's removal in April 2010, however, these restrictions were lifted and the flow of information returned to normal. In 2011, the environment was relatively favorable to internet freedom, as the interim government was stable and presidential elections in October 2011 were deemed competitive, though flawed. Despite such improvements, internet access remains limited primarily to urban areas, and a number of legal and technical restrictions on online content continue to inhibit internet users.

Over the past year, the government continued to sporadically block certain types of content that were deemed harmful or indecent, such as the "Innocence of Muslims" video that was available on YouTube, and a film festival entry about being gay and Muslim. Additionally, the parliament passed a law in October 2012 aimed at protecting children from harmful content online that was almost identical to legislation passed by Russia; however, the Kyrgyz legislation is less clear regarding restrictions on online media and was met with widespread opposition.

The 2012 court case against independent journalist and blogger Vladimir Farafonov is also likely to have a chilling effect on journalism related to political content. In February 2012, Kyrgyzstan's security service charged Farafonov with "inciting national hatred" for publishing articles online about Kyrgyz-language media and the potential effects of the 2011 presidential election on ethnic minorities living in Kyrgyzstan.[4] On July 3, 2012, Farafonov was found guilty and fined the equivalent of $1,000, avoiding the prison sentence recommended by the prosecution.

OBSTACLES TO ACCESS

Access to information and communications technologies (ICTs) has grown in Kyrgyzstan in recent years, with internet penetration rates among the highest in Central Asia, though still low by global standards. According to the International Telecommunications Union (ITU), the internet

1 "Newspaper suspended, TV station raided in Kyrgyzstan," Committee to Protect Journalists, April 2, 2010, http://cpj.org/2010/04/newspaper-suspended-tv-station-raided-kyrgyzstan.php.
2 "Страна, устремленная в будущее… Кыргызстан-2010. Хроника событий" [The country directed to the future... Kyrgyzstan-2010. Chronicle of events], August 30, 2010, http://pda.kabar.kg/kabar/full/18890.
3 "Блокировка продолжается"[Blocking goes on], Namba.kg (blog), April 6, 2010 http://blogs.namba.kg/post.php?id=470.
4 "Kyrgyzstan must drop charges against journalist," Committee to Protect Journalists, February 29, 2012, http://www.cpj.org/2012/02/kyrgyzstan-must-drop-charges-against-journalist.php.

penetration rate in 2012 stood at 21.7 percent, an increase from 14 percent in 2007.[5] Kyrgyzstan's State Communication Agency (SCA) reported a notably higher 2012 figure of 3.5 million people, or about 50 percent of the population.[6] However, a USAID-funded survey by M-Vector Consulting Agency in 2011 found that only 16 percent of respondents reported ever using the internet.[7] Among them, 51 percent were located in the capital Bishkek and 32 percent in Osh, the country's second largest city. By contrast, only 5 percent of rural respondents reported ever going online, reflecting the urban-rural divide in penetration. Similar research conducted in 2012 by the M-Vector Consulting Agency indicated about 30 percent of the population was using the internet, of which around 70 percent were using mobile devices.[8] Cybercafes are a relatively popular means of obtaining internet access, with over one-third of internet users reporting that they had accessed the internet at such a venue.[9]

Fixed-broadband access, via either fiber-optic cables or DSL, is accessible mainly in Bishkek, with broadband in the provinces provided only by the state-run KyrgyzTelecom. Broadband speeds range from 24 Mbps for DSL to 100 Mbps for the FTTX (fiber to the *x*) network, which is well-developed in Bishkek. The government has launched a CDMA450 mobile telephone and broadband network to expand telecom infrastructure into more rural areas, though it has only become partially active. CDMA450 phones have become popular in rural areas with more than 30,000 subscribers as of November 2011.

Mobile phone penetration is significantly higher than internet penetration in Kyrgyzstan, with a penetration rate of nearly 122 percent in 2012.[10] Mobile phone companies claim that their networks cover 90 percent of the populated territory in the country, thus extending the possibility of internet use for most people as mobile web access expands. At the end of 2010, Beeline (one of the largest mobile phone carriers) launched a 3G network that currently covers the entire country. In January 2012, another large firm, Megacom, launched its own 3G network in Bishkek and reported plans to cover the entire country within six months, though as of 2013 they had not implemented these plans. Saima Telecom has launched a 4G network covering Bishkek and some suburbs.

Despite the spread of ICT infrastructure across the country in recent years, the price of internet access remains beyond the reach of much of the population. As an indication of the limited access among lower income brackets, an M-Vector study conducted in 2011 found that only 6.7 percent of individuals with an average monthly income of less than KGS 2,000 (about $44) use the internet, compared to about 40 percent of those with a monthly income of KGS 20,000 to30,000 (about

5 International Telecommunication Union (ITU), "Percentage of individuals using the Internet," 2007 & 2012, accessed July 13, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
6 Report of the State Communication Agency under the government of Kyrgyz Republic for 2012, accessed July 13, 2013, http://nas.kg/images/god_ot4et2012.docx.
7 "Media Consumption & Consumer Perceptions Baseline Survey," M-vector Consulting Agency, April 2011, http://m-vector.com/upload/news/media_survey_eng/5SectionDInternet.pdf.
8 Media Consumption & Consumer Perceptions Baseline Survey 2012 (2nd Wave) Kyrgyzstan, M-vector Consulting Agency, April 2012, http://m-vector.com/upload/media_presentation/Presentation_media_2wave_fin_EN_general.pdf
9 Ibid.
10 Report of the State Communication Agency under the government of Kyrgyz Republic for 2012, accessed July 13, 2013, http://nas.kg/images/god_ot4et2012.docx

$440 to 662).[11] Moreover, given the high poverty rates in rural areas, accessing the internet is not a high priority for many people.[12] Individuals living in rural areas largely rely on mobile phone internet access because the fixed-line infrastructure is very underdeveloped. Such service costs on average between $20 and $150 per gigabyte for mobile internet access; by comparison, the average monthly income per capita is $190.[13] A lack of equipment and low computer literacy also render internet use difficult for many people in rural areas. Prices for unlimited data plans, which are primarily available in the capital, are more affordable, ranging from $5 to $100 per month for fixed-line broadband, depending on speed.[14] At the end of 2012, mobile operators began to implement data plans with unlimited internet traffic but with limited bandwidth. They are accessible at the price of $0.25 to $0.50 per day.

Fixed-line internet service providers impose different fees for accessing domestic versus international content. All fixed-line operators charge about 10 times less in fees, or do not charge fees at all, for domestic traffic compared to international traffic. Mobile phone operators do not make this distinction in their data plans and charge the same for accessing information, regardless of where it is hosted.

Many social media outlets such as YouTube, Facebook, and Twitter are freely available. However, some international blog-hosting services are subject to filtering from ISPs based in Kazakhstan. ISPs in Kyrgyzstan are not required to use government-owned channels to connect to the international internet and can establish their own. In 2010, the state-owned ISP KyrgyzTelecom completed the construction of a fiber-optic cable connection to China, but it has yet to begin functioning.[15] Currently, three out of four of Kyrgyzstan's first-tier ISPs are linked to the international internet via Kazakhstan and its state-run provider KazakhTelecom; the fourth connects through Russia.[16] As a result, websites that are blocked by the government of Kazakhstan can sometimes become inaccessible to users Kyrgyzstan as well. For example, sites such as LiveJournal, the news website Newsland,ru, and some Google services have been blocked in Kazakhstan, making them inaccessible for some users in Kyrgyzstan. As of May 2013, only Saima Telecom still receives filtered traffic from Kazakhstan, whereas other ISPs receive unfiltered traffic.

Kyrgyzstan's telecommunications sector is relatively liberalized and competitive compared to that of other countries in the region. The state-owned KyrgyzTelecom is the largest ISP with a market share of about 60 percent. The other three first-tier ISPs (Elcat, Megaline, and Saima Telecom) are privately owned. The largest among them is Megaline, which provides broadband service in

11 "Media Consumption & Consumer Perceptions Baseline Survey," M-vector Consulting Agency April 2011, http://m-vector.com/upload/news/media_survey_eng/5SectionDInternet.pdf

12 In rural areas, about 60 percent of the population lives below the poverty line, while in cities, this number is about 30 percent. Source: "USAID Local Development Program," USAID Kyrgyz Republic, accessed September 17, 2012, http://ldp.kg/en/tasks/chas-sector/sectors/agriculture/meat/.

13 World Bank, "Gross national income per capita 2011, Atlas method and PPP," World Bank Databank, 2011, accessed July 18, 2012, http://databank.worldbank.org/databank/download/GNIPC.pdf.

14 The information is obtained by comparisons of tariff plans from the sites of ISPs.

15 "Годовой отчет 2010, Кыргызтелеком" [Annual report 2010, Kyrgyztelecom], Kyrgyztelecom, accessed September 17, 2012, http://www.kt.kg/about_us/documents_and_tender/#ui-tabs-3.

16 "Internet Service Providers in Kyrgyzstan," Tilekus.com (blog), updated January 6, 2012, accessed July 24, 2013, http://www.tilekus.com/interests/internet-in-central-asia/internet-providers-in-kyrgyzstan.

Bishkek. In addition to the first-tier providers, there are 69 licensed second-tier ISPs, though only 15 are active.

There are seven mobile phone operators providing voice and data services via a variety of technical standards. The two largest competitors, with nearly equal market share, are Megacom and Beeline. Megacom was nationalized in 2010 amidst the political upheaval. There are 12 companies with frequencies for deploying 4G networks, but only 4 of them have begun to use the frequencies for this purpose, due to the large investment required in the first stage of deployment.[17]

The main body regulating the ICT industry, including radio spectrum allocation, is the State Communication Agency under the Government of Kyrgyzstan (SCA), a government body with a director and 137 members. The director and two deputies are appointed by the prime minister.[18] Some facets of the agency's work have been criticized, such as the inefficient and non-transparent allocation of radio frequencies and restrictions on wireless mesh networks. Another problematic issue has been the requirement that communication devices (including computers, modems, and wireless access points) be locally certified by the SCA. While this requirement is not systematically enforced, its selective application could serve as an instrument of political pressure and pretext for authorities to seize "uncertified" property, though this has not yet occurred.

LIMITS ON CONTENT

The government does not significantly censor the internet, but some political and news websites, as well as specific content that is deemed controversial or harmful, have been sporadically blocked in the past few years. In 2011 there were several attempts by government bodies to block political content or entire news websites, such as the case against Ferghana.ru. In 2012, the Prosecutor General's Office ordered ISPs to block access to the video "Innocence of Muslims" on YouTube, and to restrict access to a film festival entry titled "I am Gay and Muslim." In the second example, the film festival organizer brought the case to court, arguing that the restriction violated the right to freedom of expression. Additionally, following Russia's enactment of legislation to protect children from harmful content on the internet, the Kyrgyz parliament proposed similar legislation that was met with strong opposition by a variety of stakeholders.

Although the government has taken efforts to censor certain content on the internet, in general there are fewer restrictions placed on material that is available online. This may be because television remains by far the dominant medium through which citizens obtain information about their country, and thus censorship efforts have focused on broadcast media.[19] For example, in the

17 Из 12 компаний только 4 подтвердили, что развертывают сети WiMax и LTE в Кыргызстане [Only 4 from 12 companies confirmed that they are rolling out WiMax and LTE networks in Kyrgyzstan] December 5, 2012, http://www.gipi.kg/archives/4092

18 "Regulation on the State Telecommunication Agency under the government of Kyrgyz Republic," passed by a Resolution of the government of KR № 124, as of February 20, 2012.

19 According to the 2012 M-vector survey, TV still remains the primary source of information for 82.6 percent of the population. Source: Media Consumption & Consumer Perceptions Baseline Survey 2012 (2nd Wave) Kyrgyzstan, M-vector Consulting Agency, April 2012.

run-up to the 2011 presidential elections, the government passed a statute placing stringent regulations on foreign television broadcasts related to the elections and imposing high fines for violations.[20] Given the difficulty of parsing content, television carriers chose to cut off access to most foreign television channels—whether they were Russian, American, or European—in order to avoid the fines. By comparison, the websites of broadcasters such as CNN, the BBC, or Russia Today remained available throughout the campaign. Online resources were not affected by this statute as they are not considered to be mass media. Nevertheless, there have been several incidents of government entities ordering blocks of online content, including at least one news website.

In June 2011, the parliament passed a resolution instructing the government to block the independent Central Asian news website *Ferghana News*, based on charges that its content could incite national strife.[21] In February 2012, the SCA sent letters to all ISPs delineating the requirement to block the news website.[22] As of April 2012, only KyrgyzTelecom had implemented the blocking.[23] On November 19, 2012, the human rights defender organization "Partner Group Precedent," representing *Ferghana News*, filed a lawsuit against the SCA claiming that the ban on the news site violated the right to freedom of expression.[24] During the court hearings, the SCA representative stated that their letter to ISPs requiring them to take measures on blocking *Ferghana News* was of a voluntary nature and that ISPs were not forced to block the website.[25] In April 2013, the SCA sent official letters to ISPs in Kyrgyzstan confirming that they were not required to block the site. Subsequently, all ISPs—including the state one, KyrgyzTelecom—unblocked the site, though the legal status of the original parliamentary resolution is still unclear.[26]

After Russia passed a law titled "On Protection of Children from Negative and Harmful Information" in July 2012, a group of parliamentarians in Kyrgyzstan initiated similar legislation titled "On protection of children from information threatening to their health and development."[27] Although almost identical to the Russian law, this act is less specific regarding internet regulation, and if passed it could be used as a tool for internet censorship by allowing the government to close down sites without a court decision. The criteria upon which the government would make these decisions are unclear. The proposal sparked public outrage, and an internet movement named Kyrnet.kg conducted advocacy activities that compelled members of parliament to postpone the bill until it could be amended.

---

20 According to the statute, all overseas channels during an election campaign can only be broadcasted from recorded sources and must not contain any information about candidates that can be considered as propaganda or that can discredit them. See Article 22 of the Constitutional Law № 68, "On elections of the President of Kyrgyz Republic and deputies of Jogorku Kenesh of Kyrgyz Republic," as of July 2, 2011.
21 "Resolution of Jogorku Kenesh," Kenesh.kg, June 17, 2011, http://kenesh.kg/RU/Pages/ViewNews.aspx?id=8&NewsID=2678.
22 "Пресс релиз Государственного агентства связи при Правительстве Кыргызской Республики" [Press release of the State Telecommunication Agency under the government of Kyrgyz Republic], February 22, 2012.
23 "Independent News Website Partly Blocked in Kyrgyzstan," Radio Free Europe/Radio Liberty, February 22, 2012, http://www.rferl.org/content/independent_news_website_partly_blocked_in_kyrgyzstan/24492408.html.
24 Законность блокирования сайта Fergana.ru [Legality of Fergana.ru blocking], December 3, 2012, http://precedent.kloop.kg/2012/12/03/zakonnost-blokirovaniya-sajta-fergana-ru/.
25 Судебное оспаривание законности блокирования сайта Fergana.ru [Litigation of Legality of Fergana.ru blocking], December 22, 2012, http://precedent.kloop.kg/2012/12/22/sudebnoe-osparivanie-zakonnosti-blokirovaniya-sajta-fergana-ru/.
26 "Kyrgyzstan: News Site Unblocked, Yet Still Illegal," Eurasianet.org, May 7, 2013, http://eurasianet.org/node/66936.
27 На общественное обсуждение выносится законопроект «О защите детей от информации, причиняющей вред их здоровью или развитию» [Protection of Children from Negative and Harmful Information Act is submitted for public discussion], July 10, 2012, http://bit.ly/1bhGZy9.

According to the legal requirements in place under the 2005 statute "On Counteraction to Extremist Activities,"[28] the procedure by which a website can be blocked must first begin with a request to the prosecutor.[29] After the request is issued, a review committee must be assembled consisting of representatives from different organizations (linguistic, religious, legal, and so forth) that can confirm the extremist nature of the site. However, members of the committee are appointed by the government, calling into question the committee's independence and level of objectivity. Once confirmation is granted, a court issues a judicial decision to block the website.

In November 2012, the Ministry of Internal Affairs proposed amendments to the law "On Counteraction to Extremist Activities" originally passed in 2005, which would allow the government to order web hosting services to shut down websites hosted in Kyrgyzstan, or block any sites hosted outside the country, if the government recognizes the content as "extremist."[30] These amendments gave rise to criticism from parliamentarians who noted that in this case websites should be included in the category of mass media, and that the amendments need further discussion.[31] At the same time, these amendments are intended to make the process for blocking websites more transparent, since they oblige corresponding bodies to publish the list of blocked resources on their official sites. Despite the criticisms, the amendments were passed on May 8, 2013.[32]

The video "Innocence of Muslims," which provoked a wave of protests throughout the Islamic world, caused a controversy in Kyrgyzstan as well. On September 19, 2012, the Prosecutor General's Office, based on the expert conclusion of the State Commission for Religious Affairs, filed a claim that asked the court to recognize the video as extremist and ban it from show and dissemination in Kyrgyzstan.[33] At the same time, the Prosecutor General's Office instructed the SCA to take measures to restrict access to the video on YouTube.[34] Parliamentarians debated that question and were divided in opinion, with some of them calling to ignore the video and others affirming the need to protest against it. Finally, the parliament issued a resolution to block the video temporarily before the court issued a decision, which is against the constitution and other laws.[35] One day later, the court decided to recognize the video as extremist and banned it from

28 Dmitry Golovanov, "Kyrgyzstan: Extremism Outlawed," IRIS Merlin, August 2005, http://merlin.obs.coe.int/iris/2005/8/article26.en.html; "The statute on counteraction against extremist activities" as of February 20, 2009.
29 Representatives of the 10th department explained the procedure to the author in a private interview in December 2011.
30 "Во втором чтении приняты поправки в закон о противодействии экстремистской деятельности" [The amendments to the law "On Counteraction to Extremist Activities" have passed second reading], February 28, 2013, http://www.for.kg/news-216159-ru.html.
31 Поправки о закрытии экстремистских сайтов отправили на доработку [Amendments on closing extremist sites are sent to revision] November 26, 2012, http://bit.ly/18eWjdw.
32 Законы Кыргызской Республики за 2013 год [The Statutes of Kyrgyz Republic for 2013] http://minjust.gov.kg/?page_id=11941.
33 «Невинность мусульман» содержит признаки возбуждения межрелигиозной вражды [Innocence of Muslims contains religious hatred traces], September 20, 2012, http://asiapress.kg/koom/3605-nevinnost-musulman-soderzhit-priznaki-vozbuzhdeniya-mezhreligioznoy-vrazhdy.html
34 Генпрокуратура хочет запретить в Кыргызстане показ фильма «Невинность мусульман» [General Prosecutor Office wants to ban "Innocence of Muslims" film in Kyrgyzstan], September 19, 2012, http://www.knews.kg/ru/action/21685/
35 Жогорку Кенеш выразил позицию по фильму «Невинность мусульман» [Jogorku Kenesh expressed its position for film "Innocence of Muslims"] September 20, 2012, http://kabar.kg/index.php/politics/full/40755.

show and dissemination in Kyrgyzstan.[36] According to a statement by the State Committee of National Security of Kyrgyzstan, possession of the film on any storage device could have led to criminal prosecution.[37] Interestingly, the Religious Administration of Muslims of Kyrgyzstan stated that there was nothing in the video related to Islam and called on Kyrgyz Muslims not to react to the provocation.[38]

One week later, a film titled "I Am Gay and Muslim" by the Dutch director Chris Belloni was scheduled to screen at the International Documentary Film Festival on Human Rights held in Bishkek from September 24–28, 2012. On September 28, the day the film was supposed to be shown, representatives from the State Committee of National Security (SCNS) confiscated a copy of the film and issued a warning to the festival organizers, stating that the State Commission of Religious Affairs had deemed the film "extremist."[39] That same day, the Pervomaysky District Court recognized the film as extremist and banned it from demonstration and dissemination.[40] Additionally, the Prosecutor General's Office ordered the SCA to take measures to restrict access to this film for internet users in Kyrgyzstan, and on October 8, 2012, the human rights group that organized the film festival received a notice from their web hosting company stating that their website might be shut down if it contained any references to the banned film.[41] The organizer of the festival, Tolokan Ismailova, claimed that SCNS representatives did not have the authority to confiscate the film or issue the warning and brought a suit against the State Committee of National Security. Nevertheless, the court dismissed the case.[42]

The government has also sought to restrict access to terrorism-related content. In November 2011, a top official in the 10th department of the Ministry of Internal Affairs claimed that their unit for countering cyberthreats had identified 12 websites with terrorist and extremist content that were then blocked according to a court order.[43] Among the list of blocked websites was Furqon.com, which belongs to the militant group Islamic Movement of Uzbekistan.

Self-censorship exists online to a certain degree, primarily as a result of government restrictions against the incitement of national hatred. All posts on forums are strictly moderated to limit this

36 "Суд запретил распространение и показ фильма «Невинность мусульман» в Кыргызстане" [The court ruled to ban dissemination and show of the film "Innocence of Muslims" in Kyrgyztan] September 21, 2012, http://www.kabar.kg/rus/society/full/40796

37 В случае обнаружения фильма «Невинность мусульман» в компьютере или других электронных носителях, их владелец будет привлечен к ответственности – ГКНБ [In case of discovering of the film "Innocence of Muslims" on computer or any electronic devices, the owner will be criminally prosecuted], September 21, 2012, http://www.paruskig.info/2012/09/21/68993

38 ДУМК: В фильме "Невинность мусульман" нет ничего, имеющего отношение к исламу [RAMK: The film "Innocence of Muslims has nothing related to Islam"] September 18, 2012, http://bit.ly/18AlJBo.

39 "Kyrgyzstan: Dismissal of the complaint lodged by Mrs. Tolekan Ismailova," International Federation for Human Rights (FIDH), November 29, 2012, http://www.fidh.org/Kyrgyzstan-Dismissal-of-the-12515.

40 Ibid.

41 Ibid.

42 Толекан Исмаилова против Государственного комитета национальной безопасности по делу о фильме «Я – гей и мусульманин» [Tolekan Ismailova vs. State Committee of National Security regarding "I am Gay and Muslim"], December 7, 2012, http://anticorruption.kg/2012/12/07/1057/.

43 "12 сайтов заблокировано на территории Кыргызстана за распространение слухов экстремистского характера" [12 sites have been blocked in Kyrgyzstan as spreading rumors of extremist kind], Kyrgyz Telegraph Agency (KirTAG), November 28, 2011, http://www.kyrtag.kg/?q=news/13260.

type of content, and online journalists or bloggers generally try to avoid issues concerning ethnic relations.

Online platforms such as forums and social networks are actively used for manipulating public opinion, usually by "trolls" hired by different political actors to influence discussions and express favorable views. Reportedly, the compensation of a "troll" for one campaign can be anywhere from US$200–700.[44]

The Kyrgyz blogosphere is not well-developed. There are several popular blog-hosting platforms in Kyrgyzstan (such as Namba.kg, Kloop.kg, Diesel.elcat.kg, and Taboo.kg), but most blogs focus on entertainment, reprint reports from other news agencies, or simply contain a blogger's personal thoughts on different issues. There are no particularly popular blogs specifically devoted to political or social issues. Most blogs are in Russian, though some are in the local Kyrgyz language, but the latter are not as popular as the former. The internet in general has become an important source of alternative information for users, but since it is primarily the wealthier segments of the population who can afford to consistently access the internet, the wealthy are the main participants in online communities. Social media applications such as Facebook have not yet gained widespread popularity. As of February 2013, there were about 111,000 Facebook users in Kyrgyzstan, accounting for about 10 percent of the online population in the country.[45]

Several online initiatives were launched in the run-up to the 2011 elections, including the website Politmer.kg, created to allow Kyrgyz citizens to monitor the campaign promises made by the presidential candidates, and the crowd-sourcing website Map.inkg.info, created to document and map election violations. During pre-election debates, some forum topics were created to collect questions for the candidates.

Perhaps the most successful online mobilization campaign came in response to the proposed legislation titled "On protection of children from information threatening to their health and development." This proposal provoked public outrage, and in an effort to bring attention to the issue, many of the largest ISPs and content providers placed banners over their sites with slogans such as "ATTENTION! This site can be closed. Get to know details and vote against." The proposal also sparked the internet movement Kyrnet.kg, which conducted advocacy initiatives against the act. Within two months, the site had collected approximately 12,000 votes against the act. Furthermore, in a September 2012 meeting with group of parliamentarians from the political group that had initiated the act, the representatives of Kyrnet.kg showed the results of the voting and explained the shortcomings of the act. The parliamentarians agreed that the act needed further elaboration and promised to arrange an extended meeting with all of the parliamentarians who initiated the law for further discussion.[46]

---

44 Almaz Rysaliev, Yulia Goryaynova, Dina Tokbaeva, Lola Olimova, and Bakhtiyor Rasulov, "Central Asia's 'Troll Wars,'" Institute for War & Peace Reporting, February 14, 2012, http://iwpr.net/report-news/central-asias-troll-wars.
45 "Kyrgyzstan Facebook Statistics," Social Bakers, accessed March 2012, http://www.socialbakers.com/facebook-statistics/kyrgyzstan.
46 Наши лайки работают [Our likes work!], September 17, 2012, http://kyrnet.kg/archives/44.

VIOLATIONS OF USER RIGHTS

Authorities in Kyrgyzstan continued to prosecute individuals for posting material online that was deemed controversial, based on charges such as "inciting national hatred." Additionally, in February 2013 there was a case of physical assault against a journalist by a member of parliament. While this appears to be an isolated incident, it points to a broader lack of respect for journalists on the part of politicians in the country.

The rights to freedom of speech and freedom of expression are legally protected in the new constitution that was approved by referendum in June 2010, and which strengthens the power of the country's parliament vis-à-vis the president. Article 31 of the constitution guarantees the right to freedom of thought, expression, speech, and press. Article 29 provides constitutional protections over privacy, including private correspondence (by phone, mail, electronic, or others), and forbids the collection or dissemination of confidential information without an individual's consent. Nevertheless, the judiciary is not independent and remains dominated by the executive branch. Corruption among judges, who are generally underpaid, is also widespread, hindering the fairness of decisions in freedom of expression cases as well as others.

In July 2011, the government decriminalized libel to bring legislation in line with the new constitution. Nevertheless, "insult" remains a criminal offense and is punishable by a fine. Officials have long used libel charges to stifle critical media but have not applied these laws against bloggers to date.[47] The criminal code contains several provisions (Articles 299 and 299-1) that prohibit "inciting national, racial, religious or inter-regional hostility." In some cases, the government has sought to apply these provisions in a bid to restrict nonviolent political speech as well.

One of these cases involved independent journalist and blogger Vladimir Farafonov, who was charged on February 12, 2012 with inciting national hatred based on his publications on News-Asia.ru, Centrasia.ru and Parus.kg.[48] Farafonov had written a series of articles that were critical of Kyrgyz politics and which examined the potential effects of the 2011 presidential election on the country's minority populations.[49] The charge was based on the opinion of a commission convened by the security service, but given the fact that the commission was composed of only legal and political experts, Farafonov asked for Russian philology experts to review the case. These experts expressed their opinion that Farafonov had used language that was tough and sometimes tactless, but not extremist.[50] The prosecution had asked for a sentence of 8 years in jail for Farafonov;

47 "OSCE Hails Kyrgyzstan Decision to Discriminate Libel," The Telegraph, July19, 2011, http://www.telegraph.co.uk/news/worldnews/asia/kyrgyzstan/8648135/OSCE-hails-Kyrgyzstan-decision-to-decriminalise-libel.html.

48 ГКНБ Кыргызстана: Экспертиза подтвердила наличие признаков разжигания межнациональной розни в публикациях Владимира Фарафонова [SCNS of Kyrgyzstan: commision of experts proved the indications of national hatred incitement in publications of Vladimir Farafonov], February 20, 2012, http://www.24.kg/community/122018-gknb-kyrgyzstana-yekspertiza-podtverdila-nalichie.html.

49 "Kyrgyzstan must drop charges against journalist," Committee to Protect Journalists, February 29, 2012, http://www.cpj.org/2012/02/kyrgyzstan-must-drop-charges-against-journalist.php.

50 Журналист Владимир Фарафонов обвиняется в разжигании межнациональной розни! [The journalist Vladimir Farafonov is accused in national hatred incitement!], February 24, 2012, http://polit.kg/newskg/310.

however, the judge decided to reduce the sentence to a fine of KGS 50,000 (approximately $1,000). The case became widely known and aroused a wave of indignation from journalists,[51] as there were many cases of similarly tactless expressions by other authors in Kyrgyz language media outlets which received no punishment.

All traditional media outlets must register with the government. In June 2011, the Prosecutor General's Office proposed amending the statute that regulates mass media[52] to include internet news websites as a form of mass media, requiring them to have a license and to operate with the same responsibilities as traditional media outlets.[53] In January 2012, an expert from the Government Office seconded the recommendation;[54] however, it remains unclear whether online media are to be treated the same under the law as traditional news media outlets.

There are currently no restrictions on anonymous communication on the internet in Kyrgyzstan. Websites do not need to register, encryption software is freely available, and real-name registration is not required to post content online. Furthermore, registration for prepaid SIM cards is optional; however, post-paid SIM cards, which are rarely used, do require registration with a passport.

Like many former Soviet states, Kyrgyzstan maintains and updates its surveillance technology in line with Russia's practices. Kyrgyzstan's surveillance network is modeled after Russian SORM technology ("system for operational-investigative activities"), and in August 2012, Kyrgyzstan updated its surveillance network to be on the same level as current Russian interception systems.[55]

In 2010 and 2011, there were several scandals which revealed the abuse of equipment used for intercepting communications. A subsequent study from June 2011 by the non-profit Civil Initiative on Internet Policy (CIIP) analyzed the legislative framework surrounding interception and its enforcement. It concluded that there were many gaps in the law that enabled interception equipment to be used, and even abused, without sufficient oversight.[56] In April 2011, the parliament passed a decision to switch off all interception equipment deployed on the premises of mobile phone operators.[57] According to reports from September 2011 by members of parliament,

---

51 Кыргызстан: После митинга в защиту В.Фарафонова в посольство РФ переданы обращения А.Князева, У.Бабакулова и российских соотечественников [Kyrgyzstan: After rally in support of V. Farafonov, petitions of A.Knyazev, U. Babakulov and Russian countrymen were submitted to Russian Embassy] February 27, 2012, www.fergananews.com/news.php?id=18246

52 The law, "On mass-media," June 16, 2008, http://www.medialaw.kg/?q=node/9.

53 "Генпрокуратура Кыргызстана предлагает «законодательно к СМИ отнести интернет-издания и сайты, зарегистрированные в зоне kg»" [Prosecutor General's Office suggests "to legalize internet agencies and sites, registered in .kg zone, by inclusion them in the list of mass-media"], 24.kg, June 6, 2011, http://www.24.kg/community/101891-genprokuratura-kyrgyzstana-predlagaet.html.

54 Nurzada Tynaeva, "Эксперт Аппарата правительства предлагает разработать новый закон «О СМИ», чтобы регулировать информагентства" [The expert of the Government Office suggests to work out the new statute on mass-media to regulate information agencies], Knews.kg, January 17, 2012, http://www.knews.kg/ru/parlament_chro/9145/.

55 Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," World Policy Institute, Fall 2013, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

56 "Анализ законодательства КР на соответствие применения СОРМ, – предварительное заключение" [Analysis of the Kyrgyz legislation, concerning lawful using of interception equipment -preliminary conclusion], Gipi.kg, accessed September 17, 2012, http://www.gipi.kg/archives/1743.

57 Resolution of Djogorku Kenesh № 332-V as of 15.04.2011, "On switching off mobile operators' lawful interception equipment."

however, the equipment continues to function.[58] Since February 2012, the CIIP, together with the Kyrgyz State Committee on National Security and several human rights organizations, have been working on amendments to the statute on the Conduct of Investigations—the body responsible for regulating these issues—that would clarify the circumstances surrounding the use of interception and provide a more adequate legal framework. As of mid-2013, the draft was still being discussed in the parliament because of an ongoing debate between the two bodies looking to take control over the interception equipment: the Ministry of Internal Affairs and the State Committee of National Security.

Amid ongoing ethnic tensions, in 2011, there were several reported instances of physical attacks or intimidation of members of minorities associated with news websites. In August 2011, Sokhrukh Saipov, the editor and publisher of the news website UzPress, was brutally attacked, although it is unclear whether Saipov was attacked specifically for his online activities. The website publishes content in three languages about the social and political challenges affecting ethnic Uzbeks in southern Kyrgyzstan.[59] In a separate incident in May 2011, followers of the nationalist Asaba party threatened non-ethnic Kyrgyz staff of the online news agency 24.kg.[60] In 2012, there were 10 instances of physical attacks on journalists.[61] Most of them occurred during the coverage of mass rallies; however, none of these attacks were directly related to online activities.

In February 2013, Member of Parliament (MP) Tursunbai Bakir uulu, a former ombudsman, published a post on his Facebook page in which he indirectly called another MP, Irina Karamushkina, a "guest" in Kyrgyzstan because she did not know the Kyrgyz language. A journalist, Eric Israilov, defended Karamushkina by stating that she not a guest but was rather an MP and a citizen of Kyrgyzstan. The online debate became very heated, and Bakir uulu suggested that Israilov meet him face-to-face. During the meeting Bakir uulu reportedly pushed Israilov and slapped him in his face.[62] Later, the leader of the political party to which Bakir uulu belongs stated that it was a quarrel between two men and had nothing to do with political issues.[63] In a session of parliament

58 "Дастан Бекешев: В Кыргызстане в компаниях сотовых операторов до сих пор действует система СОРМ" [Dastan Bekesev: Lawful interception equipment still keeps working in mobile operators in Kyrgyzstan], 24.kg, September 8, 2011, http://www.24.kg/parlament/108440-dastan-bekeshev-v-kyrgyzstane-v-kompaniyax.html.

59 "Independent Journalist Brutally Attacked in Kyrgystan," Committee to Protect Journalists, August 15, 2011, http://www.cpj.org/2011/08/independent-journalist-brutally-attacked-in-kyrgyz.php.

60 "World Report 2012: Kyrgyzstan," Human Rights Watch, accessed August 30, 2012, http://www.hrw.org/world-report-2012/world-report-2012-kyrgyzstan.

61 В этом году в Кыргызстане совершено 10 нападений на журналистов во время выполнения им профессиональных обязанностей [There are 10 physical attacks on journalists happened during performance of their duties in this year] November 9, 2012, http://www.paruskg.info/2012/11/09/71388.

62 Депутат Турсунбай Бакир уулу оскорбил и ударил корреспондента ежедневника «Общественный рейтинг» Эрика Исраилова [The deputy Tursunbai Bakir uulu offended and attacked the journalist of daily edition "Public rating" Eric Israilov], February 15, 2013, http://inkg.info/narusheniya-prav/pravo-na-dostup-k-informatsii/2702-deputat-tursunbaj-bakir-uulu-oskorbil-i-udaril-korrespondenta-ezhednevnika-obshchestvennyj-rejting-erika-israilova

63 Феликс Кулов: Турсунбай Бакир уулу не отрицает, что ударил Эрика Исраилова, это ссора двух мужчин, а не журналиста и депутата [Felix Kulov: Tursunbai Bakir uulu doesn't deny that he slapped Eric Israilov, but it was a quarrel of two men and not deputy and journalist] February 15, 2013, http://www.24kg.org/parlament/148170-feliks-kulov-tursunbaj-bakir-uulu-ne-otricaet.html.

two months later, members of parliament blamed Israilov as the source of the conflict and recommended revoking his credentials.[64]

Instances of politically motivated cyberattacks are generally rare, including in the run-up to the 2011 presidential elections, but they do occur. In 2005, the OpenNet Initiative recorded the extensive use of distributed denial-of-service (DDoS) attacks against opposition and news websites, demonstrating a precedent for such attacks.[65] In September 2011, there was one incident of hackers defacing Kabar.kg, the online government news agency website, but this did not significantly obstruct the agency's work. In March 2012, the social entertainment resource Namba.kg experienced a DDoS attack that was apparently part of an extortion attempt.[66] In the same month, the news agency Vesti.kg also reported a DDoS attack on its site,[67] presumably because they had been republishing articles from *Ferghana News*.

During 2012 there were several incidents of cyberattacks on government sites. The sites of the Ministry of Defense (Mil.kg), the State Communication Agency (Nas.kg), and the main portal of the government (Gov.kg) were defaced at different times. However, these attacks were attributed to the overall weak security of the sites, rather than to attacks by the opposition, and all attacks were made automatically by finding some vulnerabilities.

64 Журналист Эрик Исраилов депутатам не по зубам [The journalist Eric Israilov is too tough for the deputies], April 13, 2013, http://rus.kg/news/policy/10473-zhurnalist-erik-israilov-deputatam-ne-po-zubam.html.
65 "Kyrgyzstan," OpenNet Initiative, December 18, 2010, http://opennet.net/research/profiles/kyrgyzstan.
66 As reported by the blog at: http://blogs.namba.kg/post.php?id=116481.
67 Anna Yalovkina, "Редактор "Ферганы": Трудно судить, связаны ли DDoS-атаки на "Фергану" и "Вести"" [Editor of *Fergana*: It's hard to judge whether DDoS attacks on Fergana and Vesti are related], Vg.kg, March 29, 2012, http://www.vb.kg/news/society/2012/03/29/183948_redaktor_fergany_trydno_sydit_sviazany_li_ddos_ataki_na_fergany_i_vesti.html.

LEBANON

	2012	2013
INTERNET FREEDOM STATUS	N/A	PARTLY FREE
Obstacles to Access (0-25)	n/a	14
Limits on Content (0-35)	n/a	10
Violations of User Rights (0-40)	n/a	21
Total (0-100)	**n/a**	**45**

* 0=most free, 100=least free

POPULATION: 4.3 million
INTERNET PENETRATION 2012: 61 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The Lebanese parliament reviewed numerous proposals for a long-awaited new media law that will seek to regulate internet and mobile communications (see **VIOLATIONS OF USER RIGHTS**).
- Several web users were prosecuted for libel and defamation, though charges were dropped after media pressure or public outcries (see **VIOLATIONS OF USER RIGHTS**).
- In a highly-publicized move, Telecommunications Minister denied a request by the internal security apparatus for access to phone records, e-mail, and other data for millions of Lebanese users, while igniting public discourse on the legality of such requests (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

The Lebanese public has long had a strong sense of entitlement to freedom of expression and freedom of the press, particularly in comparison to many countries in the region, although in reality some of these freedoms have been curbed. The introduction of the internet to the country in 1991 has furthered this sense while offering even more channels for Lebanese to express themselves and protest any attempt to curb their freedoms.[1] At the same time, the problems that plague traditional media also shape and influence new media and communication technologies, such as sectarian divisions, partisanship, the vague legal environment, and the poor state of infrastructure. These many issues are often attributed to a struggling economy and constant political turmoil.

Over the past year, mainstream and social media were abuzz with stories of low profile police arrests, interrogations, and intimidations that targeted online activists, bloggers, and social media users. There were many unconfirmed reports surrounding attempts by the government to censor or even force the closure of online discussion forums and social media groups that expressed political criticism. As the parliamentary committee on media and telecommunications continues to engage in confidential discussions in drafting a new media law, Lebanese continue to deal with the chaotic, confusing and somewhat restrictive legal environment of the country.

If promises are kept to introduce positive reforms of the legal, infrastructural, and economic aspects of the Lebanese ICT sector, the country can reconfirm its *avant-garde* status within the Arab world. If, on the other hand, the government fails to pass new legislation or worse, implements one of the many poorly-conceived laws it has proposed in recent years, Lebanon risks regressing into an oppressive online environment in which the rights to privacy and information are restricted by authorities. Some developments at the infrastructural level and policy level hint to a brighter future, but the recent government collapse and deteriorating situation due to the conflict in neighboring Syria suggest otherwise. The recent upsurge in political-sectarian conflict has further destabilized Lebanon and contributes to an overall sense of uncertainty over the ICT infrastructure and online media landscape.

OBSTACLES TO ACCESS

In the past, internet and mobile services had been expensive, slow, unreliable, and difficult to access, especially in rural areas and outside of the capital Beirut.[2] Recently, however, access to the internet in Lebanon has been slowly but steadily improving under pressure from activists and businesses. Figures from the International Telecommunication Union (ITU) showed that internet

[1] The internet in Lebanon was first introduced to the American University of Beirut in 1991. Public access started two years later, but the significant diffusion of public internet access did not take off until the mid-1990s when multiple ISPs were established. See http://webscience.blogs.usj.edu.lb/1636/history-of-web-in-lebanon/.

[2] Jad Melki, Yasmine Dabbous, Khaled Nasser and Sarah Mallat (2012). Mapping Digital Media: Lebanon, New York, NY: Open Society Foundation. http://www.soros.org/initiatives/media.

penetration increased from 19 percent in 2007 to 61 in 2012.[3] Broadband penetration (fixed and wireless) stands at 24 percent, although fixed-broadband remains unavailable in many rural areas.[4] Of the estimated 1.3 million internet subscribers in Lebanon, currently 722,000 of them have 3G subscriptions.[5] Nonetheless, 3G connections are slow, sporadic, and unavailable in many remote areas.[6] Overall, there are around 93 mobile telephone subscriptions per every 100 inhabitants.[7]

In October 2011, the Lebanese government dramatically increased the speed of broadband internet and introduced 3G technology to mobile services. Average internet speeds have doubled since March 2012, though Lebanon still ranks only 151st in the world for average speeds, according to the independent Household Download Index.[8] The Ministry of Telecommunications promised further improvements and the upcoming introduction of 4G.[9] In the past, however, political clashes between the ministry and operators have delayed network upgrades.[10] In addition, the ministry has been slow to respond to much-needed repairs and upgrades outside of major urban areas, although significant progress has been achieved in the past two years.

The government also substantially lowered the cost of broadband internet and mobile phone subscriptions in 2011, although consumer groups maintain that rates remain significantly more expensive than in many other countries.[11] The monthly subscription fee for ADSL starts at $22 and reaches up to $135, including the separate subscription to a fixed phone line.[12] The monthly subscription fee for 3G ranges from $10 to $100, excluding the basic mobile subscription and calling fees, which average around $40.[13] Just over a year ago, these prices were 80 percent higher. Nevertheless, they remain relatively high considering that, in 2011, Lebanon had a gross national income per capita of $9,140, which translates to $762 per month.[14] The relatively high prices have not deterred most Lebanese from using internet and mobile services extensively, particularly the youth. Internet usage and digital literacy, however, tend to drop with older and less affluent citizens, as with rural inhabitants.[15]

---

[3] International Telecommunication Union (ITU), "Percentage of individuals using the Internet," 2012, accessed August 1, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[4] Facts and Figures. (2011, December). Telecommunications Regulatory Authority. http://www.tra.gov.lb/Market-Data-Facts-and-figures.
[5] Facts and Figures. (2011, December). Telecommunications Regulatory Authority.
[6] The Daily Star. (2012, Nov 10). Internet speed increases in one year. http://www.dailystar.com.lb/Business/Lebanon/2012/Nov-10/194587-internet-speed-increases-in-one-year.ashx.
[7] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2012, accessed August 1, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[8] The Daily Star. (2013, April 3). Lebanon Internet speed to rise to 20 megabits per second. http://www.dailystar.com.lb/Business/Lebanon/2013/Apr-03/212359-lebanon-internet-speed-to-rise-to-20-megabits-per-second.ashx#axzz2PQQPW7BO.
[9] The Daily Star. (2012, Nov 10). Internet speed increases in one year. http://www.dailystar.com.lb/Business/Lebanon/2012/Nov-10/194587-internet-speed-increases-in-one-year.ashx.
[10] Sami Halabi. (2011, October 3). High Hopes and Higher Hurdles. http://www.executive-magazine.com/economics-and-policy/High-Hopes-and-Higher-Hurdles/3918.
[11] The Daily Star. (2013, February 14). Consumer group raps Lebanon telecoms rates . http://www.dailystar.com.lb/Business/Lebanon/2013/Feb-14/206361-consumer-group-raps-lebanon-telecoms-rates.ashx.
[12] See for example: Cyberia Internet: http://www.cyberia.net.lb.
[13] See for example: MTC Touch: http://www.3g-touch.com/#!mtc3g.
[14] World Bank. (2011). Lebanon. http://data.worldbank.org/country/lebanon.
[15] Melki, J. (2010). Media Habits of MENA Youth: A Three–Country Survey. *Issam Fares Institute Youth in the Arab World Working Paper Series*, *2*(1), 3–50. http://bit.ly/9PVsQ3.

Disruptions to internet services are infrequent in urban areas, but tend to occur more often outside of Beirut and in rural areas. The disruptions are usually caused by technical problems and the inability of the network to handle the increased user load.[16] Lebanon is also liable to frequent electrical blackouts, sometimes lasting several hours per day. The Lebanese government maintains a monopoly over the internet's backbone, as well as over the fixed and mobile telephone industry in general, allowing it to exercise tight control over internet service providers (ISPs).

The Lebanese telecommunications industry is government-owned and tightly regulated. Lebanon has two government-owned mobile phone companies, officially named Mobile Interim Company 1 and Mobile Interim Company 2. These operate respectively under the commercial names Alfa and Touch, which are run by the private companies Orascom Telecom Holdings and Zain, respectively.[17] Because the government sets prices and issues permits for the number of subscriptions allowed, there is little competition in the industry and the two companies practically split the market evenly between themselves.[18] The fixed-line telephone and internet network is owned and operated by Ogero, a state company headed by Abdulmenaim Youssef. Ironically, Youssef also occupies a position within the Ministry of Telecommunications that oversees the operations of Ogero.

In addition to running the internet's backbone, Ogero sets internet prices and shares in the management of online subscriptions, together with two dozen private ISPs.[19] Since no law regulates their licensing, private ISPs currently obtain a permit by decree from the Ministry of Telecommunications.[20] In addition, the government has significant control over the processing and approving of user applications for broadband services, which can usually take between six to eight weeks. Crucially, political influence can significantly interfere with the allocation of contracts to private ISPs and mobile phone operators.[21]

Lebanese media and telecommunications laws are regulated by three semi-independent advisory bodies that report to the Council of Ministers. The National Council for Audiovisual Media and the Committee for Establishing Model Bylaws and Practices deal mainly with audiovisual media (TV, radio, and satellite), while the Telecommunications Regulatory Authority (TRA) is responsible for liberalizing, regulating, and developing the telecommunications sector in Lebanon. Overall, the three bodies remain largely powerless and fail to live up to their expectations as independent regulators in a modern state. While in theory the TRA is independent from the government, in

[16] Sami Halabi. (2011, October 3). High Hopes and Higher Hurdles. http://www.executive-magazine.com/economics-and-policy/High-Hopes-and-Higher-Hurdles/3918

[17] Please see http://www.touch.com.lb/autoforms/portal/touch/about-touch/who-we-are/about-us and https://www.alfa.com.lb/aboutus/companyinfo.aspx.

[18] The Business Year. (n.d.). Interview Marwan Hayek. The Next Step. http://www.thebusinessyear.com/publication/article/2/48/lebanon-2012/the-next-step.

[19] Facts and Figures. (2011, December). Telecommunications Regulatory Authority. http://www.tra.gov.lb/Market-Data-Facts-and-figures.

[20] According to the Telecommunications Regulatory Authority (TRA), it is TRA's prerogative to assess and grant license to ISPs, but the past three ministers of telecommunication have considered that the TRA has no legal authority to do so, and the ministry has used an old law as a basis for their right to grant such license. See below for conflicts between the TRA and the Telecommunications Ministry.

[21] Jad Melki, Yasmine Dabbous, Khaled Nasser and Sarah Mallat (2012). Mapping Digital Media: Lebanon, New York, NY: Open Society Foundation. http://www.soros.org/initiatives/media. p. 89.

reality, dominant Lebanese political groups possess a great deal of influence over the institution, often rendering it powerless.[22] For this reason, the Ministry of Telecommunications remains the strongest player in the internet and communications technology (ICT) domain. In fact, the past three telecommunications ministers have gone so far as to claim that the TRA has no real authority since the law establishing its powers has not yet been implemented.[23] Tellingly, since its launch in 2007, many of the TRA's objectives have not been met, namely the transition from analog to digital networks and the privatization of the telecommunications sector. As previously stated, many of these issues are being held up by political disputes.

LIMITS ON CONTENT

No evidence suggests that the Lebanese government blocks or filters ICT content, particularly in relation to political and social issues.[24] Lebanon's Virtual Museum of Censorship, which is complete with reports about censorship in television, radio, film, literature, and theater, lists only two cases of online censorship: the government's decision to ban Facebook inside parliament in 2011, and a report about the controversial draft media law proposed by the Ministry of Information, discussed below in greater detail.[25] YouTube, Facebook, Twitter and international blog-hosting services such as Wordpress and Blogger are freely available. In fact, Facebook, Google, Yahoo, Windows Live, Wikipedia, Twitter, LinkedIn, Blogspot, and MSN rank among the top 15 most visited websites in Lebanon.[26] However, self-censorship is prominent in the blogosphere and in the country's top media outlets, which are owned by powerful figures from all sides of the political spectrum. For this reason, Lebanese enjoy access to a wide variety of views and perspectives online, even if the online media landscape reflects the country's partisan and sectarian divisions.

While most social media and communication apps are available in Lebanon, certain Voice-over-Internet-Protocol (VoIP) applications are blocked on an inconsistent basis in line with the 2002 Telecom Act.[27] In 2010, the government-owned phone company Ogero installed equipment to block VoIP throughout the network, but subsequently backed down under pressure from businesses, civil society, and politicians. It is important to note that VoIP services are mainly blocked because they cut into government revenues generated by international phone calls. Furthermore, only certain VoIP services are blocked, such as Vonage, while Skype is freely accessible. No clear government decision on the matter exists and the law banning VoIP remains in place, though its implementation remains vague and inconsistent.

[22] Jad Melki, Yasmine Dabbous, Khaled Nasser and Sarah Mallat (2012). Mapping Digital Media: Lebanon, New York, NY: Open Society Foundation. http://www.soros.org/initiatives/media, pp. 34 and 82.
[23] Sami Halabi. (2011, July 3). Redialing discord. Executive Magazine. http://www.executive-magazine.com/economics-and-policy/Redialing-discord/4770.
[24] Imad Atalla. (2010. June 8). The Daily Star. http://www.dailystar.com.lb/Opinion/Commentary/Jun/08/Lebanon-is-stifling-your-digital-freedom.ashx.
[25] The Virtual Museum of Censorship. http://www.censorshiplebanon.org/Home.
[26] Alexa. (2013, March 1). Top Sites in Lebanon. http://www.alexa.com/topsites/countries/LB.
[27] Imad Atalla. (2010. June 8). The Daily Star. http://www.dailystar.com.lb/Opinion/Commentary/Jun/08/Lebanon-is-stifling-your-digital-freedom.ashx.

One reason for the lack of blocking and filtering pertains to the highly-politicized landscape of traditional and new media in Lebanon.[28] Government officials are arguably hesitant to engage in censorship out of fears that the moves could be seen as unfairly targeting one political-sectarian group. In the past, this has been shown to quickly galvanize various groups against the government or the state security apparatus, causing riots and unrest.

While filtering is not practiced, there have been limited incidents in which government security officials pressured individuals and ISPs to remove certain comments—mainly criticisms of government officials or the army—from social media pages, blogs, or websites. Acting upon a court order, the Directorate for General Security has, in the past, pushed the administrators of Facebook groups to delete comments or close groups that are seen as defamatory. In addition, intermediaries are legally liable for content posted by users, including domain hosting services and ISPs (for more on libel cases and the arrests of intermediaries, see "Violations of User Rights").

Taboo subjects that would normally be banned from mainstream media outlets, such as pornography, gambling, content supportive of Israel, and sectarian hate speech, are freely available online. Indeed, two recent and controversial anti-Islam videos, "The Innocence of Muslims" and "The Innocent Prophet," remain accessible, despite a September 24, 2012 court decision to ban access to the former in Lebanon.[29] Legal experts had expressed skepticism about the ability of authorities to implement the court order. [30]

Many bloggers and online journalists admit to self-censorship, fearing repercussions from the government or specific political or sectarian groups.[31] The issues bloggers and online journalists avoid have changed over time; for example, criticism of Syria before 2005 was rare, but some "red lines" have remained constant, such as criticism of Saudi Arabia and its royal family. Contributing to this censorial culture were the numerous assassinations of journalists and politicians from 2005 to 2011, a period that witnessed significant shifts in power inside Lebanon. This climaxed with the high profile assassination of Prime Minister Rafik Hariri and the subsequent withdrawal of Syrian forces from Lebanon. Nonetheless, even the most controversial topics are openly debated online. For example, although homosexuality remains taboo in Lebanon and laws criminalize "unnatural sexual relationships," LGBTIQ rights organizations continue to publish content online despite occasional harassment from security officials.[32]

Lebanese users have access to a wide variety of local and international information sources. Reflecting Lebanon's pluralistic society, Lebanese media is highly partisan and controlled by the

[28] Jad Melki, Yasmine Dabbous, Khaled Nasser and Sarah Mallat (2012). Mapping Digital Media: Lebanon, New York, NY: Open Society Foundation. http://www.soros.org/initiatives/media. pp. 21-22.
[29] Al-Jazeera Blogs. (Sept 25, 2012). Lebanese court decides to block internet access to anti-Islam video. http://blogs.aljazeera.com/topic/anti-islam-video-protests/lebanese-court-decides-block-internet-access-anti-islam-video.
[30] Legal Agenda (Al-Mufakira Al-Kanouniya). (2012, October 1). A Lebanese judge interferes to stop the publication of the film "Innocent Prophet." http://www.legal-agenda.com/newsarticle.php?id=167&folder=legalnews&lang=ar, and Agence France Presse, "Lebanese court decides to block internet access to anti-Islam video," Al Jazeera English, (25 September 2012), http://blogs.aljazeera.com/topic/anti-islam-video-protests/lebanese-court-decides-block-internet-access-anti-islam-video.
[31] Human Rights Watch. (2005). False Freedom: Online censorship in the Middle East and North Africa. http://www.hrw.org/en/reports/2005/11/14/false-freedom-0.
[32] See www.helem.net.

dominant political-sectarian actors, mainly through direct ownership of prominent media outlets.[33] For example, former Prime Minister Saad Hariri owns Future TV, al-Mustaqbal, the Daily Star, and a host of other online and offline media outlets. Similarly, Speaker of Parliament Nabih Berri owns National Broadcasting Network and its affiliates, while Hezbollah controls a vast network of media outlets, including al-Manar TV and al-Nour radio. The heads of these media outlets are chosen by these dominant political figures and their news content clearly advances a particular partisan message. While ensuring plurality, this also creates a climate in which the public sphere is dominated by the agendas of the powerful political-sectarian leaders and their allies, suffocating the voices of those who fall outside the main groups.[34] At the same time, politicians are known to bribe the few independent news outlets and journalists that do exist, particularly during election periods.

Online advertising in Lebanon is growing but remains weak, partly due to the slowness and unreliability of the internet. In addition, advertising agencies have yet to grasp the internet as an advertising platform and local websites remain ill-equipped to handle sophisticated online ads.[35] Whereas affluent politicians are known to purchase bulk subscriptions to newspapers and magazines in order to influence coverage, online advertising remains too small of a factor to be targeted by political groups and businesses. In fact, the majority of advertising revenue continues to go to television and other traditional media, while online sources make up two percent of the total advertising market.[36] Importantly, there is no evidence of violations of net neutrality or of political manipulation in distributing ISP licenses. Similarly, there are no restrictions on who can acquire local or international domains and server space.

Civil society groups have used mobile and social media widely and effectively to mobilize support for their causes. Women's right groups, such as Nasawiya, have been successful in attracting media attention, mobilizing grassroots support, and achieving changes in discriminatory laws and regulations.[37] Their online efforts, combined with strategic litigation and advocacy, led to the implementation of tougher sentences for "honor crimes" in 2011.[38] In 2012, the group also advanced public debate on domestic violence, leading to the proposal of a law currently being discussed in parliament.[39]

In addition, civil society organizations have been successful in halting the passage of two problematic online media laws through online campaigning. Activists and businesses delayed and eventually canceled a parliamentary vote on the highly-restrictive "e-transaction law" in June

[33] Jad Melki, Yasmine Dabbous, Khaled Nasser, and Sarah Mallat. (2012). Mapping Digital Media: Lebanon, New York, NY: Open Society Foundation. http://www.soros.org/initiatives/media. pp. 21-22.
[34] Mapping Digital Media: Lebanon, pp. 56-58.
[35] Elias Sakr. (2012, April 20). Online Advertising untapped in Lebanon, The Daily Star, http://www.dailystar.com.lb/Business/Lebanon/2012/Apr-20/170785-online-advertising-untapped-in-lebanon.ashx
[36] Sakr, "Online Advertising Untapped in Lebanon."
[37] Jad Melki and Sara Mallat. (2013). Digital Activism: Efficacies and Burdens of Social Media for Civic Activism in Lebanon. Unpublished manuscript.
[38] Human Rights Watch. (2011). Lebanon: Law reform targets 'honor' crimes. http://www.hrw.org/news/2011/08/11/lebanon-law-reform-targets-honor-crimes.
[39] B. Anderson (2012, February 20). Lebanese demonstrate for legal protection against domestic violence. The Daily Star. http://www.dailystar.com.lb/News/Local-News/2012/Feb-20/163903-lebanese-demonstrate-for-legal-protection-against-domestic-violence.ashx.

2010.[40] In March 2012, a similar campaign to "Stop LIRA," the Lebanese Internet Regulation Act proposed by the Ministry of Information, led to a halt in deliberations on the law (for more on the e-transactions law and LIRA, please see "Violations of User Rights" below).

Online mobilization also led to the closing down of a circus that was abusing animals in 2010, as well as the advancement of animal rights legislation in 2011.[41] However, not all digital activists have been successful. One of the most publicized failures pertains to the ongoing anti-sectarianism campaign, which took off in 2011 and so far has not achieved any of its goals and has failed to mobilize a critical mass of supporters in the country.[42] Failures in this domain, however, were not related to censorship, but rather to organizational challenges.

VIOLATIONS OF USER RIGHTS

The Lebanese constitution guarantees freedom of expression as well as freedom of the press, although those rights have not always been respected in practice. Violations of press freedom typically receive an immediate and passionate reaction from the public, serving as a powerful check against the government's actions in this domain. However, no specific provisions in these pre-internet era laws relate to online speech, and many have been anticipating a new law for over a decade. Meanwhile, courts apply these and other traditional media laws to the online sphere in an inconsistent and often contradictory fashion.[43] This has produced a confusing legal environment with overlapping jurisdictions and contradictory laws governing online content, including the civil laws, the penal code, the Publications Law, the Audiovisual Law, the elections law, and the military code of justice.[44] Three serious attempts to develop new media laws have generated heated national debates in the past three years, although so far, none have generated any concrete results.[45]

Firstly, the e-transactions law, proposed in 2010, required "anyone providing online services" to apply for a license, allowed for "warrantless search and seizure" of information and equipment, and proposed a licensing and regulatory body with broad unchecked powers over e-commerce companies.[46] In early 2012, the Ministry of Interior proposed the Lebanese Internet Regulation Act (LIRA), which applied the archaic 1962 Press and Publications Law to websites and their employees.[47] Although LIRA was seen as less problematic than the e-transactions law, it included

[40] S. Malo. (2010, August 23). Where online activism meets offline action. The Daily Star. http://www.dailystar.com.lb/Spotlight/Aug/23/Where-online-activism-meets-offline-action.ashx.
[41] B. Al-Quntar. (2011, November 25). Animal rights law heads to Parliament. Al-Akhbar.
[42] Simona Sikimic. (2011, May 16). Laique demonstrators call for secular state. The Daily Star. http://www.dailystar.com.lb/News/Local-News/2011/May-16/Laique-demonstrators-call-for-secular-state.ashx.
[43] Jad Melki, Yasmine Dabbous, Khaled Nasser, and Sarah Mallat. (2012). Mapping Digital Media: Lebanon, New York, NY: Open Society Foundation. http://www.soros.org/initiatives/media. p. 86.
[44] Mapping Digital Media: Lebanon, p. 86.
[45] Media Sustainability Index. (2010/2011). The development of sustainable independent media in Lebanon. http://www.irex.org/project/media-sustainability-index-msi-middle-east-north-africa.
[46] Social Media Exchange. (2010, June 14). Tage archives: E-transactions law. http://www.smex.org/tag/e-transactions-law.
[47] OnterNet Blog. (2012, March 19). L.I.R.A: Minister's v/s Legal Point of View. http://blog.ontornet.org/?p=335.

enough vague language and restrictions to evoke fears of broad censorship.[48] For example, LIRA prohibited the publishing of "immoral content," including matters related to gambling, and did not define which websites were defined as "information websites" and thus were required to register.[49] LIRA also prohibited users from managing more than one website at a time and banned anyone convicted of a "heinous misdemeanor or felony" from owning one altogether. As mentioned, both the e-transactions law and LIRA were halted under public pressure. [50]

In contrast, the law recently proposed by Maharat Foundation was drafted through engagement with various ICT stakeholders and attempts to uphold democratic rights.[51] Nevertheless, the Maharat proposal has garnered some resistance, mainly from the Lebanese Press Federation, which sees it as a threat to its authority.[52] In contrast to the two previously mentioned bills, the Maharat law attempts to regulate print, broadcast, internet, and mobile media, thereby unifying the two main laws that currently regulate the media industry: the 1962 press and publications laws and the 1994 audiovisual law. The Maharat law also abolishes provisions that currently allow for the precautionary detention of journalists "convicted for libelous violations," and removes the distinction between political and non-political media, and no longer requires newspapers to obtain a license.[53] As of mid-2013, the law was under discussion in the Lebanese parliament's telecommunications committee.

From a legal perspective, the most serious threat to internet users and online journalists remains the country's slander and libel laws. Under Article 588 of the Lebanese penal code, defaming the president carries a sentence of 3 to 12 months, while defaming the army or other public figures carries a sentence of up to 6 months.[54] The appeals process is often drawn out and highly politicized. In practice, however, most online users targeted with such accusations are quickly released and the cases are usually forgotten or dropped under public or political pressure. However, even if the cases tend to wither away with little or no legal action, they almost always generate heated public debates and protests. In the recent past, a handful of cases caught the attention of the media and wider public.

On February 5, 2013, local blogger Abir Ghattas was summoned to an International Security Forces (ISF) police station and interrogated for an hour about a blog entry she posted four weeks prior.[55] She had been sued by the former CEO of Spinneys, a local supermarket chain, for defamation after she criticized his handling of the attempted unionization of his company's workers.

---

[48] Jillian York. (2012, April 2). Proposed Laws in Lebanon and Iraq Threaten Online Speech. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2012/03/proposed-laws-lebanon-iraq-threaten-online-speech.
[49] OnterNet Blog. (2012, March 19). L.I.R.A: Minister's v/s Legal Point of View. http://blog.ontornet.org/?p=335.
[50] Samir Kassir eyes. (2012, April 11). Activists, Bloggers Stop Lebanese Internet Regulation Act, for Now. http://www.skeyesmedia.org/en/a/Articles/Activists-Bloggers-Stop-Lebanese-Internet-Regulation-Act-for-Now.
[51] Article 19. (2009). Draft Law Amending the Press Law of Lebanon. http://www.article19.org/pdfs/analysis/lebanon-amending-the-press-law-of-lebanon.pdf.
[52] The Daily Star. (2013, April 24). Maharat lashes back at Press Federation over draft law. http://www.dailystar.com.lb/News/Local-News/2013/Apr-24/214825-maharat-lashes-back-at-press-federation-over-draft-law.ashx.
[53] The Daily Star, "Maharat lashes back at Press Federation over draft law"
[54] See: http://www.lebarmy.gov.lb/article.asp?ln=ar&id=25540.
[55] Maharat Foundation. (n.d.).Blogger Abir Ghattas forced to delete a post on her blog. http://maharatfoundation.org/?p=1328.

Abir stated she was ordered to sign a pledge that she would not harass Spinneys in the future.[56] She also received a phone call several hours later from the station's commander requesting that she remove the post or "else she will be summoned again."[57] Frustrated with the idea of returning to the police station for a fourth time in only a few months, eventually she removed the title and body of her blog entry and replaced them with the message: "Due to censorship and limitation of freedom of speech, the content of the blog post written on Jan 10, 2013 titled: Michael Wright, Spinneys CEO No More, was forcibly removed."[58] Several Lebanese bloggers took a snapshot of Ghattas' original text before she removed it and posted the article on their blogs.[59] Thus far, she has not been called back to court and the case will mostly likely fade away with no clear court decision, like other similar cases. In an interview, Ghattas noted that her experience was an unusual occurrence in Lebanon.[60]

A similar case pertains to the arrest and beating of Pierre Hashash on November 21, 2012, due to comments he made on Facebook in which he complained about the heavy amount of traffic in a roundabout holding the name of an army commander. The beating of Hashash, a rap artist and former independent candidate for parliament, caught wide media attention, and he was released one week later with no charges filed.[61]

On June 29, 2010, three Lebanese citizens, Naim Hanna, Antoine Ramya, and Chibl Kasab, were accused of defaming the president after they criticized him on a pro-president Facebook group.[62] Their comments were quickly removed from the Facebook group, which was also closed—assumingly by the group manager. Their arrests triggered a storm of tweets, blogs, and online petitions. While they were released on bail for a fee of $66 each, their cases remain pending and the charges will most likely be forgotten.[63] While other cases may exist, they are seldom reported or are difficult to verify. For example, the popular Lebanese blogger Imad Bazzi stated that he and six other bloggers were arrested, interrogated, and intimidated several times between 2005 and 2010, although evidence is not clear.[64]

Stories of extralegal methods used to identify anonymous online users also abound. These cases tend to be low profile and are often underreported out of fears of public embarrassment or due to government intimidation. One well-publicized case from 2000 pertains to gaylebanon.com, a pro-LGBTIQ rights website. Lebanese vice police tried to force Ziad Mughraby, the owner of the local ISP "Destination" and son of a human rights lawyer, to reveal the names of the website's owners.

---

[56] Ibid.
[57] Ibid.
[58] Abir Ghattas. (2013, January 10). **Title removed**. http://abirghattas.com/michael-wright-spinneys-ceo-no-more-2/.
[59] Ritakml.info. (2013, February 6). http://ritakml.info/2013/02/06/abir-ghattas-has-the-right-to-disagree-with-a-persons-actions.
[60] Interview with Abir Ghattas, Beirut, 11 March 2013.
[61] Annahar. (2012, December). Report: Military Court Releases Pierre Hashash Without Any Charges. http://www.naharnet.com/stories/en/62317-report-military-court-releases-pierre-hashash-without-any-charges.
[62] Jad Melki, Yasmine Dabbous, Khaled Nasser, and Sarah Mallat. (2012). Mapping Digital Media: Lebanon, New York, NY: Open Society Foundation. http://www.soros.org/initiatives/media. p. 87.
[63] Ya Libnan. (2010, July 2). 3 men arrested for slandering Suleiman freed on Bail. http://www.yalibnan.com/2010/07/02/3-men-arrested-for-slandering-suleiman-freed-on-bail.
[64] Jad Melki, Yasmine Dabbous, Khaled Nasser, and Sarah Mallat. (2012). Mapping Digital Media: Lebanon, New York, NY: Open Society Foundation. http://www.soros.org/initiatives/media. p. 92.

Kamal Batal, director of the human rights organization "MIRSAD," subsequently e-mailed a letter of protest to raise awareness about the issue. Under a military tribunal, both he and Mughraby were convicted of defaming the army and forced to pay a fine of $219 each.[65]

Currently, Lebanese law does not place restrictions on online anonymity or encryption software. However, there have been reports that the draft media laws currently being debated behind closed doors in parliament do require some form of registration for news websites, similar to the LIRA proposal. Prepaid mobile phones can be easily purchased around the country without any ID requirements. However, users must submit their identity card when purchasing a mobile phone contract where payment is deferred.

The issue of surveillance has garnered much public debate and controversy in the past eight years, which witnessed devastating violence and major political shifts, including a chain of political assassinations (mainly 2005-2008), a 30-day war with Israel (2006), a small-scale civil war (2008), and a political climate that continues to divide the country into two large blocks: the "March 14 Alliance" and the "March 8 Alliance."[66] At issue was the widespread and aggressive surveillance and private data acquisition by the Information Branch of the ISF, the United Nations International Independent Investigation Commission (UNIIIC), and the Special Tribunal for Lebanon (STL), which were responsible for investigating the assassinations, particularly that of the late prime minister Rafik Hariri in 2005.[67] The three organizations enjoyed almost free access to private data between 2005 and 2008, collecting sources as diverse as university transcripts, medical history, and mobile phone records in the name of national security. Their work was largely facilitated by Marwan Hmadeh, the ranking March 14 member and telecommunications minister from 2005 to 2008, himself a survivor of a 2004 assassination attempt.

In general, the laws regulating legal surveillance and the acquisition of communications data are vague and widely disputed. Attempts to develop clear privacy laws and regulations have failed, mainly because of their highly politicized nature. Currently, the typical process for acquiring user data involves a request from the ISF to the Ministry of Interior (or from the army to the Ministry of Defense), which is then sent to the prime minister for approval. The order is then sent to the telecommunications minister for execution—although in some instances the latter has refused to hand over the data to the ISF. This process was approved by the cabinet of ministries in 2009 as part of an agreement to share communication data with security and military officials. However, those who dispute this process, particularly the last three telecommunications ministers, cite the need to obey privacy laws and insist that the government's 2009 decision is limited to metadata and does

[65] Jad Melki, Yasmine Dabbous, Khaled Nasser, and Sarah Mallat. (2012). Mapping Digital Media: Lebanon, New York, NY: Open Society Foundation. http://www.soros.org/initiatives/media. p. 86-7.

[66] The past eight years have witnessed major shifts in Lebanese politics, which were triggered by the high-profile assassination of Prime Minister Rafic Hariri in 2005 that prompted massive protests and forced Syrian troops out of Lebanon, thereby changing the balance of power. These events created two major political camps: the March 8 Alliance that included Hezbollah and the Free Patriotic Movement, and was viewed as supportive of Syria and Iran, and the March 14 Alliance that included the Future Movement, the Progressive Socialist Party and the Lebanese Forces, and was seen as opposed to Syria and allied with the USA.

[67] The UNIIC and later the STL, which were established to investigate the assassination of Lebanese Prime Minister Rafik Hariri in 2005, were later accused of collecting private data not relevant to the investigation, including medical records from a local gynecological clinic that is frequented by the wives of many Hezbollah members.

not cover requests for the content of communications transactions and other specific data. During their respective periods in office, the ministers argued that large-scale, broad requests from the ISF should be accompanied by a court order. As a result, the three ministers have had conflicts with the ISF and Prime Minister Najib Mikati,[68] who had struggled to appease both sides and present himself as an independent leader.[69] The politicization of these issues and the failure of any attempts to institute clear regulations remain the most serious problems when it comes to online privacy protection.

The conflict reached its peak in December 2012 when Sehnaoui, the current telecommunications minister, stated through his Facebook page that he had rejected an ISF request dating from October 17, 2012.[70] Writing on his Facebook page in December, current telecommunications minister Nicolas Sehnaoui revealed that the ISF had requested an expansive amount of information on Lebanese citizens for a two-month period of time. The request, based on an investigation into the assassination of a former intelligence chief, included the following information: users' real names, phone numbers, addresses, usernames, passwords, IP addresses, and browsing history, as well as logs for e-mails, chatting services, discussion forums, VoIP applications, and social media.[71] In his Facebook post, the minister called upon "all bloggers, e-journalists, Tweeters and Facebook users and all members of our social media community" to pressure the council of ministers to reject the ISF request.[72] The minister had previously rejected similar requests and even sent a delegation of legal experts to France to discuss the legality of such requests.[73] The debate has addressed the legality of the ISF's right to access the content of text messages, rather than only call records and location data.[74] However, some have doubted the validity of the minister's claims and interpreted it as part of the broader dispute between the ISF, the ministry, and their respective political factions, which have occurred several times over the past years.[75]

In addition, reports of Israeli attempts to infiltrate Lebanon's telecommunications system abound. Over the past four years, several employees working for mobile and fixed phone operators were arrested for allegedly carrying out clandestine intelligence activities for Israel.[76] There were also numerous reports about spying devices discovered on the network.[77] Moreover, attempts by the

[68] Sami Halabi. (2011, July 3). Redialing discord. Executive Magazine. http://www.executive-magazine.com/economics-and-policy/Redialing-discord/4770.
[69] (Acting) Prime Minister Najib Mikati resigned March 2013, partly due to a controversy over the term extension for the ISF chief, which Mikati supported and the March 8 alliance opposed.
[70] See: http://www.facebook.com/Nicolas.Sehnaoui/posts/10152314217230285.
[71] See Hassan Chakrani. (2012, December 4). Lebanon Security Forces: Give Us Your Facebook Password. Al-Akhbar English. http://english.al-akhbar.com/print/14241, and El-Nashra. (2012, December 4). Al-Nashra unveils the documents from the information branch (ISF) requesting log files for web sites. http://www.elnashra.com/news/show/554968.
[72] See: http://www.facebook.com/Nicolas.Sehnaoui/posts/10152314217230285.
[73] Lebanese law is partly rooted in French law.
[74] Hassan Chakrani. (2012, December 4). Lebanon Security Forces: Give Us Your Facebook Password. Al-Akhbar English. http://english.al-akhbar.com/print/14241.
[75] See: http://www.dailystar.com.lb/News/Local-News/2013/Feb-21/207288-telecoms-data-requests-violate-constitution.ashx#axzz2RqKY4Jq6.
[76] Sami Halabi. (2011, July 3). Redialing discord. Executive Magazine. http://www.executive-magazine.com/economics-and-policy/Redialing-discord/4770.
[77] Sami Halabi. (2011, Jan 3). Broad band's roadblock. Executive Magazine. http://www.executive-magazine.com/special-report/Broadbands-roadblock/680.

ISF to install and operate surveillance technologies have been apparently halted recently.[78] In fact, a public debate about illegal phone lines, surveillance, and privacy ensued after the May 2011 confrontation between former minister of telecommunications Charbel Nahas and the ISF. The controversy was triggered after members of the ISF blocked the minister and his team from entering a ministry building to dismantle a non-commercial mobile network which was allegedly used by the ISF for intelligence purposes, without government sanctioning or TRA supervision.[79]

When it comes to cybercafes, operators have only a few requirements by which they must abide, pertaining to registering their business with the ministry of finance for tax purposes and ensuring that all software used in their machines is legal and licensed. Interviewed operators of cybercafes said other matters are left to their own discretion and no special requirements to aid the government exist. Customers are not obliged to identify or register and no monitoring software is installed on machines. They do, however, use firewalls and filters to block pornographic websites, particularly to protect children—a matter that caught media attention in April 2006 and led to the addition of such provisions to the proposed e-transactions law.

Cyberattacks are on the rise in Lebanon, especially those emanating from outside of the country. Over the past year, several government and news websites were attacked multiple times. For example, on April 17, 2012, a group named Raise Your Voice (RYV) simultaneously hacked 15 government websites, including the state-owned *National News Agency* and a handful of ministerial websites.[80] The same group struck again nine days later, enabling Facebook users to post comments on ten government web sites.[81] On June 16, 2012, RYV again hacked two government websites. This latter wave of attacks—seemingly initiated by a local Lebanese group—posted comments criticizing the government for their economic and developmental policies, especially in relation to the electricity shortage and the increasing poverty.[82]

More recently, on February 23, 2013, the group *Team Kuwaiti Hackers* attacked the Lebanese Parliament's website.[83] The hackers posted sectarian comments that criticized specific political groups, namely Hezbollah and the Syrian regime. Moreover, throughout 2012 and early 2013, several news reports surfaced regarding multiple sophisticated viruses that targeted Lebanese computers to infiltrate banks, the financial system, and private financial data.[84] Some experts noted

[78] Ibid.
[79] Ibid.
[80] Naharnet. (2012, April 17). 'Raise Your Voice' Hacks 15 Lebanese Government Sites. http://www.naharnet.com/stories/en/37035.
[81] Naharnet. (2012, April 26). RYV Hacks Lebanese Govt. Sites Again, Enables Facebook Users to Post Messages. http://www.naharnet.com/stories/en/38244.
[82] Justin Salhani. (2012, June 6). Two Lebanese government websites hacked. The Daily Star. http://www.dailystar.com.lb/News/Local-News/2012/Jun-16/177091-two-lebanese-government-websites-hacked.ashx.
[83] The Daily Star. (2013, February 23). Lebanese Parliament website hacked. http://www.dailystar.com.lb/News/Local-News/2013/Feb-23/207634-lebanese-parliament-website-hacked.ashx.
[84] Stephen Dockery. (2012, August 11). Virus plunges Lebanon into cyber war. The Daily Star. http://www.dailystar.com.lb/News/Local-News/2012/Aug-11/184234-virus-plunges-lebanon-into-cyber-war.ashx, and SecureList. (2012, August 10). Gauss: Abnormal Distribution. http://www.securelist.com/en/analysis/204792238/Gauss_Abnormal_Distribution.

that the attacks may have been state-sponsored and aimed at disrupting Syrian and Iranian finances.[85]

The news industry has also been a popular target of such attacks. The most significant has been the hijacking of *al-Mustaqbal* newspaper's home page on April 10, 2013. In a politically motivated attempt to discredit the Special Tribunal for Lebanon (STL), hackers posted the names of alleged witnesses in the Rafik Hariri assassination trial.[86] Other attacks have mainly attempted to overload news websites, such as those against the websites of Now Lebanon (January 19, 2012), NBN TV (February 4, 2012), al-Kifah al-Arabi (March 19, 2012), Murr TV (January 2013 and April 16, 2013), OTV (July 28, 2012), al-Mayadeen TV (August 23, 2012), *Annahar* newspaper (October 15, 2012), [87] and *Arrouwad* newspaper (April 2013).[88] Some journalists' personal web sites and social media pages have also suffered from such attacks, such as Mona Abou Hamzeh's Facebook page (May 15, 2012), Rouaida Mroueh's website (March 24, 2012), and Paula Yacoubian's Facebook page (January 18, 2013).[89]

Many of these cyberattacks are dealt with promptly, though the perpetrators are seldom identified and detained. In one reported incident, the Lebanese Cyber Crime and Intellectual Property Rights Bureau Unit, which belongs to the ISF, apprehended two Lebanese hackers accused of breaking into e-mails and Facebook accounts, stealing their owners' identities, and blackmailing them for ransom.[90] The increase in similar hacking attacks and blackmail attempts has alarmed Lebanese security officials, who remain poorly equipped to deal with them.[91]

There have been relatively fewer attacks on the websites of political parties, civil society groups, and activists in Lebanon, despite their large numbers and the controversial issues they champion. Such incidents include the attacks on the websites of Lebanese Press Photographers (April 14, 2012), the Mohammad Hussein Fadlallah Foundation (April 16, 2012), the Palestinian Human Rights Foundation (June 15, 2012), and the Lebanese Parliamentary Monitor (November 26, 2012).[92] Most recently, the Lebanese Dental Association's website was hacked and the attackers posted the Israeli flag on the homepage.[93] Such cyberattacks are likely to increase in the near future and take on a more significant political role, especially if the situation in Syria continues to deteriorate or in the case of military conflict with Israel.

---

[85] Al-Monitor. (n.d.). Cyber attack on Lebanese banks: Are Iran, Syria finances target? http://www.al-monitor.com/pulse/iw/contents/articles/opinion/2012/al-monitor/a-cyber-attack-against-lebanese.html.
[86] The Daily Start. (2013, April 12). Al-Mustaqbal, STL take action over hacking incident. http://bit.ly/1bNHYJa.
[87] See: http://blogbaladi.com/annahar-releases-mobile-app-and-gets-hacked.
[88] Samir Kassir eyes. (2013, April 15). Arrouwad's Website Hacked twice in two days. http://www.skeyesmedia.org/ar/News/Lebanon/3073.
[89] For a more exhaustive list, please see: http://www.skeyesmedia.org.
[90] LBC International. (2012, January 9). Facebook and email hackers arrested in Lebanon. http://www.lbcgroup.tv/news/16230/facebook-and-email-hackers-arrested-in-lebanon.
[91] Layal Kiwan. (2013, April 9). تسونامي الهجمات الالكترونية يضرب لبنان وهدف القرصنة الابتزاز المادي. Lebanon Live News. http://www.lebanonlivenews.com/idetails.php?id=12725.
[92] For a more exhaustive list, please see: http://www.skeyesmedia.org.
[93] Samir Kassir Eyes. (2013, April 12). Press and Cultural Freedom Violations January – February – March 2013 LEBANON, SYRIA, JORDAN, PALESTINE http://bit.ly/12QffiY.

LIBYA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	18	17
Limits on Content (0-35)	9	9
Violations of User Rights (0-40)	16	19
Total (0-100)	**43**	**45**

* 0=most free, 100=least free

POPULATION: 6.5 million
INTERNET PENETRATION 2012: 20 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- A Libyan court ordered Russia Today to remove libelous content from its website and temporarily blocked the news site until it cooperated (see **LIMITS ON CONTENT**).
- Media reports indicate that Qadhafi's extensive surveillance apparatus remains online and operates with little judicial oversight. State control over internet and mobile phone providers is indicative of the lack of checks and balances in the country's governance (see **VIOLATIONS OF USER RIGHTS**).
- Militia groups temporarily abducted a social media activist and threatened a British journalist into leaving the country, a sign that nonstate actors are continuing to add to the overall sense of instability and insecurity in the online media environment (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

It has now been two years since the 2011 Libyan revolution, when a popular uprising and ensuing civil war deposed the country's long-time leader, Muammar Qadhafi, and placed the country on a shaky path to democracy. Elections for the General National Council (GNC), Libya's 200-member legislative body, were held in July 2012 amidst praise from international observers.[1] The GNC elected Prime Minister Ali Zeidan, a former human rights lawyer, and confirmed his choices for cabinet in November 2012. While the composition of Libya's first democratically-elected government in 60 years is a great step forward, there are several legal and institutional challenges that require immediate attention. The actions of militias, including armed Islamist groups, offset many of the gains the government has made in removing many obstacles to internet access and limits on online content.

The internet became publicly available in Libya in 1998, though prices were excessively high and access was limited to the elite. Thousands of cybercafes sprang up after 2000, eventually offering cheap internet to both urban and rural users.[2] Furthermore, over the following decade, the state telecom operator reduced prices, invested in a fiber-optic network backbone, and expanded ADSL, WiMAX, and other wireless technologies throughout the country.[3] In its initial stages, there were few instances of online censorship in Libya.[4] However, it was not long until the Qadhafi regime began to target opposition news websites, particularly after the lifting of United Nations sanctions in 2003 led to increased access to surveillance and filtering equipment.[5] Overall, the highly repressive online environment, which included harsh punishments for any criticism of the ruling system, contributed to an extreme degree of self-censorship by internet users.[6]

Since the victory of the Libyan rebels in 2011, the online information landscape has been relatively open. The country has witnessed a flurry of self-expression as Libyans seek to make up for lost time under the Qadhafi era, resulting in an increase in news sites, the development of a market for online advertising, and massive growth in Facebook use. However, the civil war also impacted investment in the country's information and communications technology (ICT) sector, namely by inflicting damages to the infrastructure and sidelining an earlier $10 billion development plan for

[1] See "Carter Center Congratulations Libyans for Holding Historic Elections," The Carter Center, July 9, 2012, http://www.cartercenter.org/news/pr/libya-070912.html and "Libya: Final Report, General National Congress Election," European Union Election Assessment Team, July 7, 2012, http://eeas.europa.eu/eueom/missions/2012/libya/pdf/eueat-libya-2012-final-report_en.pdf.
[2] Gamal Eid, "Libya: The Internet in a conflict zone," The Arabic Network for Human Rights Information, 2004, http://www.anhri.net/en/reports/net2004/libya.shtml.
[3] "Libya – Telecoms, Mobile and Broadband," Budde.com, accessed August 21, 2013, http://www.budde.com.au/Research/Libya-Telecoms-Mobile-and-Broadband.html.
[4] Doug Saunders, "Arab social capital is there – it's young and connected," The Globe and Mail, March 5, 2011, http://www.theglobeandmail.com/news/world/doug-saunders/arab-social-capital-is-there-its-young-and-connected/article1930770/.
[5] "Libya," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/libya.
[6] Ismael Dbarra, "Internet in Libya: Everyone is rebelling against continued blocking and censorship," Elaph (Arabic), March 5, 2009, www.elaph.com/Web/politics/2009/3/415948.htm.

2020.[7] Additionally, residual self-censorship, weak legal protections, and uncertainties about the continued existence of the Qadhafi-era surveillance apparatus pose ongoing challenges to internet freedom in the country.

OBSTACLES TO ACCESS

Internet penetration has traditionally been very low in Libya. While the percentage of the population with access to the internet has quadrupled from 2007 to 2012, the latest estimates still put this amount at only 19.9 percent.[8] Of these users, an estimated 80 percent use the wireless WiMAX service, 17 percent connect using traditional fixed-lines, and 3 percent employ a fiber-optic connection.[9] The number of fixed-broadband subscriptions is relatively low, at just over 1 subscription per every 100 inhabitants in 2012.[10] However, due to the difficulties in obtaining a standard internet subscription, it should be noted that many Libyans use unregistered or illegal satellite technology to access the internet.

Compared to the relatively low internet penetration rate, mobile phone use is ubiquitous. There are an estimated 9.59 million subscriptions in Libya, representing a penetration rate of 148.2 percent.[11] Prices have dropped systematically since the introduction of a second mobile provider in 2003, resulting in greater affordability. By 2013, the price of a prepaid SIM card from the main provider, Libyana, was LYD 5 ($4). Smartphones and 3G connectivity have been available since 2006, though the prohibitive cost of more upscale models impedes their wider dissemination.[12]

Similarly, the cost of a home internet connection remains beyond the reach of a large proportion of Libyans, particularly those living outside major urban areas. As of early 2013, a dial-up internet subscription cost LYD 10 per month ($8), an ADSL subscription was LYD 20 ($16) for a 7 GB data plan, and WiMAX was LYD 40 ($31) for a 10 GB data plan, after initial connection fees. By comparison, gross national income per capita was only $1,078 per month, pushed up by relatively high salaries in oil and gas firms.[13] The LTT announced a plan to decrease the prices of leased lines up to 45 percent starting from August 2012 to coincide with the month of Ramadan.[14] The LTT also decreased initial WiMAX account connection fees for individual users from LYD 160 ($124) to

[7] "Libya – Telecoms, Mobile and Broadband," Budde.com, accessed August 21, 2013, http://www.budde.com.au/Research/Libya-Telecoms-Mobile-and-Broadband.html.
[8] "Percentage of individuals using the Internet," International Telecommunications Union, 2012, accessed August 19, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[9] Tom Westcott, "Improving Libya's Internet Access," *Business Eye*, February 2013, pp. 18, available at http://www.libyaherald.com/business-eye-issue-1-february-2013-2/.
[10] "Fixed (wired-) broadband subscriptions," International Telecommunications Union, 2012, accessed August 19, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[11] "Mobile-cellular subscriptions" International Telecommunications Union, 2011.Available at http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[12] "Libyana Introduces 3G Services for First Time in Libya," The Tripoli Post, September 26, 2006, http://www.tripolipost.com/articledetail.asp?c=2&i=311.
[13] "Libya – World Development Indicators" The World Bank, accessed August 21, 2013, http://data.worldbank.org/country/libya#cp_wdi.
[14] "Discounts up to 45% in the service of custom fonts," [in Arabic] Libya Telecom & Technology, http://www.ltt.ly/news/d.php?i=206, accessed July 23, 2013.

LYD 120 ($93) and from LYD 260 ($202) to LYD 220 ($171) for households.[15] As of the first quarter of 2013, a dial-up internet subscription cost LYD 10 per month ($7), an ADSL subscription was LYD 20 ($15) for 20GB, and WiMAX was LYD 30 ($23) for 15GB. WiMAX modems remain in short supply since February 2012, resulting in high prices for second-hand devices sold on the site Open Souk, Libya's online marketplace.[16]

Many foreign and Libyan organizations and individuals in need of a reliable and legal internet service contract have been driven towards "two-way" satellite internet technology. As two-way technology has become more popular, connection fees and equipment costs have been lowered. Prices are now at LYD 800 ($622) for the hardware and a monthly subscription costs LYD 255 ($198) for a fast connection and 30 GB bundle, depending on the number of users.[17]

The Libyan civil war heavily disrupted the country's telecommunications sector, with the damage estimated at over $1 billion.[18] Upgrades have been projected in an effort to respond to demands for increased capacity, such as the laying of the European Indian Gateway and Silphium submarine cables,[19] the construction of additional WiMAX towers,[20] the creation of Wi-Fi hotspots, the installation of a long distance fiber-optic cable within the country,[21] and the development of next generation broadband.[22] The adult literacy rate is 89 percent and a wide range of websites and computer software is available in Arabic.[23] However, limited computer literacy, particularly among women, has been an obstacle to universal access.

Since there have been little improvements to ICT equipment since the Qadhafi era, internet speeds remain extremely slow at an average speed of less than 256Kbps, prompting frustrated Libyans to create the Facebook page titled, "I hate Libyan Telecom and Technology," which has reached over 19,000 followers.[24] IT experts familiar with the issue have cited poor infrastructure, a lack of quality of service, technology constraints and continued lack of regulations. Furthermore, broadband is not widely available, bandwidth limitations exist for fixed-line connections, wireless users face slower speeds due to heavy congestion during peak hours, and there is a general lack of resources and personnel to perform maintenance and repairs.[25]

---

[15] "Now, Libya Max service from Libya Telecom and Technology worth 120 dinars for personal rather than 160," [in Arabic] Libya Telecom & Technology, http://www.ltt.ly/news/d.php?i=188, accessed July 23, 2013.
[16] See http://ly.opensooq.com/ or https://www.facebook.com/OpenSooq.Libya it even has a mobile app now.
[17] See http://www.giga.ly/ or https://www.facebook.com/Giga.ltd
[18] "Libya – Telecoms, Mobile and Broadband," Budde.com, accessed August 21, 2013, http://www.budde.com.au/Research/Libya-Telecoms-Mobile-and-Broadband.html.
[19] "The Activation of The New Upgraded Submarine Cable System between Libya and Italy," The Tripoli Post, December 25, 2011, http://www.tripolipost.com/articledetail.asp?c=11&i=7562.
[20] "ZTE suggest Libya will boast nationwide WiMAX network by Aug-13," TeleGeography, January 24, 2013, http://www.telegeography.com/products/commsupdate/articles/2013/01/24/zte-suggests-libya-will-boast-nationwide-wimax-network-by-aug-13/.
[21] "Italian Company to Install Fiber-Optic Network," Libya Business News, September 29, 2012, http://bit.ly/RbnhMm.
[22] Tom Westcott, "Improving Libya's Internet Access," *Business Eye*, February 2013, pp. 18, available at http://www.libyaherald.com/business-eye-issue-1-february-2013-2/.
[23] "Literacy rate, adult total (% of people ages 15 and above)," The World Bank, accessed August 21, 2013, http://data.worldbank.org/indicator/SE.ADT.LITR.ZS/countries.
[24] See https://www.facebook.com/ihateltt
[25] Interview with ex-Libyana IT engineer on March 2013.

Qadhafi's forces strategically limited access to the internet and mobile phones during the civil war, with general access restored in August 2011.[26] Since the end of the conflict, there have been no government-imposed restrictions on connectivity, but problems remain due to damaged infrastructure. Since May 2012 there have been several disruptions to service, such notably a 26-hour cut in the entire Eastern region in June 2012[27] and cuts in areas of Tripoli during in July 2012.[28] Rolling blackouts continued over the past year, particularly due to an overload in electricity demand during summer and winter months, when air conditioning or heating is used. These blackouts are due, in part, to damage to the electricity grid that occurred as a result of the civil war, estimated at $1 billion.[29]

The state-run Libyan Post Telecommunications and Information Technology Company (LIPTC), formerly the General Post and Telecommunications Company (GPTC), is the main telecommunications operator and is fully owned by the government. In 1999, the GPTC awarded the first internet service provider (ISP) license to Libya Telecom and Technology (LTT), a subsidiary of the state-owned firm. At least seven other companies—including Modern World Communication, Alfalak, and Bait Shams—have also been licensed to provide internet services, though LTT retains sole control over Libya's international gateway to the internet.[30] The LIPTC owns two mobile phone providers, Almadar and Libyana, while a third provider, Libya Phone, is owned by the LIPTC's subsidiary, LTT.

Since the revolution, most people access the internet from their homes and workplaces (particularly those working for foreign organizations or companies), followed by mobile phones, and hotel lobbies. The cybercafe industry, quasi-decimated in many parts of Libya during the conflict, is starting to return to profitable business through catering mainly to foreign workers and Voice over Internet Protocol (VoIP) calls.

The post-conflict regulatory environment remains very unclear. The newly elected government has a Ministry of Communication, but it has expressed no clear vision for the future. During the Qadhafi era, decisions on licensing were made by the government-controlled GPTC. There was talk in 2006 surrounding the creation of a new regulator, the General Telecom Authority (GTA), though after the 2011 uprising, it remained unclear whether the GTA had come into existence. Some suspected the GTA had been formed to oversee the monitoring of online activities.

---

[26] "Project Cyber Dawn v1.0, Libya," The Cyber Security Forum Initiative, April 17, 2011, p. 20,http://www.unveillance.com/wp-content/uploads/2011/05/Project_Cyber_Dawn_Public.pdf

[27] "Internet service back in each of the following areas," [in Arabic] Libya Telecom & Technology, http://www.ltt.ly/news/d.php?i=200, accessed July 23, 2013.

[28]"Internet service outages and Libya iPhone spare result in optical fiber," [in Arabic] Libya Telecom & Technology, http://www.ltt.ly/news/d.php?i=203, accessed July 23, 2013.

[29] "Cost of last year's damage to electricity industry put at $1bn," The Libya Herald, March 28,2012, http://www.libyaherald.com/cost-of-last-years-damage-to-electricity-industry-put-at-1-bn/.

[30] United Nations Economic Commission for Africa, "The Status of Information for Development Activities in North Africa," (paper presented at the twentieth meeting of the Intergovernmental committee of experts, Tangier, Morocco, April 13-15, 2005), http://www.uneca.org/na/Information.pdf;"Internet Filtering in Libya – 2006/2007," OpenNet Initiative, 2007,http://opennet.net/studies/libya2007; "Telecoms in Libya"[in Arabic], Marefa.org, accessed August 30, 2012, http://bit.ly/1bhJYKc.

LIMITS ON CONTENT

The Libyan web has opened up extensively since the fall of Qadhafi in August 2011. The online media landscape quickly developed as restrictions and regulations on publishing dissipated during the extended period of instability. As internet use has increased, so has the market for online advertising, contributing to the overall expansion of Libyan news sites and online services. Facebook in particular has become an important news source for many Libyans. Under the various transitional and interim governments, censorship remained low and sporadic. Over the past year, however, there have been a few cases of the state blocking content for political reasons. Moreover, habits from decades of oppressive rule and the continued threat posed by militias contribute some degree of self-censorship among users, particularly on sensitive subject areas. These concerns presented some limits on content over the past year, although it is still too early to tell what direction Libya is moving during this highly-fluid, uncertain transitional period.

Web 2.0 services such as YouTube, Facebook, Twitter, and international blog-hosting platforms are freely accessible in Libya. In fact, the "Innocence of Muslims" film that sparked protests outside the American consulate in Benghazi was not blocked by Libyan authorities, although it was made inaccessible by YouTube's parent company, Google. Facebook was inaccessible for at least one day in November 2012, although the LTT was quick to explain on its website that this was not the result of state censorship but rather a glitch from the company.[31] While the defeat of the Qadhafi regime led to a cessation of state blocking in August 2011, many Qadhafi-era government webpages containing information on laws and regulations from before the uprising are inaccessible, as is the online archive of the old state-run Libyan newspapers. Some of these websites may have become defunct after the officials running them were ousted or hosting fees were left unpaid, but others were likely taken down deliberately when the revolutionaries came to power.

As mentioned, there have been some instances of blocking recorded during the coverage period. For example, the website of the television channel Russia Today (RT) was inaccessible in Libya in early March 2013. RT had posted an interview with Mahmoud Jibril, head of the National Forces Alliance, in which it was alleged that Libya's last Prime Minister under Qadhafi, Baghdadi al-Mahmoudi, was tortured in custody by government authorities after his recent extradition from Tunisia.[32] The Ministry of Communications and Information Technology actually confirmed that RT was blocked on their Facebook page, as well as the blocking of another website called Makala.[33] The English site of RT was later unblocked, although as of March 2013, the Arabic version could only be accessed through a cached copy or proxy.

[31] "Reasons for the stop of social networking site Facebook," [in Arabic] Libya Telecom & Technology, http://www.ltt.ly/news/d.php?i=215, accessed July 23, 2013.
[32] Chris Stephen and Luke Harding, "Libya's former PM Mahmoudi 'tortured' on forced return to Tripoli," The Guardian, June 27, 2012, http://www.guardian.co.uk/world/2012/jun/27/libya-mahmoudi-tortured-return-tripoli.
[33] See post by the Ministry of Communications and Informatics – Libya [in Arabic], https://www.facebook.com/cim.gov.ly/posts/403340369762444.

Some pornographic websites are also among those that continue to be blocked since the end of hostilities, according to a decision made by an ad hoc Temporary Steering Committee formed after the liberation of Tripoli. The committee is formed of conservative rebel fighters in a bid to be seen as the guardians of public morality. Prior to the war, "indecency" was prohibited but sexually-explicit sites were never blocked. This development has not yet been reversed by the LTT, perhaps due to the conservative outlook of some political factions vying for influence in the future of Libya. There is little transparency and no legal framework related to the blocking of websites in Libya, as the regulations have not yet been formulated. Technically, all regulations of the Qadhafi era remain valid.

Though the environment has loosened considerably since Qadhafi, a sizable number of Libyan bloggers, online journalists and ordinary citizens continue to practice some degree of self-censorship due to continued instability and the uncertain political situation.[34] Under the newly elected government, visas for foreign journalists have become more difficult to obtain. In January 2013, through a picture she posted on Twitter, a *Washington Post* reporter revealed that she had been made to sign a written pledge not to portray the country in a manner that might be provocative or distort civil peace.[35] In addition, given the already tense and violent environment, many bloggers and individuals choose not to comment on social taboos such as rape or conflicts between warring tribes and cities. Online writers also shy away from expressing religious opinions for fear of being marked as an atheist or a Shiite sympathizer, both of which can be life threatening. Many also avoid publishing content critical of the 2011 revolution. It should be noted that many commentators are more afraid of retribution from armed groups and non-state actors rather than the government. Such unseen pressures contribute to an atmosphere of self-censorship and incomplete freedom.[36]

Despite these trends, an increasing number of bloggers have demonstrated a willingness to use their real name when posting online. Blogging first emerged in Libya in 2003. While even Qadhafi launched his own blog in 2006, the number of blogs based inside the country remained low compared to other Arab countries.[37] Since the start of the revolution in February 2011, however, the contingent of blogs written by those inside Libya has notably increased and many Libyans have focused on topics related to political activism. Bloggers, online journalists, and other users have vocally expressed a diverse range of visions for the post-Qadhafi political order, the interim government, and other topics.

After decades of harsh censorship, the online media landscape in Libya is now diverse, with few dominant news providers and many local or privately-owned outlets. The online advertising market is also growing in the country, allowing independent news sites, such as the Libya Herald, to

[34] "2013 World Press Freedom Index: Dashed Hopes After Spring," Reporters Without Borders, http://en.rsf.org/press-freedom-index-2013,1054.html, last accessed in March 2013.
[35] See https://mobile.twitter.com/ahauslohner/status/293706323747557377/photo/1
[36] Tracey Shelton, "Libya's media has its own revolution," Global Post, March 18, 2012, http://mobile.globalpost.com/dispatch/news/regions/africa/120301/libya-media-revolution-newspapers-television-radio-journalism-free-speech.
[37] Claudia Gazzini, "Talking Back: How Exiled Libyans use the web to push for change," Arab Media Society, February, 2007, 3, http://www.arabmediasociety.com/articles/downloads/20070312142030_AMS1_Claudia_Gazzini.pdf.

generate money more than one year after its founding. Websites related to the Amazigh (whose language was banned under Qadhafi) and other minorities are now flourishing. Interestingly, Facebook is often the platform of choice for city and even government officials to publish updates and official communication. From April 2012 to April 2013, the number of Facebook users in Libya increased from some 400,000 to 860,000.[38] The social networking site was the most visited website in the country and has also become the main source of news about Libya for a large number of users inside and outside the country.[39]

In 2012 and early 2013, Facebook, Twitter and other digital media were used to mobilize Libyans for activism around a variety of causes. For example, on March 14, 2013, activists coordinated protest in Tripoli and at Libyan embassies around the world to protest violence against women. Social media had been crucial in bringing attention to numerous cases of sexual harassment against terminally ill hospital patients in Libyan hospitals. In addition, social media was a factor in the September 21, 2012 protests in Benghazi, in which over 30,000 Libyans expressed their anger at the continued presence of armed militias, including the terrorist group Ansar al-Shariah, and demonstrated their solidarity with the United States for the killing of the American Ambassador J. Christopher Stephens and two American guards during the storming of the US consulate in Benghazi on September 11.[40] In another example of how the internet is being used to engage citizens, the host of the popular TV show called Libya Tonight[41] held an interactive discussion with Facebook followers during a media training session at the American University in Cairo in March 2013.[42] Mass text message campaigns were also used to rally support in the run-up to the July 2012 elections and for a number of other announcements.

VIOLATIONS OF USER RIGHTS

Freedom of opinion, communication, and press are guaranteed by Libya's Draft Constitutional Charter, released by the Libyan Transitional National Council in September 2011 to outline Libya's governance during the transitional and interim period following the fall of the Qadhafi regime.[43] The formation of a committee to draft the new constitution has been delayed numerous times, as Libya searches for stability and rule of law in the post-conflict period. Legal reforms are essential to ensure that the rights enshrined in the draft charter are implemented. Although it has now been two years since Qadhafi's ouster, scars from his 42-year rule linger in the national psyche. Restrictive laws remain on the books and a murky surveillance apparatus continues to function with little judicial oversight. The gravest threat to user rights, however, are the country's armed groups.

[38] Libya Facebook Statistics," Socialbakers, accessed April 10, 2012, http://www.socialbakers.com/facebook-statistics/libya, and Ghazi Gheblawi, "Free speech in post-Gaddafi Libya," Index on Censorship, April 2013, http://www.indexoncensorship.org/2013/04/freedom-of-speech-in-libya/.
[39] "The Top Sites in Libya," Alexa, accessed April 10, 2012, http://www.alexa.com/topsites/countries/LY.
[40] Suliman Ali Zway and Kareem Fahim, "Angry Libyans Target Militias, Forcing Flight," The New York Times, September 21, 2012, http://www.nytimes.com/2012/09/22/world/africa/pro-american-libyans-besiege-militant-group-in-benghazi.html?_r=0.
[41] See https://www.facebook.com/LIC.LibyaTonight
[42] See http://on.fb.me/19GODzU.
[43] "Draft Constitutional Charter for the Transitional Stage," Libyan Transitional National Council, September 2011, available at http://www.refworld.org/docid/4e80475b2.html.

A British journalist writing for a Libyan news site was chased out of the country by Islamist fighters after exposing the group's "kill list," consisting of senior security officials.

During the Qadhafi era, several laws provided for freedom of speech, but these protections were typically offset by vague language restricting the same freedoms. For example, the 1969 Libyan Constitutional declaration and the 1988 Green Charter for Human Rights both guarantee freedom of speech and opinion but also note that these must be "within the limits of public interest and the principles of the Revolution."[44] Discussions over a new press law in 2007 and a telecommunications law in 2010 did not progress and were not implemented.[45] Since 2012, the judiciary has become increasingly independent, although all state bodies are still subject to pressure from the armed militias that defeated Qadhafi. For example, in April 2013, rebel fighters key to the removal of Qadhafi besieged the justice and foreign ministries to demand the passing of the Isolation Law, a bill that outlawed former Qadhafi officials from public life.[46]

Laws from the Qadhafi era remain on the books, including measures that provide for harsh punishments for those who published content deemed offensive or threatening to Islam, national security, territorial integrity, or the reputation of Qadhafi. The penal code calls for imprisonment or the death penalty for anyone convicted of disseminating information critical of the state or the "Leader of the Revolution." The 1972 Publications Act imposes fines and up to two years in prison for a variety of violations, including libel, slander, and "doubting the aims of the revolution."[47] Particularly egregious was a law on collective punishment, which allowed the authorities to punish entire families, towns, or districts for the transgressions of one individual.[48] Because of their vague wording, these laws could be applied to any form of speech, whether transmitted via the internet, mobile phone, or traditional media. A 2006 law mandates that websites registered under the ".ly" domain must not contain content that is "obscene, scandalous, indecent or contrary to Libyan law or Islamic morality."[49] Under Qadhafi's rule, several internet users and online journalists were detained, prosecuted, and in some cases, killed, for disseminating or accessing information deemed undesirable by the regime.

Although there is less fear of government repression in the post-Qadhafi era, threats still remain, particularly with so few mechanisms to hold the government or militias accountable should they abuse their power. George Grant, the British journalist who worked for the online publication the Libya Herald, was forced to flee Libya in January 2013 following alleged threats from Islamists, according to his tweets and an interview with the BBC.[50] One month earlier, Grant had written an

---

[44] IREX, "Media Sustainability Index – Middle East and North Africa," *Media Sustainability Index 2008* (Washington D.C.: IREX, 2008), 27, http://www.irex.org/system/files/MENA_MSI_2008_Book_Full.pdf.
[45] IREX, "Media Sustainability Index – Middle East and North Africa," *Media Sustainability Index 2006/2007* (Washington D.C.: IREX, 2009), 33, http://www.irex.org/system/files/MENA%20MSI%202007%20Book.pdf.
[46] Rana Jawad, "Why Libya's militias are up in arms," BBC News, April 30, 2013, http://www.bbc.co.uk/news/world-africa-22361101.
[47] Freedom House, "Libya," *Freedom of the Press 2011*, http://www.freedomhouse.org/report/freedom-press/2011/libya.
[48] IREX, "Media Sustainability Index – Middle East and North Africa," *Media Sustainability Index 2005* (Washington D.C.: IREX, 2006), 36, http://www.irex.org/system/files/MENA_MSI_2005-Full.pdf.
[49] "Internet Filtering in Libya – 2006/2007," OpenNet Initiative, and "Regulations," Libya ccTLD, accessed August 30, 2012, http://nic.ly/regulations.php.
[50] See http://www.facebook.com/video/video.php?v=10100408892583391

article regarding a suspected "death list" of senior security officials, drawn up by Islamist fighters seeking to undermine the state security presence in Benghazi.[51] In another example, the Libyan online activist Hamid al-Tubuly was reportedly abducted in December 2012 by members of the Supreme Security Council, a non-state militia, who released him only after a direct plea by the head of the GNC.[52] However, it was also rumored that al-Tubuly was not targeted for his online activism but rather because the militia wanted to take possession of his house.

The Qadhafi regime had direct access to the country's DNS servers and engaged in widespread surveillance of online communications. State of the art equipment from foreign firms such as the French company Amesys[53] and possibly the Chinese firm ZTE were sold to the regime, enabling intelligence agencies to intercept communications on a nationwide scale and collect massive amounts of data on both phone and internet usage.[54] Correspondents from the *Wall Street Journal* who visited an internet monitoring center after the regime's collapse reportedly found a storage room lined floor-to-ceiling with dossiers of the online activities of Libyans and foreigners with whom they communicated.[55] Extensive efforts were also made to develop the capacity to eavesdrop on Skype and VSAT connections. According to current and former staff of LTT, the government even obtained backdoor access to Thuraya satellite phones, which were widely perceived as a secure means of communication.[56] In general, Libyans must present identification when purchasing a SIM card.

While many Libyans would like to believe that such widespread surveillance has ceased, uncertainties remain over the actions of domestic intelligence agencies in the new Libya. A July 2012 report from the *Wall Street Journal* indicated that surveillance tools leftover from the Qadhafi era had been restarted, seemingly in the fight against loyalists of the old regime.[57] Others suspect that it has been activated to target those with an anti-Islamist agenda. During an interview on al-Hurra TV in March 2012, the Minister of Telecommunications stated that such surveillance had been stopped because the interim government wanted to respect the human rights of Libyans. An organization representing IT professionals in Libya refuted his remarks in an online statement, claiming those working in the telecom sector report that the surveillance system has been reactivated. Such allegations could not be independently verified, however.[58] Given the lack of an independent judiciary or procedures outlining the circumstances under which the state may

[51] For the article in question, see George Grant and Mohamed Bujenah, "Update II: Security forces arrest man in connection with Benghazi killings, four policemen killed in failed release attempt," Libya Herald, December 16, 2012, http://www.libyaherald.com/2012/12/16/security-forces-arrest-possible-faraj-drissi-assassin-sparking-reprisal-killings/.
[52] Umar Khan, "Abducted social network activist Hamid al-Tubuly hits out at the SSC, denies involvement with Mohammed Qaddafi," Libya Herald, December 11, 2012, http://www.libyaherald.com/2012/12/11/abducted-social-network-activist-hamid-al-tubuly-hits-out-at-the-ssc-denies-involvement-with-mohammed-qaddafi/.
[53] Ivan Sigal, "Libya: Foreign Hackers and Surveillance," Global Voices, October 27, 2011, http://advocacy.globalvoicesonline.org/2011/10/27/libya-foreign-hackers-and-surveillance/.
[54] Ibid.
[55] Paul Sonne and Margarent Coker, "Firms Aided Libyan Spies," The Wall Street Journal, August 30, 2011, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html.
[56] Sonne and Coker, "Firms Aided Libyan Spies."
[57] Margaret Coker and Paul Sonne, "Gadhafi-Era Spy Tactics Quietly Restarted in Libya," The Wall Street Journal, July 2, 2012, http://online.wsj.com/article/SB10001424052702304782404577488493816611850.html.
[58] "Libya Telecom" Facebook post [in Arabic], March 31, 2012 at 7:16am, https://www.facebook.com/LibyaTelecom/posts/201142566662920.

conduct surveillance, there is little to prevent the government, security agencies, or militias who have access to the equipment from resuming the practice.

During the Qadhafi era, opposition websites such as Libya Watanona, or those affiliated with the Muslim Brotherhood or minority groups such as the Amazigh, were periodically hacked. The government was widely suspected of being behind the attacks.[59] In January 2011, the opposition website al-Manara came under cyberattack after it had posted videos of early anti-Qadhafi protesters in Bayda and al-Mostakbal.[60] Periodic attacks continued in 2012 and 2013, with both pro-Qadhafi and pro-revolution pages hacked by individuals or groups unaffiliated with the government.

[59] "Internet Filtering in Libya – 2006/2007," OpenNet Initiative, 2007, http://opennet.net/studies/libya2007
[60] Amira Al Hussaini, "Libya: Gaddafi wages war on the internet as trouble brews at home, "Global Voices, January 17, 2011, http://globalvoicesonline.org/2011/01/17/libya-gaddafi-wages-war-on-the-internet-as-trouble-brews-at-home/.

MALAWI

	2012	2013
INTERNET FREEDOM STATUS	N/A	PARTLY FREE
Obstacles to Access (0-25)	n/a	16
Limits on Content (0-35)	n/a	11
Violations of User Rights (0-40)	n/a	15
Total (0-100)	**n/a**	**42**

* 0=most free, 100=least free

POPULATION: 16 million
INTERNET PENETRATION 2012: 4 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Traditional and online media restrictions relaxed under Joyce Banda, who assumed the presidency in April 2012 following the death of President Bingu wa Mutharika (see **INTRODUCTION**).
- In May 2012 the National Assembly repealed Section 46 of the penal code that had empowered the information minister to ban any publications deemed "contrary to the public interest" (see **VIOLATIONS OF USER RIGHTS**).
- A draft E-Bill was introduced in October 2012 that aims to implement a legal framework for regulating ICTs (see **VIOLATIONS OF USER RIGHTS**).
- A government plan to implement a so-called "spy machine" for monitoring mobile phone companies was struck down by a court in late 2012 but sanctioned by parliament in mid-2013 (see **VIOLATIONS OF USER RIGHTS**).
- In October 2012, criminal libel charges were brought against an online news correspondent, though he was acquitted in February 2013 (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Internet and mobile phone services were first introduced in Malawi in the late 1990's, though after decades of flagging economic development, the impact of information and communication technologies (ICTs) has been limited for most Malawians compared to other countries in Sub-Saharan Africa. Penetration rates for digital media tools remain well below average for the region due primarily to poor infrastructure and the high cost of access. Nevertheless, the development of Malawi's ICT sector has become a government priority under President Joyce Banda, who in her inaugural state of the nation address in May 2012 set out a vision for deploying ICTs as a catalyst for economic development.[1]

Banda came to power in April 2012 following the death of former President Bingu wa Mutharika, who was known for his heavy-handed approach towards the opposition and restrictions against fundamental freedoms, including digital media freedoms. In 2011, the Malawi Communication Regulatory Authority (MACRA) under the Mutharika government introduced a Consolidated ICT Regulatory Management System that became locally known as the "spy machine," which ostensibly aimed to monitor the performance of mobile phone companies to improve quality of service. The courts placed an injunction on the system in late 2012, but in June 2013, parliament gave MACRA its endorsement to install the machine, despite the court's ruling.

The government does not systematically block or filter internet content in Malawi; however, during violent anti-government protests in July 2011, MACRA reportedly ordered internet service providers (ISPs) to block certain opposition news and social media websites, among other media tools. No such blocks have occurred under President Banda, though a controversial E-Bill was introduced in October 2012 that aims to implement a legal framework for regulating ICTs. Criticized for its potential to limit internet freedom, the draft E-Bill would require editors of online public communications services to reveal their personal information and allow the government to appoint "cyber inspectors" to monitor online activity in the public domain.[2]

While harassment and violence against traditional media journalists was prolific under the late president Mutharika, online journalists were not targeted. One online journalist was arrested in October 2012 for allegedly insulting the new president and charged with criminal libel, though he was acquitted in February 2013 for lack of evidence.

OBSTACLES TO ACCESS

Malawi is a landlocked and densely populated country that suffers from widespread poverty. With 80 percent of the population residing in rural areas, the agricultural sector comprises the bulk of

[1] Cleopa Timon Otieno, "President Banda Unveils Malawi's ICT Vision as Government Sets Up 7 Telecentres," *Telecentre,* (blog), May 25, 2012, http://bit.ly/1dSjL2v.
[2] "Malawi Alert: E-Bill Puts Freedom of Expression Online in Cross-hairs," *Nyasa Times*, October 4, 2012, http://bit.ly/1fWVQAR.

the country's economic output. Accordingly, Malawi's presence on the internet is one of the lowest in the world, with a penetration rate of just over 4 percent as of the end of 2012, according to the International Telecommunications Union.[3] Meanwhile, there were about 1,200 fixed broadband subscriptions in 2012 for a penetration rate of 0.1 percent,[4] and broadband speeds average 0.1 Mbps or less.[5] Mobile phone penetration in Malawi is also low at 28 percent,[6] compared to an average of 76 percent across the continent as of February 2013.[7]

Most users log on at internet cafes, as computers are a luxury for ordinary households in Malawi, and very few households have access to the internet at home. Nevertheless, the recent introduction of affordable 3G and 3.75G mobile broadband services has led to increasing mobile internet access and declining patronage at local internet cafe operations, which charge a minimum of 5 Malawian kwacha per minute, about $1.00 per hour, and close at 6pm.[8] In addition, service on the GSM network has expanded throughout the country to cover 93 percent of the population following the removal of a number of regulatory barriers such as long registration processes, making Malawi's GSM signal coverage one of the highest in Africa.[9] DSL services are also available, and Malawi Telecommunications Limited (MTL) launched WiMAX wireless broadband services in May 2012.[10] Competition between private ISPs has further enabled wireless internet access through Wi-Fi hotspots, particularly in urban areas of the country.

While Malawi's ICT sector has experienced tremendous growth in recent years, the cost of access remains a major challenge for ordinary people. The government does not regulate the price of internet access, enabling operators to charge as they wish and making the cost of access prohibitively high for many Malawians. As of early 2013, the monthly price of fixed-line internet access is US$16.50, while a monthly mobile 3G data plan costs about US$24 for 1.5GB of data.[11] The high cost of internet access in Malawi is symptomatic of the many challenges that ISPs face, one being the lack of a local internet exchange point, which forces telecoms to rely on upstream service providers that are usually based outside Africa. As a result, data that should be exchanged locally within Malawi or regionally must pass through Europe or North America where upstream providers are based, leading to an unnecessary and expensive waste of upstream bandwidth.

---

[3] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[4] International Telecommunication Union, "Fixed (Wired)-broadband Subscriptions, 2000-2012."
[5] Broadband Commission for Digital Development, "The State of Broadband 2012: Achieving Digital Inclusion for All," September 2012, http://www.ericsson.com/res/docs/2012/the-state-of-broadband-2012.pdf.
[6] International Telecommunication Union, "Mobile-cellular Telephone Subscriptions, 2000-2012."
[7] "World's Mobile Penetration," *Parseco*(blog), December 18, 2012, http://www.parseco.com/worlds-mobile-penetration/.
[8] Richard Chirombo, "Mobile Phones Push Internet Cafes Under," *Sunday Times*, January 22, 2012, http://www.bnltimes.com/index.php/sunday-times/headlines/business/3907-mobile-phones-push-internet-cafes-under.
[9] Vivien Foster and Maria Shkaratan, "Malawi's Infrastructure: A Continental Perspective," Africa Infrastructure Country Diagnostic, World Bank, March 2010, http://siteresources.worldbank.org/INTAFRICA/Resources/Malawi_country_report_2011.01.pdf.
[10] "MTL Launches New Wireless Broadband Internet Service," *Daily Times*, May 4, 2013, http://www.bnltimes.com/index.php/daily-times/headlines/business/6218-mtl-launches-new-wireless-broadband-internet-service.
[11] "Comparing African Pre-paid Mobile Broadband Plans," *OAfrica,* September 24, 2012, http://www.oafrica.com/mobile/african-pre-paid-mobile-broadband-plans/.

Another major challenge facing the telecommunication sector in Malawi is that the country's power and ICT backbones are entirely national in nature, with no regional integration at present, although a number of cross-border connections have been proposed.[12] Due to Malawi's landlocked location, the country's connection to the international fiber network runs through Mozambique, Zambia, South Africa and Tanzania.[13] Three new submarine cables are currently competing to be the first to start service in Malawi as the country plans to extend a fiber-optic backbone through Tanzania to the coast.[14] If a suitable regulatory regime is also put in place, the new cables will bring down the cost of international bandwidth and deliver a boost to the broadband market. Meanwhile, the high costs of infrastructural development in rural areas has led to an unwillingness by providers to invest in the country's remote regions, though the regulatory authority MACRA is looking to subsidize fees to encourage operators to deploy ICT services in the country's less profitable yet neediest areas.

A low literacy rate of 64 percent and a significant digital gender divide are also hindering progress and access to ICTs in Malawi, while unreliable electricity and the high cost of generator power in the country strain ICT use. Only 7 percent of the country has access to electricity, giving Malawi one of the lowest electrification rates in the world.[15] The electricity grid is concentrated in urban centers, though only 25 percent of urban households have access, compared to a mere 1 percent of rural households. Half the formal sector enterprises in Malawi have backup generators, which is twice the amount found in other low-income African countries.

According to statistics released in May 2013, there are 22 operational ISPs in Malawi, and despite high operating costs and the limited availability of international bandwidth, there is reasonable competition between the providers. Malawi Net, formed in 1997, was the country's first private ISP, followed in 1999 by Malawi Sustainable Development Network Programme, a semi-government owned and United Nations Development Project-funded ISP. In the new millennium, several private ISPs followed suit, including Africa-Online, Globe Internet Company, Skyband, and most recently, Malawi Telecommunications Limited (MTL). MTL also serves as the country's telecommunication backbone since most ISPs and mobile phone service providers use MTL's infrastructure.[16] Previously a government-owned entity, MTL was privatized in 2005 and is now 80 percent owned by Telecomm Holdings Limited, while the government retains the other 20 percent.

Malawi's two major players in mobile phone services, Airtel Malawi and Telecom Networks Malawi, together command a mobile teledensity of 18 percent and recently launched 3G mobile

[12] "PPIAF Assistance in Malawi," Public Private Infrastructure Advisory Facility, March 2012, http://www.ppiaf.org/sites/ppiaf.org/files/documents/PPIAF_Assistance_in_Malawi.pdf.
[13] "Video: Internet Service Prices Still High in Malawi," *OAfrica*, December 8, 2011, http://www.oafrica.com/video/video-internet-service-prices-still-high-in-malawi/.
[14] Beatrice Philemon, "Malawi Keen on Submarine Cable Connection with Tanzania," *Ippmedia*, March 18, 2012, http://www.ippmedia.com/frontend/index.php?l=39583.
[15] "Telekom Networks Malawi (TNM) Ltd. – Malawi – Feasibility Study," GSMA Green Power for Mobile, 2012, http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/TNM_Malawi_Feasibility-Study.pdf.
[16] "Telecommunications in Malawi," *MBendi*, accessed June 1, 2013, http://www.mbendi.com/indy/cotl/tlcm/af/ma/p0005.htm.

services based on UMTS/HSPA technology.[17] A third mobile operator, G-Mobile, was licensed in 2008 but the rollout of the new network experienced delays. It is currently in court fighting against the revocation of its license as a result of a failure to start services on time.[18] A fourth license was awarded to Celcom in 2011, and the launch of its services is expected in 2013. Meanwhile, the government has encouraged more competition in the market by introducing a converged licensing regime, which enabled the country's two fixed-line operators, MTL and Access Communications, to enter the mobile market. Both telecoms are already operating CDMA-based fixed-wireless networks that support full mobility and broadband access using high-speed EVDO technology.

MACRA is Malawi's sole regulator, established under the 2008 Communication Act to ensure reliable and affordable ICT service provision throughout Malawi. Its mandate is to regulate the whole communications sector with respect to telecommunications, broadcasting, postal services, and the management of the radio frequency spectrum. As a regulator, it also issues operating licenses for mobile and fixed-line phone service providers, ISPs, and cybercafes, though political connections are often necessary to receive such licenses.

The institutional structure of MACRA is not without political interference as its board is comprised of a chairman and six other members appointed by the president and two ex-officio members—the secretary to the Office of the President and Cabinet and the Information Ministry secretary. The director general, whose appointment also passes through the president's scrutiny, heads the authority's management and supports the board of directors in the execution of its mandate.

LIMITS ON CONTENT

Increasing government manipulation of online content through pro-government trolls is the most notable trend of 2012 and 2013, as the Malawian government seems to be grappling with the desire to restrict critical online speech in spite of their technical inability to do so.

The government of Malawi does not systematically block or filter any websites primarily out of a lack of capacity, though it has demonstrated a desire to censor internet content in the past. During violent anti-government protests in July 2011, MACRA reportedly ordered ISPs to block certain news websites and social media networks, including Facebook and Twitter, in a supposed effort to quell the spread of violence.[19] The UK-based Malawian online publication, *Nyasa Times*, also experienced repeated distributed denial-of-service (DDoS) attacks that shut down its servers and effectively disrupted its reporting of the protests. Known for its critical coverage and sometimes exaggerated articles about the government, *Nyasa Times* was reportedly blocked again in November

[17] Universal Mobile Telecommunications Service (***UMTS***) and high-speed packet access (***HSPA***).
[18] Frank Jomo, "Malawi Court Halts Regulator Canceling G-Mobile's License, Times Reports," Bloomberg, May 25, 2011, http://www.bloomberg.com/news/2011-05-25/malawi-court-halts-regulator-canceling-g-mobile-s-license-times-reports.html.
[19] Michael Malakata, "Malawi Blocks Social Media Networks to Quell Protests," *Computer World*, July 22, 2011, http://news.idg.no/cw/art.cfm?id=3DFADEBE-1A64-67EA-E44251D79A4C6F57.

2011, after it had published stories about government corruption and Mutharika's health problems.[20]

Under the country's new leadership, however, no such efforts to block or filter online content have occurred. There have been no reports of content removal—even of illegal content such as child pornography or copyright infringement—under either the former or the current government. However, a draft Electronic Transactions and Management Bill in the works as of mid-2013 aims to provide the government with a legal instrument to deal with illicit online material, according to a spokesperson from the Office of the President and Cabinet.[21]

Social media platforms are freely available in Malawi, though in advance of the January 2013 protests against the country's current economic hardships, the authorities called on citizens to abstain from using Facebook and Twitter in an attempt to prevent the demonstrations from getting out of hand.[22] Rebelling against the call to self-censor online, activists went on Facebook to criticize the government's efforts to limit freedom of speech and to express concern over the possible blocking of online content. Nevertheless, social networks and other digital communication tools remained unrestricted during the protests.

Despite the country's technical inability to block or filter online content, there are concerns that Malawi is currently attempting to move towards an administrative form of internet censorship through a draft E-Bill that was proposed in October 2012 (see "Violations of User Rights").[23] While the first draft of the bill prescribes restrictions against internationally-recognized illegal content, press freedom watchdogs such as the Media Institute of Southern Africa and the Media Council of Malawi expect the bill's second draft to include more problematic provisions that will restrict government criticism, stemming from concerns over various unofficial suggestions the authorities have made about the need to deal with online publications that allegedly "insult" or "spread falsehoods" about the government.

Online users and commentators practice a degree of self-censorship, though users have become less fearful since Banda took power as a result of the reduced levels of harassment and violence against traditional journalists that was common under the late Mutharika's regime. Otherwise, online journalists usually exhibit caution in handling stories associated with ethnic, racial or religious minorities, while comments have been less cautious and much more open to discussing topics of controversial nature.

Nevertheless, there has been an increasing presence of pro-government trolls infiltrating conversations on social media and online news websites to attack commentary that is critical of the government. In addition, pro-government activists zealously promote content that President Banda

[20] "Malawi Authorities Blocking Nyasa Times Website," *The Zimbabwean*, November 8, 2011, http://www.thezimbabwean.co.uk/news/16305/malawi-authorities-blocking-nyasa-times-website.html.
[21] Interview conducted by a Freedom House consultant.
[22] "Malawi Police Urges Against Facebook Updates, Tweets on Demos," *Nyasa Times*, January 16, 2013, http://www.nyasatimes.com/2013/01/16/malawi-police-urges-against-facebook-updates-tweets-on-demos/.
[23] Simon Mponela, "Malawi Government to Censor Online Publications," *Amalawi*, October 2, 2012, http://www.amalawi.info/index.php/2012/10/02/malawi-government-to-censor-online-publications/.

posts on her official Facebook page.[24] Conversations in Facebook groups where the trolls regularly appear suggest that they may be on an unofficial government payroll. Meanwhile, the government launched its own news website, *MANA Online*, in August 2012 to compete with dissenting online news outlets in the country,[25] and the UK-based news portal, Nyasa Times, has close connections with the President Banda through two journalists who are also members of the Presidential Press Secretariat.

The Malawian blogosphere is still in its infancy but is growing, with media publishers such as Blantyre Newspapers Limited trying to host bloggers on their websites to enhance their image as an independent news source. In May 2012, blogging was recognized as an important part of journalism for the first time when the Media Institute of Southern Africa's blogging award of the year was presented to the prominent blogger and journalist, Kondwani Munthali, marking a notable development in Malawi's media history.[26] In May 2013, the award went to another Malawian journalist, Rebecca Chimjeka.[27]

Nevertheless, many Malawian civil society groups have not been able to develop websites or an online presence primarily because the bulk of the people they serve reside in rural areas where literacy levels are low and access to ICTs limited or non-existent. In addition, economic conditions in the country have made it difficult for journalists and media groups to launch online outlets, and the high cost of using the .mw domain—currently being administered by the Malawi SDNP on behalf of the Malawian government—makes it expensive to provide locally-produced content. According to an official at the SDNP, the cost of using the .mw domain is $100 a month for the first two months after registering for the domain and $50 a month thereafter. Furthermore, online advertising is low due to businesses having a limited understanding of the internet and their hesitancy to advertise with independent media outlets.

The most influential ICT tool at the moment is the mobile phone through which SMS messages are disseminated to garner political support or conduct opinion polls. For example, in the 2009 elections, the Democratic Progressive Party took advantage of increasing mobile phone penetration to campaign for their presidential candidate via SMS. In December 2012, the country's leading print media group Nation Publications Limited, conducted an opinion poll on presidential candidate preferences via SMS and Facebook,[28] which the government accused of being biased after the results showed President Banda losing.[29]

---

[24] Her Excellency Dr Joyce Banda's Facebook page, accessed September 2013, https://www.facebook.com/pages/Her-Excellency-Dr-Joyce-Banda/325799237543309?ref=stream.
[25] Gregory Gondwe, "MANA Launches Online Service," *Biz Community,* August 15, 2012, http://www.bizcommunity.com/Article/129/23/80053.html.
[26] Victor Kaonga, "Kondwani Munthali: Malawi's Blogger of the Year," *Global Voices*, May 15, 2012, http://globalvoicesonline.org/2012/05/15/malawi-kondwani-munthali-malawis-blogger-of-the-year/.
[27] Rebecca Chimjeka's personal blog available at, http://rebeccachimjeka.wordpress.com.
[28] "Malawi Paper Carrying Opinion Poll on Presidential Candidates," *Nyasa Times*, December 7, 2012, http://www.nyasatimes.com/2012/12/07/malawi-paper-carrying-opinon-poll-on-presidential-candidates/.
[29] Pius Nyondo, "Malawi State House Accuses Newspaper of Endorsing Presidential Candidate Ahead of 2014," *Maravi Post*, December 12, 2012, http://www.maravipost.com/national/society/2478-malawi-state-house-accuses-newspaper-of-endorsing-presidential-candidate-ahead-of-2014-polls.html.

A growing number of public demonstrations have been organized through SMS and social media, including nationwide protests on January 17, 2013 fueled by anger against rising inflation.[30] Demonstration organizers launched online campaigns on Facebook and Twitter to urge public participation in the street protests, and as a result, the president eventually conceded to pressure by reducing her personal travel expenses. Nevertheless, there were no major policy changes in response to the protests.

VIOLATIONS OF USER RIGHTS

The repeal of Section 46 of the penal code in May 2012 marked an opening for overall media freedom in Malawi, but an E-Bill proposed in October 2012 threatens to limit freedom of expression online. A criminal libel case was lodged against an online journalist in October, demonstrating the Banda government's sensitivity towards critical speech, though a court acquitted him for lack of evidence. Courts also placed an injunction on the regulatory authority's effort to implement a "spy machine" on mobile phone companies.

Malawi has strong constitutional guarantees for freedom of the press and expression, though there are several laws that restrict these freedoms in practice, such as the 1967 Protected Flag, Emblems and Names Act and the 1947 Printed Publications Act, which restricts the media from reporting on the president, among other limitations.[31] Nevertheless, Malawi's judiciary is generally regarded as independent and has rendered several significant decisions against the government in recent years. Most notably, the National Assembly in May 2012 repealed Section 46 of the penal code that was enacted under former President Mutharika in January 2011 with the aim of empowering the information minister to ban any publications deemed "contrary to the public interest."[32] The provision's repeal was widely applauded by civil society and human rights groups.

While existing legislation primarily pertains to traditional media, the government introduced an E-Bill in October 2012 that aims to implement a legal framework for regulating ICTs. Widely criticized for its potential to limit internet freedom, the E-Bill would require editors of online public communications services to make their personal information—including names, addresses, telephone and registration numbers—available to the public. The bill would also allow the government to appoint "cyber inspectors" who would have the power "monitor and inspect any website or activity on an information system in the public domain and report any unlawful activity" to the regulatory authority.[33] The E-Bill is undergoing review as of mid-2013, and the Malawian

[30] Frank Jomo, "Malawians Protest Against Soaring Costs, Slump in Kwacha," Bloomberg, January 17, 2013, http://www.bloomberg.com/news/2013-01-17/malawians-protest-against-soaring-costs-slump-in-kwacha.html.
[31] "Malawi 2012," in *African Media Barometer* (Friedrick-Bert-Stiftung: 2012), http://www.fesmedia-africa.org/uploads/media/AMB_Malawi_2012.pdf, 15, 17.
[32] "Malawi MPs Vote to Repeal Media Ban Law, Sec 46," *Nyasa Times*, May 30, 2012, http://www.nyasatimes.com/2012/05/30/malawi-mps-vote-to-repeal-media-ban-law-sec-46/; Committee to Protect Journalists, "CPJ Welcomes Repeal of News Censorship Law," news release, June 1, 2013, http://ifex.org/malawi/2012/06/01/news_censorship_law/; "MISA meets with President Joyce Banda, pushes for Access to Information Law," MISA/IFEX, June 27, 2012, http://www.ifex.org/malawi/2012/06/27/meeting_president/.
[33] "Malawi Alert: E-Bill Puts Freedom of Expression Online in Cross-hairs," *Nyasa Times*, October 4, 2012, http://www.nyasatimes.com/2012/10/04/malawi-alert-e-bill-puts-freedom-of-expression-online-in-cross-hairs/.

government has reportedly sought input from individuals and institutions on the draft's provisions.[34]

Libel is both a criminal and civil offense in Malawi, punishable with up to two years' imprisonment if prosecuted as a criminal charge, though most libel cases are processed as civil offences or settled out of court. In October 2012, criminal libel charges were brought against Justice Mponda, a correspondent for the online publication, *Malawi Voice*, which President Banda has reportedly criticized for its publication of "misleading and unbalanced" stories. Mponda was arrested and had his computers and other equipment seized for allegedly insulting the president and publishing false information.[35] He was released on bail the day after his arrest and formally charged with "publishing false news likely to cause public fear,"[36] though a court acquitted Mponda of all charges due to lack of evidence in February 2013.[37]

In 2011, the regulatory authority MACRA attempted to implement a Consolidated ICT Regulatory Management System (CIRMS), locally known as the "spy machine," ostensibly for the purpose of effectively monitoring the performance of mobile phone companies and improving quality of service. Purchased from the U.S.-based company, Agilis International, for US$6.8 million, the system would allow MACRA to obtain data from telephone operators, including the time, duration, and location of calls, SMS messages sent and received, the type of handset used, and other subscriber details.[38] In October 2011, a court granted an injunction against MACRA's request to roll-out the spy machine,[39] and in September 2012, Malawi's High Court issued a ruling that banned the implementation of the system altogether.[40] MACRA has since taken the issue to the Supreme Court to appeal the ban.[41] In February 2013, the parliamentary media and communications committee stepped up its support of the system,[42] and in June, parliament gave MACRA its endorsement to install the machine, despite the court rulings. The machine's roll-out now awaits the Supreme Court's decision regarding MACRA's appeal.[43]

---

[34] "Malawian Govt Seeks Views Draft Electronic Legislation," *telecompaper*, October 2, 2012, http://www.telecompaper.com/news/malawian-govt-seeks-views-draft-electronic-legislation--899011.
[35] "Malawi Online Journalist Arrested," MISA/IFEX, October 16, 2012, http://www.ifex.org/malawi/2012/10/16/malawi_online_journalist/.
[36] "Malawi Alert-Update: Arrested Online Journalist, Justice Mponda, Granted Bail," MISA Malawi, October 17, 2012, http://www.mw.misa.org/index.php?option=com_content&view=article&id=139:malawi-alert-update-arrested-online-journalist-justice-mponda-granted-bail-.
[37] Knowledge Chiwambo, "Malawi Court Free Online Journalist Mponda," *Newstime Africa*, February 9, 2013, http://www.newstimeafrica.com/archives/30755.
[38] Gregory Gondwe, "'Spy Machine' Brings Telecoms Fears," *Biztech Africa*, November 14, 2011, http://www.biztechafrica.com/article/spy-machine-brings-telecoms-fears/1437/?section=government.
[39] "Malawi Court Stops Govt from Using 'Spy Machine,'" *Mabvutojobani*, Otocber 16, 2011, http://mabvutojobani.com/2011/10/16/malawi-court-stops-govt-from-using-%E2%80%98spy-machine%E2%80%99/.
[40] Peter Chipanga, "Court Quashes Malawi Communication Regulatory Authority 'Spy Machine,'" *Newtimes Africa*, Septe 23, 2013, http://www.newstimeafrica.com/archives/28417.
[41] "Macra Takes 'Spy Machine' Ban to Supreme Court," *telecompaper*, October 29, 2012, http://www.telecompaper.com/news/macra-takes-spy-machine-ban-to-supreme-court--904627.
[42] Hudson Mphande, "Malawi MPs Endorse 'Spy' Machine," *Nyasa Times*, June 25, 2013, http://www.bnltimes.com/index.php/daily-times/headlines/national/13850-mps-endorse-spy-machine.
[43] Gregory Gondwe, "Telecom Operators Lose Ground in 'Spy Machine' Fight," *Biztech Africa*, June 27, 2013, http://www.biztechafrica.com/article/telecom-operators-lose-ground-spy-machine-fight/6330/.

Meanwhile, there are no SIM card registration requirements in Malawi, nor is there evidence that ISPs or cybercafés are required to proactively monitor users or retain user data. By law, service providers are required to hand over user information when presented with a court order; however, such legal safeguards have failed to prevent police abuse in the past, particularly under the Mutharika regime. For example, in early 2012, when the Mutharika government suspected a group led by then-Vice President Joyce Banda of scheming to overthrow it, the authorities demanded mobile phone companies hand over transcripts of the group's mobile phone and SMS communications, which Mutharika planned to use against Banda before his death.

Under Malawi's new leadership, there have been no physical assaults, extra-legal detentions, or technical attacks against opposition activists, bloggers, or ordinary users, though harassment and violence against traditional media journalists was prolific under the late president Mutharika, especially during the anti-government protests in July 2011 that killed 18 people.[44]

[44] Reporters Without Borders, "Letter to President Mutharika about his Threats to Journalists," March 20, 2012, http://en.rsf.org/malawi-letter-to-president-mutharika-20-03-2012,42163.html.

MALAYSIA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	10	9
Limits on Content (0-35)	14	15
Violations of User Rights (0-40)	19	20
Total (0-100)	43	44

* 0=most free, 100=least free

POPULATION: 29 million
INTERNET PENETRATION 2012: 66 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- In the run-up to the May 2013 elections, news outlets covering the opposition faced cyberattacks and content disruptions (see **VIOLATIONS OF USER RIGHTS**).
- A legal amendment holding website owners liable for seditious comments posted by users took effect in July, despite civil society opposition (see **VIOLATIONS OF USER RIGHTS**).
- A 2012 act on public security effective since 2012 may strengthen police surveillance powers (see **VIOLATIONS OF USER RIGHTS**).
- Police charged a blogger for criticizing the Malaysian state of Johor's new Sultan in 2012 (see **VIOLATIONS OF USER RIGHTS**).
- Toronto-based Citizen Lab found spyware sold only to governments on "a Malaysian election-related document" circulating before the polls (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

The Malaysian government's encouragement of internet and mobile phone access has driven steady growth in new media since the first internet service provider (ISP) was inaugurated in 1992. By 2012, internet penetration was measured at 66 percent, among the highest in the region.

In May 2013 general elections, the Barisan Nasional coalition clung to power with just under 50 percent of the popular vote, having lost its two-thirds parliamentary majority in 2008 for the first time since 1969.[1] Its leader, Prime Minister Najib Razak, publicly promotes internet freedom.[2] Yet his government detained at least eight bloggers in the months following 2008 elections, many for sedition, or criticism of Malaysia's royalty, which includes the sultans who constitutionally rule nine of the country's 16 states and federal territories. In the past two years, with elections looming, officials reinforced commitments not to censor the internet, prosecuted fewer bloggers, and pledged legislative reforms.[3] When these reforms materialized in 2012, however, they fell short of international standards. One notorious security law was repealed, but its replacement allows the public prosecutor to intercept electronic communications without judicial oversight in security investigations. An amendment to the Evidence Act 1950 rendering intermediaries liable for seditious comments posted by users raised considerable civil society opposition in April, but went quietly into effect in July. Meanwhile, police launched two new investigations for online criticism of the Sultan of Johor; one blogger still faces charges.

Online mobilization was widely perceived as contributing to the opposition's 2008 electoral gains,[4] and elections this year were marred by attempts to manipulate online discourse. Internet users noted a palpable increase in the presence of "cybertroopers," commentators paid by political parties on all sides to attack their opponents. Other activity seemed to favor the government: Web news outlets covering the opposition faced cyberattacks in the lead-up to the polls, and some apparent filtering, though it was not clear if this was executed by the hackers or signaled a more formal intervention by officials or service providers. Online reporting—some from the past year—helped expose the government's multi-million dollar sponsorship of pro-Najib articles published by supposedly objective international blogs and news outlets since 2008. And in mid-2013, Toronto-based Citizen Lab reported that at least one electronic document containing election-related information in Malay appeared to be spreading spyware to recipients. The government is

1 In 1973, the Barisan Nasional, which translates as National Front, absorbed the Alliance Party coalition which had governed Malaysia since 1957. "A Tawdry Victory," *Economist* (blog), May 6, 2013, http://www.economist.com/blogs/banyan/2013/05/malaysias-election-0.
2 The government first pledged to keep Malaysia's internet free of interference in 1998. See OpenNet Initiative, "Country Profile—Malaysia," August 7, 2012, http://opennet.net/research/profiles/malaysia.
3 Kal Kamel, "No Internet Censor, But Bloggers Must Know Where to Draw the Line: Malaysian Prime Minister," *Grey Review*, April 25, 2011, http://www.greyreview.com/2011/04/25/no-internet-censor-but-bloggers-must-know-where-to-draw-the-line-malaysian-prime-minister/.
4 "Malaysia's Uneasy Dance with the Web," *Asia Sentinel*, August 17, 2010, http://asiasentinel.com/index.php?option=com_content&task=view&id=2645&Itemid=178.

investigating online news portal *Malaysian Insider* for quoting international reports about that spyware, which could allow authorities to spy on citizens without their knowledge.[5]

Despite these challenges, citizens continued to communicate voraciously via social networks. News websites, once outliers, are now an indispensable part of Malaysia's information landscape. Internet users effectively documented police crackdowns on political protests in 2011 and 2012 that were downplayed by tightly-controlled traditional media, and police cooperated with organizers of a much more peaceful rally in January 2013. In October 2012, an appeals court ruling overturned an "irrational" home ministry ruling against *Malaysiakini*, an independent news website seeking a print publication license.[6] The ministry repeatedly refused to grant the outspoken outlet a license—the kind of decision which encourages self-censorship among print and broadcast owners, even though some licensing requirements were relaxed in 2012.[7] In characterizing *Malaysiakini's* right to publish a newspaper as fundamental, the judge took a step towards ensuring that Malaysia's vibrant internet culture will continue to have a powerful, positive impact on the nation's broader free expression restrictions. That vision was not shared by the home minister and the attorney general, who appealed the ruling.[8]

OBSTACLES TO ACCESS

Internet penetration was measured at 66 percent in 2012, one of the higher rates in Asia;[9] officials pledged to increase it to 80 percent in 2013.[10] Malaysians can access the internet through home connections, workplaces, and mobile phones. In April 2012, Kuala Lumpur's municipal government even introduced a policy requiring businesses seeking food and beverage licenses to provide inexpensive Wi-Fi.[11]

Cybercafes also play an important role in bridging the digital divide, though one persists. More than 80 percent of internet users lived in urban areas as recently as 2010,[12] and penetration remains low in less populated states in East Malaysia, where most residents belong to indigenous groups.

The introduction of wireless WiMax technology in 2008 has helped bring broadband to regions that are difficult to reach via cable; four WiMax providers were in operation as of mid-2013. The government has also prioritized development of the broadband infrastructure. In 2010, a National

5 The presence of the spyware in Malaysia does not reveal who is employing it, but it is marketed to governments. See Violations of User Rights.
6 Hafiz Yatim, "Malaysiakini Wins Court Battle Over Print Licence," *Malaysiakini,* October 1, 2012, http://bit.ly/V5bcKG.
7 Reporters Without Borders, "Media Freedom in Malaysia is Far From Assured, Open Letter Tells Prime Minister," May 15, 2012, http://en.rsf.org/malaisie-media-freedom-in-malaysia-is-far-15-05-2012,42628.html.
8 Human Rights Watch, World Report 2013, Country Reports, "Malaysia," January 31, 2013, http://bit.ly/ZbdTes, 2.
9 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx; The Economic Transformation Programme Report 2012, 188.
10 The Economic Transformation Programme Report 2012, 188, http://bit.ly/17l5Y0j.
11 Choong Mek Zhin, "DBKL to Make it a Requirement for Restaurants to Provide Wi-Fi Services," *Star Online*, January 9, 2012, http://thestar.com.my/metro/story.asp?file=/2012/1/9/central/10210201&sec=central.
12 ComScore, "Malaysian Internet Usage Driven Primarily by People in Central Region," press release, October 7, 2010, http://bit.ly/bQWgXU.

Broadband Initiative introduced five programs to expedite broadband and mobile expansion, some in cooperation with Telekom Malaysia, the country's largest—and formerly state-owned—telecommunications company, which retains a monopoly over the fixed-line network.[13] By 2011, around 250 Community Broadband Centers were established nationwide and nearly 500,000 netbooks distributed to students and low income citizens in rural and suburban areas.[14] In 2012, the 1Malaysia Broadband Affordable package offered five states with lower penetration rates decent broadband speeds for under MYR 38 ($12) per month.[15]

Mobile phone usage surpassed the country's total population in 2011. By 2012, mobile penetration was at 141 percent, indicating that some individuals had multiple phone lines.[16] Mobile internet access is available, generally affordable and popular among young people. Approximately 20 percent of Malaysians aged 20-24 reportedly accessed the internet via their mobile phones in 2011.[17]

Regulation of the internet falls under the purview of the Malaysian Communications and Multimedia Commission (MCMC), which is overseen by the minister of information, communications, and culture. Both the MCMC and the ministry are guided by the 1998 Communication and Multimedia Act (CMA), which gives the information minister a range of powers, including licensing the ownership and operation of network facilities. This could serve as a means of control as it does for the traditional media, though no examples of this have been documented, perhaps because the 25 private ISPs often have government connections. The two largest ISPs are TMnet, a subsidiary of the privatized national phone company Telekom Malaysia, and Jaring, which is owned by the Ministry of Finance. The same is true for mobile providers. The largest, Maxis Communications, was founded by Ananda Krishnan, who also owns Malaysia's biggest satellite broadcaster and enjoys close ties to former Prime Minister Mahathir Mohamad.[18] Two new mobile phone providers, YTL Communications and Umobile, have joined the market since 2008. Though ostensibly unrelated to the government, observers believe they benefit from political connections.

In recent years, some local authorities have introduced restrictions on cybercafes to curb illegal online activities, particularly gambling, which is grounds for closure if detected on cafe premises. Select states have capped the number of cybercafe licenses available, making it difficult for legitimate new venues to open.[19]

---

13 Sira Habu and Shaun Ho, "RM 1 Billion Initiative to Promote High-Speed Broadband Usage," *Star Online*, March 25, 2010, http://thestar.com.my/news/story.asp?file=/2010/3/25/nation/5931577&sec=nation.
14 Ministry of Information Communication and Culture Malaysia, "Rural Broadband Initiatives in Malaysia," September 21, 2011, http://www.scribd.com/doc/68533475/Rural-Broadband-Initiatives-in-Malaysia.
15 "1Malaysia Broadband Affordable Packages for 5 States," *Malaysian Wireless*, September 8, 2012, http://www.malaysianwireless.com/2012/09/1malaysia-broadband-affordable-packages-for-5-states/.
16 International Telecommunication Union, "Mobile-cellular Telephone Subscriptions, 2000-2012."
17 "Malaysian Internet Usage Takes Off in 2010," Nielsen Wire (blog), April 25, 2011, http://bit.ly/fh3qMN.
18 Colin Kruger, "Billionaire Eyes Australian Media," *Sidney Morning Herald*, May 28, 2011, http://www.smh.com.au/business/billionaire-eyes-australian-media-20110527-1f81u.html.
19 Peter Boon, "Cyber Cafe Licences Not Issued Anymore—Ministry," *Borneo Post Online*, October 15, 2012, http://www.theborneopost.com/2012/10/05/cyber-cafe-licences-not-issued-anymore-ministry/.

The CMA provides for the ministry to appoint the MCMC chairman and three government commissioners, plus two to five commissioners from non-governmental entities; the current three are from the private sector.[20] Since 2008, the process for appointing members of the MCMC advisory board has become more transparent and participatory, involving consultations with diverse stakeholders and the inclusion of civil society members on the board. Yet the MCMC remains a driving force in efforts to curtail online speech, including investigations into online portals and bloggers.

LIMITS ON CONTENT

Malaysian bloggers, though still practicing self-censorship on some issues, were an effective check on power in 2012. Though content manipulation increased in the run-up to elections, websites helped expose it, and also thwarted an apparent effort to block or throttle their content that coincided with coordinated cyberattacks. As they had in 2011, internet users braved a police crackdown to muster protesters in a massive demonstration in late April and early May 2012 that was barely reflected in traditional media reports. A more peaceful January 2013 rally benefitted from digital tools to ensure it went smoothly.

A provision of the CMA explicitly states that none of its wording "shall be construed as permitting the censorship of the Internet." The Multimedia Super Corridor, an information technology development project, includes a 10-point Bill of Guarantees that promises no censorship to member ICT businesses.[21]

While the Malaysian government blocks some websites for violating Malaysian laws, it has not systematically targeted political content in the past. In 2009, Information, Communications, and Culture Minister Dr. Rais Yatim sought to "evaluate the readiness and feasibility of the implementation of the Internet filter at [the] Internet gateway level," but backtracked due to opposition.[22] In mid-2013, officials said a total 6,640 sites had been blocked since 2008.[23]

Authorities also take administrative measures to restrict information. The MCMC can instruct websites to remove content, including some perceived as critical of the government. Issues such as Islam's official status, race, royalty, and the special rights

20 Malaysian Communications and Multimedia Commission Act 1998, available at: http://www.agc.gov.my/Akta/Vol.%2012/Act%20589.pdf.
21 Multimedia Super Corridor, "MSC Malaysia 10-Point Bill of Guarantees," accessed August 2013, http://www.mscmalaysia.my/news/introducing-msc-malaysia-certified-solutions; MCMC, "Communications and Multimedia Act 1998," accessed August 2013, http://www.skmm.gov.my/Legal/Acts/Malaysian-Communications-And-Multimedia-Commission.aspx.
22 Rebekah Heacock, "Malaysia Considers, Backs Down from National Internet Filter," OpenNet Initiative (blog), August 13, 2009, http://opennet.net/blog/2009/08/malaysia-considers-backs-down-national-internet-filter.
23 "More Than 6,000 Websites Blocked for Violations Since 2008," *Bernama,* via *Malay Mail Online,* July 5, 2013, http://www.themalaymailonline.com/malaysia/article/more-than-6000-websites-blocked-for-violations-since-2008.

enjoyed by *bumiputera*, who are ethnic Malays and other indigenous people, as opposed to the ethnic Chinese and Indian minorities, are also considered sensitive. Discussing them can lead to prosecution, so internet users do exercise self-censorship, levels of which appeared to remain constant in 2012 and early 2013.

Procedures for administrative requests are generally nontransparent and lack judicial oversight and avenues for appeal. In 2009, the MCMC directed *Malaysiakini* to take down two videos containing sensitive religious and political content. When *Malaysiakini's* Editor-in-Chief Steven Gan refused, the MCMC urged the attorney general to prosecute him. He still risks a potential fine of up to MYR 50,000 ($14,300) and up to one year in prison,[24] but in 2013 the attorney general had yet to pursue the case, which remains the only reported one of its kind. The MCMC also issues administrative requests to service providers. In 2011, ISPs blocked access to 10 file-sharing websites citing Section 263 of the CMA and copyright laws.[25] Google blocked access to the infamous anti-Muslim video, "Innocence of Muslims," at the MCMC's request in September 2012.[26]

Many government-linked companies and public universities internally restrict access to *Malaysiakini* and other sites perceived as politically sensitive, though online news outlets represent an increasingly serious challenge to traditional media. *Malaysiakini* was listed as the nation's 15th most popular website by one source in 2013.27 This popularity, combined with the combative political reporting published by independent or opposition-aligned outlets, may have lead the government or its supporters to try and stop readers accessing them in the lead-up to 2013 elections, when a handful of news website technical staff discovered packets of information sent by their servers were not reaching readers, rendering their content temporarily inaccessible.[28] Some remained available on select ISPs. The platforms all fixed the problem within 48 hours, and at least two filed a complaint with the MCMC, which has yet to respond. The exact nature of the apparent blocking or throttling—which occurred while many of the sites were being targeted by hackers—remains unclear.

---

24 One showed Muslim demonstrators desecrating the head of a cow—an animal Hindus consider sacred—to protest the relocation of a Hindu temple; the second showed a political speech. See Reporters Without Borders, "Malaysiakini Website Refuses to Bow to Censorship," news release, September 24, 2009, http://en.rsf.org/malaysia-malaysiakini-website-refuses-to-24-09-2009,34575.

25 "Pirate Bay, MegaUpload and Others Blocked By Government Order," *Torrent Freak* (blog), June 9, 2011, http://torrentfreak.com/pirate-bay-megaupload-others-blocked-by-government-order-110609/.

26 Tashny Sukumaran, "Google Malaysia blocks 'Innocence of Muslims' video clip," September 17, 2012, http://www.thestar.com.my/story.aspx?file=%2f2012%2f9%2f17%2fnation%2f20120917111604.

27 "Top Sites in Malaysia," Alexa Web Information Company, accessed January 29, 2013, http://www.alexa.com/topsites/countries/MY.>

28 Oiwan Lam and Leila Nachawati, "Malaysia: News Sites Face Attacks on Eve of Elections," *Global Voices Advocacy,* May 4, 2013, http://advocacy.globalvoicesonline.org/2013/05/04/malaysia-news-sites-face-attacks-on-eve-of-elections/.

Despite these limits, expanded internet access has led to the emergence of a vibrant blogosphere. English and Malay are the dominant languages, and many civil society groups, including those representing ethnic minorities, have a dynamic online presence. Social networking is almost ubiquitous. One 2011 report said Malaysians over 15 spent approximately a third of their time online social-networking,[29] while a November 2012 article said Malaysians visited social media platforms a staggering 14 billion times a month.[30] Prime Minister Najib leads the way with his own blog and over a million followers on both Facebook and Twitter.[31] Other government representatives are embracing ICTs. The police force, for example, has Facebook and Twitter accounts where officers provide updates on policing activities and occasionally respond to accusations of abuse by members of the public.[32]

Some of this engagement is manipulative in nature, something that has become increasingly evident in the past three years. Both government and opposition figures privately acknowledge paying "cybertroopers," including bloggers and other online commentators, to generate favorable content on their behalf and denigrate their opponents.[33] Since traditional media restrictions caused opposition groups to embrace online platforms relatively early, the government's efforts to catch up have been costly—and so far, comparatively ineffective. The Barisan Nasional has a dedicated group of bloggers, Unit Media Baru, generating content on their behalf. Its members deny accepting payment for their efforts, which observers point out are deliberately misleading: they countered the well-established opposition news website *Sarawak Report* by creating a pro-government equivalent titled *Sarawak Reports*.[34]

The scale of these campaigns was exposed in 2012, when the government admitted paying international PR firm FBC Media MYR 83.8 million ($26.5 million) between 2008 and 2010 to boost Prime Minister Najib's image abroad after the BBC publicly apologized for airing programs with "inappropriate" sponsorship.[35] *Sarawak Report* also said Abdul Taib

29 ComScore, "Social Networking Accounts for One Third of All Time Spent Online in Malaysia," press release, October 17, 2011,http://www.comscore.com/Press_Events/Press_Releases/2011/10/Social_Networking_Accounts_for_One_Third_of_All_Time_Spent_Online_in_Malaysia.
30 "Malaysia Internet Usage Statistic," SEO Consultant (blog), November 24, 2012, http://www.seoconsultant.com.my/2012/11/malaysia-internet-usage-statistic/.
31 Najib Razak's Facebook page, accessed July 19, 2012, www.facebook.com/najibrazak; Najib Razak's blog, "1Malaysia," accessed July 19, 2012, http://www.1malaysia.com.my/.
32 Polis Diraja's Facebook page, http://www.facebook.com/PolisDirajaMalaysia.
33 Joanna Yap, "PRS' Cyber-Troopers Ready for Coming Polls," *Borneo Post Online*, March 22, 2012, http://www.theborneopost.com/2012/03/22/prs-cyber-troopers-ready-for-coming-polls/; Lim Guan Eng, "Najib's New Army of Cyber Troopers with a History of Dirty Tricks is Proof that the 13th General Election Will be the Dirtiest Election Yet," *DapMalaysia*, November 21, 2011, http://dapmalaysia.org/english/2011/nov11/lge/lge1414.htm.
34 Yu Ji, "Taking the Battle Online," February 8, 2012, http://thestar.com.my/news/story.asp?file=/2012/2/8/sarawak/10692418.
35 Mariam Mokhtar, "Sorry No Cure, BBC," *Free Malaysia Today,* February 17, 2012, http://www.freemalaysiatoday.com/category/opinion/2012/02/17/sorry-no-cure-bbc/; "BBC's Worldwide Apology Exposes Malaysian Govt's Image," *Harakah Daily*, February 13, 2012, http://en.harakahdaily.net/index.php/berita-utama/4376-bbcs-worldwide-apology-exposes-malaysian-govts-image.html.

Mahmud, the chief minister of Sarawak State, had separately contracted FBC Media for online publicity campaigns.[36] FBC Media, which denied wrongdoing, collapsed in 2011.[37] In March 2013, the U.S.-based media company BuzzFeed revealed that U.S. lobbying firms working on behalf of the Malaysian ruling party or its associates funded a print and online campaign, "spanning May 2008 to April 2011," in American media outlets, much of it criticizing opposition leader Anwar Ibrahim.[38]

Despite this kind of intervention, online tools have been effective for political mobilization and exposing the government's grip on traditional media. Disparate groups united to quash a 2011 government proposal to expand the Printing Presses and Publications Act to online content,[39] and leaders subsequently pledged to abolish it altogether,[40] though in practice this resulted only in tepid reforms in 2012. The act, one of several that restrict traditional media, helped give their more aggressive online counterparts the edge when reporting on political issues.

Nowhere is this more apparent than during the political rallies for electoral reform, whose organizers, the Coalition for Free and Fair Elections, have leveraged online platforms to bring tens of thousands of supporters to the streets; even the name of the rallies—Bersih 2.0 in 2011 and 3.0 in 2012—is borrowed from the technology community. In 2011, while mainstream media downplayed reports of police brutality against the largely peaceful protesters, internet users circulated nearly 900,000 tweets and 1,600 videos documenting violence, and 200,000 Facebook users petitioned for Najib's resignation.[41] In 2012, that gap widened. More bloggers and online news portals weighed in to keep people informed about the rally and the security forces' methods to control it, which included beatings, tear gas and water cannons.[42] Yet print media coverage declined compared to the previous year to what the local Centre for Independent Journalism described as a "near blackout."[43]

---

36 "New Revelations Link FBC Media to BN's Dirty Tricks Blogging Campaigns—Latest Expose!" *Sarawak Report*, August 7, 2011, http://www.sarawakreport.org/2011/08/dirty-tricks-new-revelations-link-fbc-media-to-bns-blogging-campaigns/.
37 Ian Burrell, "TV Company at Centre of Global News Fixing Row Goes into Administration," October 28, 2011, http://www.independent.co.uk/news/media/tv-radio/tv-company-at-centre-of-global-news-fixing-row-goes-into-administration-2376943.html.
38 "Govt Paid US Writers for Covert Campaign," *FMT News,* March 2, 2013, http://www.freemalaysiatoday.com/category/nation/2013/03/02/govt-paid-us-writers-to-handle-covert-campaign/.
39 "Publications Act to be Amended to Address Loopholes," *Star Online*, January 26, 2011, http://thestar.com.my/news/story.asp?file=/2011/1/26/nation/7873307&sec=nation.
40 Committee to Protect Journalists, "CPJ Welcomes Malaysian Reform Vow," news alert, September 16, 2011, http://cpj.org/2011/09/cpj-welcomes-malaysian-reform-vow.php.
41 Jerrenn Lam, "Malaysia: Bersih 2.0 Rally Rattles the Government," *Global Voices*, July 11, 2011, http://globalvoicesonline.org/2011/07/11/malaysia-bersih-2-0-rally-rattles-the-government/; Joshua Ongys, "Statistics on Bersih 2.0 Rally – Malaysia 9 July 2011," *Joshuaongys*, July 9, 2011, http://joshuaongys.com/2011/07/bersih-2-0-rally-malaysia-9-july-2011-online-social-media-statistics-youtube-facebook-twitter/.
42 Jerrenn Lam, "Malaysia: Thousands Joined Bersih 3.0 Protest," *Global Voices*, April 30, 2012, http://globalvoicesonline.org/2012/04/30/malaysia-thousands-joined-bersih-3-0-protest/.
43 Reporters Without Borders, "Major Protest Prompts Attacks on Journalists, Censorship and Missing Media Replaced by Civil Society," May 5, 2012, http://en.rsf.org/malaisie-major-protest-prompts-attacks-on-05-05-2012,42567.html.

Prior to the 2013 general elections, authorities changed tactics and allowed an opposition demonstration to go ahead without riot police. Organizers agreed to 27 conditions to obtain approval to gather under the new Peaceful Assembly Act which opposition leaders have criticized as a measure to restrict legitimate gatherings.[44] On January 12, 2013, 100,000 Malaysians participated in a People's Uprising Rally championing a change in government and various political reforms. While subsequent demonstrations were more restive, in this case at least, both police and organizers communicated effectively to inform the public about the event on social media.

VIOLATIONS OF USER RIGHTS

Legal harassment remained a primary means for the authorities to intimidate critical bloggers in 2012 and 2013, with at least one blogger facing charges for criticizing the Sultan of Johor. A much-touted legislative reform package failed to check many existing laws used against internet users, and even amended one law to hold intermediaries liable for content posted by others. Though heavy jail terms are unusual, that threat—along with the risk of fines for defamation—still prevents many bloggers from taking full advantage of Malaysia's dynamic online environment. While one higher court supported *Malaysiakini's* right to a license to expand to print form, another decision disappointed internet freedom activists when a judge determined that the 2010 detention of a cartoonist and blogger was lawful. The May 2013 election also had an impact on user rights, as opposition news websites faced cyberattacks, and a list of candidates circulating online was discovered to contain spyware.

Malaysia's constitution provides citizens with "the right to freedom of speech and expression," but allows for limitations on this right. The government exercises tight control over online media—along with print and broadcast media—through restrictions on licensing and the use of laws including the Official Secrets Act and the Sedition Act. Violations of these laws are punishable by fines and several years in prison.

The government has also pursued prosecutions based on the CMA's broadly worded section 211, which bans content deemed "indecent, obscene, false, threatening, or offensive," and Section 233, when such content is shared via the internet.[45] Defamation is a criminal offence under sections 499-520 of Malaysia's penal code.[46] Media outlets benefit from stronger privileges under the Defamation Act 1957 if they can prove allegedly libelous content is accurate and was published without malice;[47] lacking this protection, bloggers risk punitive damages.

---

44 "100,000 Throng Stadium Merdeka for 'Uprising' Rally," *Malaysiakini*, January 12, 2013, http://www.malaysiakini.com/news/218741; Human Rights Watch, "Malaysia: Backsliding on Rights," press release, February 1, 2013, http://www.hrw.org/news/2013/02/01/malaysia-backsliding-rights.
45 OpenNet Initiative, "Country Profile—Malaysia."
46 Bhag Singh, "Criminal Offence," *Star Online*, July 29, 2008, http://bit.ly/1hfKwhc.
47 Abdul Latiff Ahmad et al., "Regulating Blogs in Malaysia," The Innovation Journal: The Public Sector Innovation Journal, Vol. 16(3), 2011, http://www.innovation.cc/scholarly-style/latiff_ahamad_regulating_malasian_blogs16v2i11a.pdf.

In April 2012, several important changes were made to the legal framework surrounding freedom of expression and national security. In the year's most troubling development, parliament passed an amendment to the 1950 Evidence Act that holds intermediaries liable for seditious content posted anonymously on their networks or websites.[48] This would include hosts of online forums, news outlets, and blogging services, as well as businesses providing Wi-Fi services.[49] The amendment also holds someone liable if their name is attributed to the content or if the computer it was sent from belongs to them, whether or not they were the author.[50] The legal change was pushed through hurriedly, but garnered significant public backlash after its passage, including online petitions; this failed to prevent it going into effect in July 2012.[51]

At the same time, the Internal Security Act—which allowed for infinitely renewable detentions without trial and had been used to hold bloggers,[52]—was abolished and replaced by the Security Offenses (Special Measures) Act (SOSMA). The new law provides several improved protections to detainees, requiring police to immediately inform a detainee's family and reducing the maximum amount of time they can hold a suspect without charge or trial.[53] It also includes a provision explicitly stating that "no person shall be arrested and detained…solely for his political belief or political activity."[54] Despite these improvements, the law also includes restrictive provisions absent in its predecessor. For example, it grants wide-ranging powers for the public prosecutor—and in emergency situations, the police—to intercept communications without the need for a court order in cases involving security offenses.[55]

The government also made changes to the penal code that could allow for punishment of political speech by classifying ill-defined "activity detrimental to parliamentary democracy" as a criminal offence. Civil society groups fear this could render criticism of government officials or policies punishable with jail time, although the law minister said the provision would only apply to violent activities.[56] Meanwhile, the legislative revisions failed to check other problems, like the use of sedition and official secrets charges to harass bloggers and internet users.

No bloggers were serving long-term jail sentences in 2013, though Malaysian authorities have a history of criminally prosecuting online content producers. Police charged at least eight internet

48 Eva Galperin, "This Week in Internet Censorship: Points system for Weibo, Activist Released in Bahrain, Censorship in Malaysia, Ethiopia, and More," Electronic Frontier Foundation, May 31, 2012, https://www.eff.org/deeplinks/2012/05/week-internet-censorship-points-system-weibo-activist-released-bahrain-censorship.
49 Teoh El Sen, "Pakatan Seeks to Halt New Evidence Act," *Free Malaysia Today*, June 28, 2012, http://www.freemalaysiatoday.com/category/nation/2012/06/28/pakatan-seeks-to-halt-new-evidence-act/.
50 Parliament of Malaysia, "Act to amend the Evidence Act 1950, 2012," http://www.parlimen.gov.my/files/billindex/pdf/2012/DR162012E.pdf.
51 A. Asohan, "Govt Stealthily Gazettes Evidence Act Amendment, Law is Now in Operation," *Digital News Asia*, August 8, 2012, http://www.digitalnewsasia.com/digital-economy/govt-stealthily-gazettes-evidence-act-amendment-law-is-now-in-operation.
52 "Malaysia Detains 'Dissent' Writer," BBC News, September 23, 2008, http://news.bbc.co.uk/2/hi/asia-pacific/7630789.stm.
53 Parliament of Malaysia, "Security Offences (Special Measures) Act 2012," http://www.parlimen.gov.my/files/billindex/pdf/2012/DR152012E.pdf.
54 Security Offences (Special Measures) Act 2012.
55 Security Offences (Special Measures) Act 2012.
56 Shahanaaz Habib, "A Matter of Trial and Error," *Star Online*, April 22, 2012, http://thestar.com.my/news/story.asp?file=/2012/4/22/nation/11153338&sec=nation.

users for criticism of the monarchy in 2009,[57] and questioned others.[58] Many prosecutions were dropped, but at least one defendant elected to pay a fine of RM10,000 ($ 2,700) rather than face the threat of trial.[59] Legal proceedings can be lengthy and uncertain, regardless of the outcome. Police continue to investigate Raja Petra Kamarudin, founder of the *Malaysia Today* blog, who fled into exile in 2009 to avoid sedition charges and continues to criticize the administration from overseas.[60] Sedition charges against another blogger, Khairul Nizam Abdul Ghani, dating from 2010 comments about the late Sultan of Johor, were only abandoned in June 2012.[61]

While the use of sedition laws against internet users declined in 2011,[62] police detained two critics of Johor's new Sultan on the charge in 2012. One Facebook user was arrested in November 2012 for posts considered insulting to the Sultan. When a judge declined to extend his remand after three days, police released and immediately rearrested him; he later told journalists he was questioned in solitary confinement for a total seven days before being released without charge.[63] In July, police briefly detained Syed Abdullah Syed Hussein al-Attas, who blogs pseudonymously as "Uncle Seekers," also on allegations that 64 of his posts insulted the Sultan under the Official Secrets Act.[64] Charges against him are still pending.

Politically-motivated defamation suits seeking damages disproportionate to the offense have become another threat to online expression since a landmark 2007 blogger prosecution by a government-linked newspaper.[65] In August 2012, a Kuala Lumpur court sentenced blogger and opposition People's Justice Party member Amizudin Ahmat to three months in jail for breaking a gag order relating to Dr. Rais Yatim, Malaysia's information and culture minister, resulting from one such case. In 2011, Ahmat was ordered to pay MYR 300,000 ($97,000) in damages for falsely

57 International Freedom of Expression eXchange, "Government Hounds Bloggers That Criticise Royalty," news alert, March 25, 2009, http://www.ifex.org/malaysia/2009/03/25/government_hounds_bloggers_that/.
58 Centre for Independent Journalism, "Debate on Royal Powers Draws Attacks and Threats; Bloggers Ahiruddin Attan and Jed Yoong Questioned by Police," via International Freedom of Expression eXchange, March 4, 2009, http://www.ifex.org/malaysia/2009/03/04/capsule_report_debate_on_royal/.
59 Centre for Independent Journalism, "Six People Charged with 'Insulting' Royalty Online," International Freedom of Expression eXchange, March 16, 2009, http://www.ifex.org/malaysia/2009/03/16/six_people_charged_with_insulting/.
60 Teh Eng Hock, "Raja Petra Can't Be Tried in Britain," *Star Online*, May 26, 2010, http://thestar.com.my/news/story.asp?file=/2010/5/26/nation/6340987&sec=nation. K. Kabilan, "RPK: 1Malaysia Will Be Najib's Downfall," *Free Malaysia Today*, May 25, 2010, http://politicalwatchmalaysia.blogspot.com/2010/05/rpk-1malaysia-will-be-najibs-downfall.html; "Perkasa Makes Police Report Against Raja Petra," *Malaysia Today*, January 7, 2010, http://malaysia-today.net/mtcolumns/newscommentaries/29452-perkasa-makes-police-report-against-raja-petra.
61 "Malaysian Blogger Charged with Insulting Dead Sultan," *China Post*, January 31, 2010, http://www.chinapost.com.tw/asia/malaysia/2010/01/31/243065/Malaysian-blogger.htm; Sarban Singh, "Blogger pleads not Guilty to Insulting Johor Royals (Update)," *Star Online*, January 29, 2010, http://thestar.com.my/news/story.asp?file=/2010/1/29/nation/20100129170602&sec=nation.
62 Only one blogger was held for 24 hours in March 2011. See, "Blogger 'Arrested' at Midnight Under Sedition Act," *Malaysia Today*, March 19, 2011, http://malaysia-today.net/mtcolumns/from-around-the-blogs/38903-blogger-arrested-at-midnight-under-sedition-act.
63 G. Vinod, "PAS Member: I Did Not Threaten to Kill Saiful," *Free Malaysia Today*, May 19, 2010, http://www.freemalaysiatoday.com/fmt-english/news/general/5771-pas-member-i-did-not-threaten-to-kill-saiful; Nerea Rial, "Malaysian Arrested Over Facebook Insults," *New Europe Online*, November 5, 2012, http://www.neurope.eu/article/malaysian-arrested-over-facebook-insults; Susan Loone, "Ahmad Subjected to Daily Grilling of 8-9 Hours," *Malaysiakini*, November 10, 2012, http://www.malaysiakini.com/news/213941.
64 Committee to Protect Journalists, "In Detaining Blogger, Malaysia Invokes Secrets Act," news alert, July 11, 2012, http://www.cpj.org/2012/07/in-detaining-blogger-malaysia-invokes-secrets-act.php.
65 Soon Li Tsin, "Bloggers Sued for Defamation," *Malaysiakini*, January 18, 2007, http://www.malaysiakini.com/news/62257.

accusing the minister of criminal actions in a blog post, even though he subsequently deleted and apologized for the content. An appeals court reduced additional costs Ahmat was required to pay for related legal expenses but upheld the ruling, which included an order not to blog further about the minister.[66] When Ahmat ignored this order in eleven subsequent articles, the high court found him in contempt; the jail term was deferred pending appeal. A suit brought by an opposition parliamentarian was less successful. In 2012, Nga Kor Ming sought 10 million MYR ($3,200,000) in damages over corruption allegations made by Ahmad Sofian Yahya on the blog *Sekupangdua*. Though Nga withdrew the claim, the blogger countersued when articles on the politician's website implied the court had ruled in Nga's favor; he, too, withdrew the suit.[67]

Another 2012 high court ruling disappointed free expression advocates. In September 2010, police arrested cartoonist Zulfiklee Anwar Ulhaque, better known as Zunar, and seized newly-published volumes of his cartoons—including many previously published on his blog—deemed insulting to the prime minister and his deputy. After they released him without charge,[68] Zunar and his publishing house sued the government for unlawful detention and loss of income.[69] In a ruling that missed the point that satirical content should not be criminalized, a judge ruled in July 2012 that the arrest was lawful, though confiscating the books was not.[70]

A small number of other criminal cases have involved religion.[71] One in particular may contribute to Malaysia's global reputation for negative intervention in online freedom of expression issues: In 2012, the authorities stopped Saudi Arabian journalist Hamza Kashgari at a Malaysian airport en route to seek asylum in New Zealand after his online comments about the Prophet Mohammed attracted death threats and government harassment in his own country.[72] Although his lawyer said he had filed a court injunction to prevent Kashgari from being deported, Malaysian authorities sent him home, saying they did not receive it in time.

Real-name registration is not required for participation in in Malaysia's blogosphere, nor is it required to use a cybercafe. Civil society groups have successfully resisted tentative efforts to implement registration, such as the 2011 Computing Professionals Bill that, if passed, would have

---

66 International Freedom of Expression eXchange, "Opposition Blogger Ordered to Pay Exorbitant Damages to Minister," news alert, July 22, 2011, http://www.ifex.org/malaysia/2011/07/22/amizudin_defamation_suit/; http://en.rsf.org/malaysia-opposition-blogger-ordered-to-pay-20-07-2011,40659.html.

67 "Blogger Sues DAP's Nga for Defamation," September 22, 2012, *Bernama*, via *Malaysian Insider*, http://www.themalaysianinsider.com/litee/malaysia/article/blogger-sues-daps-nga-for-defamation/.

68 "Malaysian Cartoonist Goes into Hiding After Sedition Arrest," RFI English, September 28, 2010, http://www.english.rfi.fr/asia-pacific/20100928-malaysian-cartoonist-goes-hiding-after-sedition-arrest.

69 K. Pragalath, "Partial Victory for Cartoonist Zunar," *Free Malaysia Today*, July 31, 2012, http://www.freemalaysiatoday.com/category/nation/2012/07/31/partial-victory-for-cartoonist-zunar/; Tom Spurgeon, "CR Holiday Interview #7: Zunar," *Comics Reporter*, December 27, 2010, http://www.comicsreporter.com/index.php/cr_holiday_interview_7_zunar/.

70 Reporters Without Borders, "Court's Ruling on Cartoonist's Suit Sets Disturbing Precedent for Media Freedom," July 31, 2012, http://en.rsf.org/malaisie-court-s-ruling-on-cartoonist-s-31-07-2012,43134.html.

71 In August 2010, the right–wing group Perkasa lodged a complaint against blogger Helen Ang for authoring an article that questioned the position of Islam in Malaysia; as of 2013, the case was still pending, but observers felt it was unlikely the attorney general would pursue it. "Perkasa Lodges Report Against Blogger," *Malaysian Insider*, August 9, 2010, http://www.themalaysianinsider.com/malaysia/article/perkasa-lodges-report-against-blogger/.

72 Committee to Protect Journalists, "Malaysia Deports Saudi Arabian Columnist," news alert, February 13, 2012, http://www.cpj.org/2012/02/malaysia-deports-saudi-arabian-columnist.php.

required IT professionals working on Critical National Information Infrastructure projects to register with a government-appointed board.[73] Responding to critics, the Ministry of Science, Technology, and Innovation said that registration would be voluntary, and the bill never made it to parliament.[74] Beginning in 2007, all mobile phone owners, including the roughly 18 million customers using prepaid service at the time, were required to register as part of an effort to decrease rumor mongering. [75] The rule appears to have been weakly enforced.

The extent of government surveillance of ICT content is not known, but privacy protections are generally poor in Malaysia.[76] In 2008, the MCMC formed a panel composed of representatives from the police, the attorney general's office, and the Home Ministry to monitor websites and blogs. Although it still appears to be active, it has not publicly intervened in internet freedom issues. Court documents indicate that police regularly gain access to the content of text messages from telecommunications companies, sometimes without judicial oversight. A 2011 government initiative to provide free email accounts to all citizens over the age of 18 prompted fears it would expand the government's ability to monitor people's online activities.[77] The project, which was designed to offer an "authenticated online identity through which the people can securely carry out their transactions with the government," had only 23,000 subscribers by March 2013.[78] SOSMA, which allows for the interception of communications without a judicial order in poorly-defined security investigations, also contains scope for abuse.[79]

The Malaysian Personal Data Protection Act 2010, which regulates the processing of personal data in commercial transactions, came into effect on January 1, 2013. The law makes it illegal for commercial organizations to sell personal information or allow third parties to use it, with penalties up to RM100,000 ($ 27,400) or one year imprisonment. Federal and state governments are exempted from the law, as is data processed outside Malaysia.[80]

In March 2013, the University of Toronto-based research group Citizen Lab reported detecting software known as FinFisher, described by its distributor Gamma International as "governmental IT intrusion and remote monitoring solutions," on 36 servers worldwide, including one in Malaysia.[81]

---

73 Lim Yung-Hui, "Malaysian IT Community Response to Board of Computing Professionals Malaysia Bill 2011: Where's the Beef?," *Forbes*, December 12, 2011, http://www.forbes.com/sites/limyunghui/2011/12/12/malaysian-it-community-response-to-board-of-computing-professionals-bill-2011-wheres-the-beef/; Vijandren Ramadass, "Computing Professionals Bill 2011 – Draft," *Lowyat*, December 9, 2011, http://www.lowyat.net/v2/index.php?option=com_content&task=view&id=5800&Itemid=2.
74 "MCA: Computing Professionals Bill Will Stifle Talent Growth," *New Straits Times,* December 21, 2011, http://www.nst.com.my/latest/mca-computing-professionals-bill-will-stifle-talent-growth-1.22120.
75 "Dec 15 Registration Deadline Stays: MCMC," *Bernama*, August 18, 2006, http://www.bernama.com/kpdnhep/news.php?id=214811&lang=en.
76 Privacy International, "Privacy in Asia: Final Report of Scoping Project," November 2009, https://www.privacyinternational.org/issues/asia/privacy_in_asia_phase_1_report.pdf.
77 Rebekah Heacock, "Malaysia: Government's Free E-mail Plan Met with Opposition," OpenNet Initiative (blog), April 26, 2011, http://opennet.net/blog/2011/04/malaysia-governments-free-e-mail-plan-met-with-opposition.
78 Economic Transformation Programme Report 2012, 187.
79 Mickey Spiegel, "Smoke and Mirrors: Malaysia's "New" Internal Security Act," *Asia Pacific Bulletin,* no. 167, East West Center (June 2012), http://www.eastwestcenter.org/publications/smoke-and-mirrors-malaysias-new-internal-security-act.
80 Barry Ooi, "How the Personal Data Protection Act Impacts the Market Research Industry," December 29, 2012, http://biz.thestar.com.my/news/story.asp?file=/2012/12/29/business/12511744&sec=business.
81 Morgan Marquis-Boire et al., "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab, March 13, 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

The software potentially allows the server to steal passwords, tap Skype calls, or record audio and video without permission from other computers, according to Citizen Lab, which noted that the presence of such a server did not prove who was running it. The same month, the *Malaysian Insider* documented Fin Fisher's presence in Malaysia, based on a *New York Times* report.[82] In response, the MCMC launched an investigation into the report, which it described as "speculative and ill-researched," and threatened the site with a fine of up to RM 50,000 ($15,200) or one year imprisonment for false reporting under the CMA. No charges have been reported against the website or its staff. In May, however, Citizen Lab reported they had further identified "a Malaysian election-related document" they characterized as a "booby-trapped candidate list" containing surveillance spyware.[83] Because the spyware is only marketed to governments, "it is reasonable to assume that some government actor is responsible," the group concluded.

Physical violence, though less extreme than in many neighboring countries, still affects journalists reporting for traditional media in Malaysia, and their online colleagues are not immune: a *Malaysiakini* photojournalist was among several who reported security forces obstructing and beating them on the sidelines of the political rally Bersih 3.0.[84]

A graver threat to independent online news outlets and some opposition-related websites is distributed denial-of-service (DDoS) attacks, which force sites to crash by overloading the host server with requests for content, often at moments of political importance. Some observers believe such attacks are either sponsored or condoned by Malaysian security agencies, since they often align with government priorities. In March 2013, the new U.K.-based online radio station Free Malaysia Radio—which promised listeners content prohibited in traditional media—suffered DDoS attacks during its first program, an interview with opposition leader Anwar Ibrahim.[85] The online radio portal was inaccessible for some days. Malaysiakini, which has endured 35 DDoS attacks, was one of many sites reporting on the opposition which was subjected to an apparently coordinated assault in April 2013 before the elections.[86]

---

82 The contested report: Boo Su-Lyn, "Malaysia Uses Spyware Against Own Citizens, NYT Reports," *Malaysian Insider,* March 14, 2013, http://www.themalaysianinsider.com/malaysia/article/Malaysia-uses-spyware-against-own-citizens-NYT-reports. The original *New York Times* report: Nicole Perlroth, Researchers Find 25 Countries Using Surveillance Software," *New York Times* (blog), March 13, 2013, http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/.
83 "Short Background: Citizen Lab Research on FinFisher Presence in Malaysia," Citizen Lab, May 2013, https://citizenlab.org/wp-content/uploads/2013/05/shortbg-malaysia1.pdf.
84 Committee to Protect Journalists, "Journalists Assaulted, Detained During Rally in Malaysia," April 30, 2012, http://www.cpj.org/2012/04/journalists-assaulted-detained-during-rally-in-mal.php.
85 "New Radio Station Under DDOS Attack, *Free Malaysia Today,* March 26, 2013, http://www.freemalaysiatoday.com/category/nation/2013/03/26/new-radio-station-under-ddos-under-attack/.
86 Human Rights Watch, "Malaysia: Violence, Cyber Attacks Threaten Elections," May 1, 2013, http://www.hrw.org/news/2013/05/01/malaysia-violence-cyber-attacks-threaten-elections. See also, Shawn Crispin, "Internet Opening is Shrinking," *Attacks on the Press*, Committee to Protect Journalists (Wiley: New York, February 2013), http://cpj.org/2013/02/attacks-on-the-press-internet-opening-is-shrinking.php.

MEXICO

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	11	11
Limits on Content (0-35)	11	10
Violations of User Rights (0-40)	15	17
Total (0-100)	37	38

* 0=most free, 100=least free

POPULATION: 116.1 million
INTERNET PENETRATION 2012: 38 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- A civil society coalition successfully lobbied for freedom of access to the internet to be guaranteed as a right under the Mexican constitution (see **OBSTACLES TO ACCESS**).
- In 2012 and 2013, Mexico continued to be one of the most hostile environments in the world for journalists and bloggers, who were subject to retaliatory violence from drug cartels and organized crime (see **VIOLATIONS OF USER RIGHTS**).
- A new telecommunications bill was approved by the Senate on April 30, 2013, and offers the potential to increase ICT competition and affordability once implemented (see **OBSTACLES TO ACCESS**).
- In October 2012, two contributors to digital newspaper *e-consulta* were kidnapped and robbed by Tlaxcala state police. In April 2013, retaliatory defamation cases were leveled against five others associated with the site (see **VIOLATIONS OF USER RIGHTS**).
- Evidence of widespread surveillance, including the real-time warrantless recording of citizens' phone calls, came to light in 2012 after secret government documents were made public (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Internet penetration in Mexico has experienced dramatic growth since the first connection was established in February 1989; however, the majority of the population still lacks affordable access, an issue that is particularly pronounced in rural areas. Such disparity is largely due to infrastructural deficiencies and high prices exacerbated by the concentrated ownership of the telecommunications sector in the hands of a few influential companies. A recently approved telecommunications bill intended to combat monopolization, however, is expected to result in increased competition and affordability. Further legislation that began as a citizen initiative in January 2013 also resulted in the inclusion of a provision in the Mexican Constitution guaranteeing access to the internet as a civic right. Although this is a significant development, as of yet there is no secondary legislation defining exactly how the government will guarantee this right in practice.[1]

Although positive legislation pertaining to communications was recently passed, in 2012, documents were leaked detailing pervasive surveillance technologies used by the Mexican government. The real-time, warrantless recording of citizens' phone calls, along with interception of email, text messages, and other personal communications were among the more concerning provisions of the government's surveillance procedures.

Mexico still ranks as one of the most dangerous climates in the world for journalists. While widespread intimidation, threats, violence, and self-censorship were historically limited to traditional media, writers for critical websites and narcoblogs have been victim to increasing harassment, cyberattacks, physical violence, and murder as their reporting has gained prominence. Recent legislation pertaining to the protection of journalists marks an important departure from Mexico's historical record of impunity for attackers; however the real world impact of such legislation remains to be seen.

Between May 2012 and April 2013, Mexico was witness to at least one forced disappearance related to online content, as well as three retaliatory murders for online journalism. In early 2013, threats against online media reporting on high-risk security situations allegedly extended to a bounty of 600,000 pesos ($47,000) for information relating to the identification of the administrator of high profile site *Valor por Tamaulipas*.

Despite such threats, online forums such as social-networking site Facebook and microblogging platform Twitter have emerged as tools for civil society activism and mobilization. A network of regional sites including *Valor por Tamaulipas* has had some success in warning citizens of safety concerns and cartel violence—coverage that is particularly timely given a recent decision by some state governments to avoid reporting on violence in official media.

[1] E-mail interview with Jorge Luis Serra, Knight International Journalism Fellow, reporter, editor, and digital expert, as well as the author of internet platforms allowing citizens to report and track crime in Mexico; Internet para Todos Mexico, http://internetparatodos.mx.

Social networks are also increasingly used for political activism in Mexico. In May 2012, the video sharing site YouTube was instrumental in the mobilization of the YoSoy132 movement, which gained traction on Facebook and Twitter, resulting in nationwide protests concerning free elections and free speech.

OBSTACLES TO ACCESS

Internet penetration in Mexico has increased significantly over the past decade, growing from approximately 5 percent in 2000 to 38.4 percent in 2012.[2] This figure is low for a country with Mexico's level of economic development; however, experts anticipate that penetration will reach 65 percent by 2014, a figure predicated in large part on the growing prevalence of smart phones.[3] If actualized, such a projection would bring Mexico into the range of its peers in the Organization for Economic Cooperation and Development (OECD).[4]

In recent years, growth among household penetration rates has progressed more slowly than other points of internet access, such as mobile and office connections; a reality due in part to the fact that only 30 percent of Mexican homes have computers. As of August 2012, household internet access was reported to have grown a slight 2.3 percent from 2011 figures, increasing to 23.3 percent.[5] Technological advancement in Mexico remains uneven, with 11 million of the country's approximately 40.6 million internet users concentrated in Mexico City and other urban areas. According to the National Institute of Geography and Statistics (INEGI), in urban areas, landline coverage hovers around 50 percent, while in rural areas this figure drops to 25 percent.[6]

Such limited connectivity—combined with high subscription fees—has resulted in a relatively small percentage of internet users with broadband access. This figure has enjoyed modest growth in

[2] Insituto Nacional de Estadicia y Geografia and Comsion Federal de Telecomunicaciones, "Boletin de Prensa Numero 270/12," press bulletin, August 2, 2012, http://www.inegi.org.mx/inegi/contenidos/espanol/prensa/boletines/boletin/comunicados/especiales/2012/agosto/comunica1.pdf. See also, International Telecommunication Union, *Statistics: Percentage of Individuals Using the Internet, 2000-2012*, June 17, 2013, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls; World Internet Project, *"Estudio 2012 de Habitos y Percepciones de los Mexicanos sobre Internet y Diversas Tecnologias Asociadas"* [2012 Study of the Habits and Perceptions of Mexicans Regarding the Internet and Other Associated Technologoies], 2012 Report, http://www.scribd.com/fullscreen/110836917?access_key=key-23sx28wav3vk306badtz.

[3] World Internet Project, "*Estudio 2012 de Habitos y Percepciones de los Mexicanos sobre Internet y Diversas Tecnologias Asociadas*."

[4] The average penetration rate in OECD countries, as defined by households with internet access, was measured at 74.9 percent in 2011. See, "OECD Key ICT Indicators, File 6b," http://www.oecd.org/internet/broadband/oecdkeyictindicators.htm; Azteca Noticias, "*Penetracion de Inernet en Mexico es Baja: Amipci*" [Internet Penetration in Mexico is Still Low: Amipci], May 7, 2012, http://www.aztecanoticias.com.mx/notas/tecnologia/110807/penetracion-de-internet-en-mexico-es-baja-amipci.

[5] INEGI, "*Penetracion de Internet en Mexico*" [Internet Penetration in Mexico], August 2012, http://www.inegi.org.mx/inegi/contenidos/espanol/prensa/boletines/boletin/comunicados/especiales/2012/agosto/comunica1.pdf; Gabriel Sosa Plata, "*La Penetracion de Internet en Mexico*" [Internet Penetration in Mexico], Mexican Communication Magazine, August 18, 2011, http://mexicanadecomunicacion.com.mx/rmc/2011/08/18/la-penetracion-de-internet-en-mexico/#axzz1jqEkt6lM.

[6] Of the 30.6 million users over the age of six, an estimated 25.6 million live in urban areas. Mexican Internet Association, *AMIPCI 2009 Report on Internet Users' Habits* [in Spanish], May 2010, http://www.amipci.org.mx/estudios/temp/Estudiofinalversion1110-0198933001274287495OB.pdf (site discontinued).

recent years, however, increasing by 5.2 percent between June and December 2012.[7] Mexico now counts 11.6 broadband subscribers per 100 inhabitants. By comparison, the average for OECD countries is 26.3.[8] As evidenced by the aforementioned figures, broadband service in Mexico, which ranges from 389 pesos ($30) to 599 pesos ($78) per month, compared to a minimum monthly wage of 1,770 to 1,860 pesos ($114 to $126) depending on location, still remains out of reach for many Mexicans.[9]

Cybercafes, which are generally easy to access in small cities and tourist destinations, offer a more affordable means of accessing the internet than do home subscriptions. Accordingly, as of May 2012, 54 percent of internet users reported accessing the web outside their homes.[10] Rates for internet access at cybercafes, which are not bound by special restrictions and require only a regular business license for operation, range from 10 to 15 pesos ($0.77 to $1.15) per hour.[11]

Mexico's mobile phone sector is primarily controlled by six private companies, however America Movil, owned by Mexican billionaire and world's richest man Carlos Slim Helu, which counts both Telmex and Telcel as subsidiaries, dominates the information and communication technologies (ICT) landscape with 80 percent of landline subscriptions and 70 percent of the wireless market.[12] Top competitors Axtel and Movistar account for only 6 percent of fixed lines and 20 percent of wireless connections, respectively.[13] According to the Federal Commission of Telecommunications (COFETEL), mobile phone access is significantly more widespread in Mexico than internet use, with 96.7 million subscribers, or 87 percent of the population, as of the end of 2012,[14] a figure that has been projected to increase to 100 percent by 2014.[15]

Such accelerated growth is due in part to a recent drop in prices for mobile phone use,[16] increasing availability of smartphones, and promotions that narrow the price gap between basic phones and

---

[7] OECD, "Fixed and Wireless Broadband Subscriptions per 100 Inhabitants" and "Yearly Penetration Increase," in *OECD Broadband Statistics*, See: (1) and (2) OECD, updated July 18, 2013, http://www.oecd.org/internet/broadband/oecdbroadbandportal.htm#Services_and_speeds.

[8] OECD, "Fixed and Wireless Broadband Subscriptions Per 100 Inhabitants." ; OECD , *OECD Review of Telecommunication Policy and Regulation in Mexico,* (OECD Publishing: 2012), http://www.oecd.org/sti/broadband/50550219.pdf.

[9] OECD, "Fixed Broadband Basket Prices," *OECD Broadband Statistics* updated July 18, 2013, http://www.oecd.org/internet/broadband/oecdbroadbandportal.htm#Services_and_speeds; Misalario, "Mexico Salarios Minimos" [Minimum Wage in Mexico], modified November 27, 2012, http://bit.ly/18eV6D2.

[10] Mexican Internet Association, *AMIPCI 2010 Report on Internet Users' Habits* [in Spanish].

[11] "Why an Internet Café Is Still Good Business in Mexico," *Internet Cafes*(blog), July 1, 2010, http://internetcafes.com.mx/2010/07/por-que-un-cafe-internet-aun-es-buen-negocio-en-mexico/ (subscription required).

[12] Susan Crawford, "Mexico's Lucky to Have Just One Man Blocking Internet Equality, We've Got a Bunch," *Wired*, May 13, 2013, http://www.wired.com/opinion/2013/05/when-it-comes-to-internet-access-and-cost-were-just-like-mexico/; Henry Lancaster, "Mexico – Mobile Market Insights, Statistics and Forecasts," BuddeComm, last updated July 4, 2012, http://www.budde.com.au/Research/Mexico-Mobile-Market-Insights-Statistics-and-Forecasts.html.

[13] Dolia Estevez, "U.S. Government Puts Pressure on Carlos Slim, Mexico's Telecom Sector to Open up to Competition," *Forbes*, April 1, 2013, http://onforb.es/14AIypz.

[14] "Alcanza Mexico 87% de Penetracion en Telefonica Celular: Cofetel" [Mexico Reaches 87% Penetration in Mobile Phones: COFETEL], *Milenio,* August, 27, 2012 http://www.milenio.com/cdb/doc/noticias2011/d0c48fff2e2b7bc219046de523e53ff9.

[15] Ariadna Cruz, "La Telefonia Movil Sigue al Alza en Mexico" [Mobile Lines Still Growing in Mexico], *El Universal*, November 14, 2011, http://www.eluniversal.com.mx/finanzas/91029.html.

[16] In May 2011, COFETEL ordered telecom firms to reduce interconnection fees between landlines and mobile phones to a more affordable level. The fees were dropped to 0.39 pesos ($0.03) for mobile phones. The decision was later affirmed by the

smartphones.[17] As of August 2012, industry insiders estimated that 17 million (approximately 17.5 percent) of the country's 96.7 million mobile phones were smartphones.[18] In 2013, the number of smartphones in Mexico is expected to increase by approximately 40 percent, a figure that would make Mexico the second largest smartphone market in Latin America after Brazil and the tenth largest in the world.[19]

While Mexico's embrace of both smartphones and mobile internet has been enthusiastic, its investment in telecommunications is the lowest of any OECD nation; its adoption of high speed internet is consequently also low compared to other OECD members.[20] Under the 2009 Law for the Development of an Information Society, former President Felipe Calderón addressed Mexico's serious gaps in internet access by explicitly providing responsibility for the development of ICTs to the State.[21] In May 2010, the Department of Communications and Transportation announced an investment of 1.5 billion pesos ($115.5 million) to extend internet access to neglected regions deemed unprofitable by private companies.[22] Such access was to be facilitated via the creation of a national network of fiber-optic cables in conjunction with allowances for third parties to offer internet services.[23] Nearly three years later, however, achievements have been marginal, as evidenced by the statistics cited above.[24]

In January 2012, the OECD published a report recommending quick legal and regulatory reforms in order to boost competition and investment in Mexico's ICT sector.[25] In March 2013, only four months into his six-year term, President Enrique Peña Nieto introduced a substantial telecommunications reform bill. Approved without delay by the House and passed 108 to 3 in the Senate in late April 2013, the reform marks a notable change in the government's attitude toward the telecommunications sector.[26] Once implemented, the reform will increase competition via

---

Supreme Court. See: "Cofetel Reduces Interconnection Fees" [in Spanish], *Revista Opcion*, June 10, 2011, http://www.revistaopcion.com/tag/de-mayo/.

[17] Maris Olvera, "*A la baja precios de smartphones*" [Smartphone Prices Decreasing], *El Universal-Querétaro*, May 27th, 2013, http://m.eluniversalqueretaro.mx/vida-q/27-05-2013/la-baja-precios-de-smartphones.

[18] Interview with Guillermo Perezbolde, Vicepresident of Marketing, Public Relations and Social Media at Asociación Mexicana de Internet.

[19] Julio Sanchez Onofre, "México, Mercado "Top 10" Global de Smartphones en 2013: IDC" [Mexico: 'Top Ten' Global Market for Smartphones in 2013: IDC], *El Economista*, June 11, 2013, http://eleconomista.com.mx/tecnociencia/2013/06/11/mexico-mercado-top-10-global-smartphones-2013-idc.

[20] Susan Crawford, "Mexico's Lucky to Have Just One Man Blocking Internet Equality, We've Got a Bunch," *Wired* online, May 13, 2013, http://www.wired.com/opinion/2013/05/when-it-comes-to-internet-access-and-cost-were-just-like-mexico/.

[21] Special Committee of Congress for the Promotion of Digital Access to Mexicans, *De Ley Para el Desarallo de la Informacion, a Cargo de los Diputados Integrantes de la Comision Especial para la Promocion del Acceso Digital a los Mexicanos y Otros Legisladores* [*Bill to Promote the Development of the Society of Information*], 2009, http://jmcane.files.wordpress.com/2009/04/ley-desarrollo-sociedad-de-la-informacion-mexico.pdf.

[22] "SCT Will Invest 1.5 Billion Pesos for the Internet" [in Spanish], *El Universal*, June 23, 2010, http://www.eluniversal.com.mx/notas/689775.html (site discontinued).

[23] James Thomasson, William Foster, and Laurence Press, *The Diffusion of the Internet in Mexico* (Austin: Latin American Network Information Center, University of Texas, 2002), http://lanic.utexas.edu/project/etext/mexico/thomasson/thomasson.pdf.

[24] Karol Garcia, "Broadband," [in Spanish] *Media Telecomm*, May 2, 2012, http://bit.ly/IJAKCp (site discontinued).

[25] OECD, *OECD Review of Telecommunication Policy and Regulation in Mexico*, January 30, 2012, http://www.oecd.org/document/18/0,3746,en_2649_34223_49453202_1_1_1_1,00.html.

[26] Al Jazeera, "Mexican Senate Approves Telecoms-Reform Bill," *Al Jazeera*, May 1, 2013, http://www.aljazeera.com/news/americas/2013/05/2013515845225187.html; Dolia Estevez, "Mexico's Congress Passes Monopoly-Busting Telecom Bill, Threatening Tycoon Carlos Slim's Empire," *Forbes*, May 1, 2013, http://onforb.es/10WdzEo.

asymmetric regulation, forced divestment of companies with a monopoly on telecommunications, and lightened restrictions on foreign investment.[27] The reform also contains the product of Mexico's first successful citizen initiative pertaining to legislation – a provision guaranteeing all citizens access to the internet. The provision was championed by 17 civil society organizations that joined forces in January 2013. After gathering 127,198 signatures from constituents advocating for freedom of internet access to be a constitutional right, the proposal was submitted to Congress. Freedom of access to the internet is now included in Article 6 of the Mexican constitution.[28]

A number of other conditions contained in the bill, such as the formation of a new independent regulatory commission known as the Federal Telecommunications Institute, (IFETEL) ensure increased transparency of media regulation.[29] Currently, two regulatory bodies oversee the Mexican telecommunications industry: the Federal Commission of Telecommunications (COFETEL), and the Federal Competition Commission (CFC). Neither body is vested with the power to alter permits, order divestment, or issue fines.[30] Such powers reside with a Cabinet secretary, a position that has frequently been accused of bowing to telecommunications firms.

COFETEL, which operates with limited transparency and is not entirely independent from the executive, has likewise been accused of being partial to special interests. The president directly appoints COFETEL commissioners without the need for Senate approval; commissioners then choose COFETEL's president, who serves a four-year term and is subject to re-election, from their ranks.[31] While the Federal Competition Commission has a better reputation, in practice the institution remains weak and has limited power to enforce sanctions on large companies such as Telmex.

IFETEL, the new autonomous regulatory apparatus to be created under the telecommunications reform, will act as an antitrust body, protecting against monopolistic practices. In addition to issuing rulings, IFETEL will have the power to unilaterally punish non-competitive practices with the withdrawal of corporations' licenses, the application of asymmetric regulation, and the unbundling of media services—stipulations that portend a sea change in the Mexican ICT landscape.[32]

---

[27] "Working through a Reform Agenda," *Economist*, April 6, 2013, http://econ.st/Y2t8n5.
[28] Internet para Todos Mexico, *Libre Internet para Todos* [*Free internet for All*], accessed August 9, 2013, http://internetparatodos.mx/.
[29] Juan Montes, "Mexico Telecoms Reform Bill Advances," *Wall Street Journal,* March 22, 2013 http://online.wsj.com/article/SB10001424127887324373204578375542294095614.html.
[30] COFETEL, "Scope of Action," [in Spanish] Federal Competition Commission, accessed August 31, 2010, http://www.cofetel.gob.mx/wb/Cofetel_2008/Cofe_ambito_de_accion.
[31] OCDE, "Review Questions for Mexico's Regulatory Reform in the Telecommunications Sector," March 22, 2010, http://bit.ly/1bhGqnX: 7.
[32] Víctor Pavón-Villamayor, "Ifetel, La Mayor Apuesta en Telecomunicaciones," [Ifetel, The Biggest Bet in Telecommunications], *Forbes México*, April 25, 2013, http://www.forbes.com.mx/sites/la-mayor-apuesta-en-telecomunicaciones-ifetel/; Juan Montes, "Mexico Telecoms Reform Bill Advances," *The Wall Street Journal*, March 22, 2013, http://on.wsj.com/Yt7bAG.

LIMITS ON CONTENT

Although there are significant threats to online journalists and bloggers in Mexico, including both cyberattacks and physical violence, in 2012 and 2013 social media subscriptions sustained their upward momentum. Internet-mediated political activism also increased and played an influential role in both the YoSoy132 protests as well as the development and subsequent success of Mexico's first successful civil action to amend the Constitution, a campaign that resulted in a state guarantee of internet access for all.[33] Despite significant obstacles to funding, a handful of independent news sites covering civil society initiatives and protests continued to attract growing audiences. As internet use grows in Mexico, however, requests from government agencies for user data and removal of content are also on the rise.

Mexican authorities sometimes employ technical methods to filter or curb access to online content, but aside from the sporadic application of defamation laws to content posted online, no additional legislation yet restricts the internet as a medium for mass communication. This absence of regulation, even on content internationally recognized as harmful, is evident from Mexico's ranking as second worldwide in the production and distribution of child pornography.[34]

Although there are no laws that specifically govern online content, government agencies have been issuing more requests for content removal and user data in recent years, as evidenced by Google's recent transparency report.[35] In 2011, Google received only one request from the Mexican government for content removal. Between July and December 2012, the report's most recent coverage period, the figure increased to twelve. Recent requests for removal of videos hosted on YouTube or content posted on Blogger pertained to content which was allegedly defamatory or critical of the government, or presented a risk to privacy and security. In most cases, Google found that the content in question did not violate YouTube's community guidelines or local laws and declined to remove them. Government requests for user data are also on the rise, increasing by 26 percent from December 2011 to December 2012. Despite this increase, however, Google's rate of compliance has stayed within a narrow range over the past few years, with the company releasing data in only 24 percent of cases.[36]

Although self-censorship was once largely limited to traditional journalists who faced threats of retribution for reporting on police activity and drug trafficking, the phenomenon has been increasing steadily among online journalists and bloggers. In 2011, as online sources of news about

[33] *Internet Para Todos*, [Internet for All], accessed September 7, 2013, http://internetparatodos.mx. The provision which guarantees internet access as a civic right is now included in Article 6 of the Constitution.
[34] Elsy Lopez, "Mexico, Principal Productor de Pornografía Infantil en el Mundo" [Mexico,Top Producer of Child Pornography in the World], *Milenio*, June 4 2013, http://www.milenio.com/cdb/doc/noticias2011/577409eff8ed0e4164086d202b95715e; Angel Aldaz, "Mexico, Gran Productor de Pornografia Infantil" [Mexico, a Major Producer of Child Pornography], *Periodistasenlinear*, April 2012, http://www.periodistasenlinea.org/modules.php?op=modload&name=News&file=article&sid=4011.
[35] Google, *Google Transparency Report*, *Mexico – Government Removal Requests*, http://www.google.com/transparencyreport/removals/government/MX/?p=2011-12.
[36] *Google Transparency Report, Mexico – User Data Requests,* http://www.google.com/transparencyreport/userdatarequests/MX/.

cartel-related violence drew increasingly larger audiences, several contributors to social networks were brutally murdered for acting as informants on cartel activity. Violence against online reporters has continued in recent years, and while some writers have been intimidated into silence, there is nonetheless a dynamic community of bloggers and online journalists attempting to spread information about cartel activity and citizen safety.[37]

Such courageous citizen journalism may be tempered by a recent agreement between the Federal Security Council and some state governments to refrain from reporting on violence unless absolutely necessary. The decision to suppress such news allegedly arose from a campaign to decrease fears of insecurity within the country, while also promoting an international image of Mexico as a country transitioning away from widespread violence.[38] Such policies emphasize the importance of online journalists' efforts to report on the full scope of events in their communities. In addition to the attempts of government agencies to downplay violence, online content is reportedly also subject to manipulation by politicians with close ties to media outlets.[39]

Economic constraints also influence the diversity of media in Mexico. Scarce funding and lack of interest in online advertising create challenges for individuals and nonprofits seeking to establish sustainable online outlets in Mexico. Reliance on public advertising renders independent media vulnerable to manipulation of content or closure due to lack of funding, although manipulation appears to be the more widespread of the two trends. Despite such impediments, however, efforts to develop politically oriented web portals that are financially independent have gained momentum in recent years. *El Respetable*, a political website run from Jalisco, has become very influential at the local level.[40] *Pijama Surf*, a website dedicated to presenting diverse types of social information, has grown drastically over the past three years, and now garners more than two million hits per month, drawing largely on an audience between 19 and 35 years of age.[41]

Among the most striking examples of successful independent digital media is *Animal Político*, a popular site which counts more followers on Facebook than any other news outlet in Mexico.[42] In order to raise revenue for the site without compromising content based on advertisers' political leanings, *Animal Político* is now practicing brand journalism, offering social media consulting and digital content to private companies. Additional financing is derived from syndicated content and

[37] "Acoso del Gobernador de Puebla Rafael Moreno Valle Contra E-Consulta" [Harassment by the Puebla Governor Rafael Moreno Valle Against E-Consulta)," YouTube, October 25, 2011, http://www.youtube.com/watch?v=tbqGB24McG8; Interview with Daniel Moreno, editor of Animal Político, February 2012 (www.animalpolitico.com).
[38] SDP Noticias.com, "Gobierno federal recomendó "dosificar" datos sobre violencia: Mario Anguiano, gobernador de Colima" [Federal Government Recommended Proportionate Violence Data: Mario Anguiano, Governor of Colima], *SDP Noticias*, Jan 29, 2013, http://www.sdpnoticias.com/nacional/2013/01/29/gobierno-federal-recomendo-dosificar-datos-sobre-violencia-mario-anguiano-gobernador-de-colima
[39] Reporters Without Borders, "Mexico," June 4, 2013, http://en.rsf.org/report-mexico,184.html.
[40] Interview with Ivabelle Arroyo, Director of El Respetable Mexico City, http://www.elrespetable.com/.
[41] Interview with Juan Manuel Ortega Riquelme, founding partner at Pijama Surf, March, 2013, www.pijamasurf.com.
[42] Tania Lara, "Populare Mexican News Site *Animal Politico* Seeks to Eliminate Dependence on Government Advertising," Knight Center for Journalism in the Americas, *Journalism in the Americas* (blog), April 30, 2013, https://knightcenter.utexas.edu/blog/00-13751-popular-mexican-news-site-animal-politico-seeks-eliminate-dependence-government-advert.

private sponsorships.[43] *Animal Político*'s approach, which appears to be unique among Mexican media, is clearly working. In July 2012 alone, visits to the site increased from 700,000 to 2 million.

Social media sites such as Facebook, Twitter, YouTube, and international blog-hosting services are widely used in Mexico by citizens, advocacy groups, and political parties. [44] As of September 2012, Mexico was home to the second largest community of Facebook users in Latin America after Brazil—and the fifth largest in the world—with an estimated 38,463,860 users.[45] The number of Mexicans with Twitter accounts (a group which includes President Enrique Peña Nieto[46]) has also ballooned, growing from 146,000 in February 2010 to more than 11 million in early 2013.[47]

Although netizens have been utilizing social media to provide critical warnings to local communities about dangerous cartel-related situations,[48] members of organized crime have also begun using such applications to exchange information on military checkpoints. Such subversive use of social networks has prompted calls by some Mexican politicians for increased government monitoring and regulation, though to date no such legislation has been passed.[49]

In addition to their aforementioned uses, Facebook and Twitter are also growing in popularity as forums for political commentary and mobilization, a trend which was witnessed in the lead-up to the July 2012 general elections.[50] In May 2012, students at Iberoamericana University used online tools to assist in mobilizing protests against the potential return of the Revolutionary Institutional Party (PRI) to the executive. Rallies were held against PRI candidate Enrique Peña Nieto (elected

---

[43] Tania Lara, "Populare Mexican News Site *Animal Politico* Seeks to Eliminate Dependence on Government Advertising," Knight Center for Journalism in the Americas, *Journalism in the Americas* (blog), April 30, 2013, https://knightcenter.utexas.edu/blog/00-13751-popular-mexican-news-site-animal-politico-seeks-eliminate-dependence-government-advert.

[44] Octavio Islas, Amaia Arribas, and Erika Minera, "El Empleo Propagandistico de Internet 2.0 en Campanas a Puestos de Eleccion Ciudadana, Estado de Mexico, Julio 2009" [The Use of Web 2.0 Propaganda in Campaigns for Elected Office, State of Mexico, July 2009], *Razon y Palabra* 14 no. 70, November 2009–January 2010, http://www.razonypalabra.org.mx/N/N70/Final_Argentina.pdf.

[45] Social Bakers, "Mexico Facebook Statistics," SocialBakers, accessed March 9, 2012, http://www.socialbakers.com/facebook-statistics/mexico.

[46] Deborah Esch, "Mexico: Felipe Calderón's Cabinet on Twitter," *Global Voices*, April 19, 2011, http://globalvoicesonline.org/2011/04/19/mexico-felipe-calderons-cabinet-on-twitter/; Felipe Coredero, "Mexico: President Felipe Calderón's Twitter Use," *Global Voices*, May 19, 2011, http://globalvoicesonline.org/2011/05/19/225272/; Claudia Benassini, "El Gabinete de Calderón en Twitter" [Calderón s cabinet on Twitter] *Razón y palabra*, April 2012, http://www.razonypalabra.org.mx/caja_pandora/gabinete.html.

[47] Daniel Medina, "Twitter en Mexico, Algunos Numeros" [Twitter in Mexico, Some Numbers], *Webadictos*, February 8, 2010, http://www.webadictos.com.mx/2010/02/08/twitter-en-mexico-algunos-numeros/; Damien Cave, "Mexico Turns to Twitter and Facebook for Information and Survival," *New York Times*, September 24, 2011, https://www.nytimes.com/2011/09/25/world/americas/mexico-turns-to-twitter-and-facebook-for-information-and-survival.html?_r=1; European Travel Commission, *New Media Trend Watch: Mexico*, last updated June 29, 2013, http://www.newmediatrendwatch.com/markets-by-country/11-long-haul/56-mexico.

[48] Damien Cave, "Mexico Turns to Twitter and Facebook for Information and Survival," New York Times, September 24, 2011, https://www.nytimes.com/2011/09/25/world/americas/mexico-turns-to-twitter-and-facebook-for-information-and-survival.html?_r=1; Miguel Castillo, "Mexico: Citizen Journalism in the Middle of Drug Trafficking Violence," *Global Voices* , May 5, 2010, http://globalvoicesonline.org/2010/05/05/mexico-citizen-journalism-in-the-middle-of-drug-trafficking-violence/.

[49] Alexis Okeowo, "To Battle Cartels, Mexico Weighs Twitter Crackdown," *Time*, April 14, 2010, http://www.time.com/time/world/article/0,8599,1981607,00.html/r:t#ixzz0laM8OTIa.

[50] Kaitlyn Wilkins, "Social Media in Mexico: 5 Things You Need to Know," Ogilvy Public Relations Worldwide (blog), September 24, 2009, http://blog.ogilvypr.com/2009/09/social-media-in-mexico-5-things-you-need-to-know/.

to the office of president in the July elections despite the protests) to discourage the return of what some protesters view as a monopolistic political party "in cahoots" with state media.[51]

After national news outlets downplayed the protest as merely a display by agitators sponsored by the opposition, 131 students from the university created a video to prove that they were indeed registered students acting independent of any political party. The non-partisan video, which advocated for free, fair, and transparent elections as well as greater freedom of speech, was uploaded to YouTube with the hash tag #YoSoy132 and quickly gained a large following on social networks. The so-called "Mexican Spring" grew to become a national movement with thousands of students, unionized workers, and farmers organizing peaceful regional marches. As the movement grew, it gained recognition from the government, which allowed protestors to demonstrate. National television channel Televisa even afforded airtime to YoSoy132.[52] While the protests may have had little impact on electoral results, many Mexicans concur that such mobilization marked an important shift in citizen activism.

VIOLATIONS OF USER RIGHTS

In 2012 and 2013, violations of user rights in Mexico were on the rise. As in previous years, threats and violence from drug cartels plagued online reporters, resulting in three murders during the coverage period. State-sponsored smear campaigns against crime reporters and unannounced surveillance of private citizens came to light, marring the landscape of digital freedom. Although positive legislation to safeguard journalists and NGOs was passed, weak rule of law protections at the state level have impeded implementation.

The Mexican Constitution guarantees freedom of speech, freedom of the press, and privacy of personal communications, however, recent reports concerning a ubiquitous state surveillance apparatus call such protections into question. While there are no legal ramifications for online activity other than defamation or libel, criminal defamation statutes still exist in 13 of Mexico's 32 states.[53] The upper echelons of the judiciary are viewed as independent; however, state level legal bodies have been accused of ineffectual conduct and biased behavior.

In June 2012, the Law for the Protection of Human Rights Defenders and Journalists was passed in Mexico, effectively establishing mechanisms for the protection of media workers and NGOs.[54] Among the law's provisions is a requirement that state governments work in conjunction with

[51] Allison Kilkenny, "Student Movement Dubbed the 'Mexican Spring,' *The Nation*, May 29, 2012, http://www.thenation.com/blog/168099/student-movement-dubbed-mexican-spring.

[52] Octavius Rod, "Students Start the So-Called 'Mexican Spring' through the Movement '#YoSoy132,'" Justice in Mexico Project, May 29, 2012, http://justiceinmexico.org/2012/05/29/students-start-the-so-called-mexican-spring-through-the-movement-yosoy132/.

[53] Commission on Human Rights, Congress General of the United States of Mexico, *Gaceta Parlamentaria, Número 3757-VIII*, [Parliamentary Gazette, No. 3757-VIII], April 25, 2013, http://gaceta.diputados.gob.mx/Black/Gaceta/Anteriores/62/2013/abr/20130425-VIII/DictamenaD-18.html

[54] Leah Danze, "Mexico's Law to Protect Journalists and Human Rights Activists Remains Ineffective," LAWG International, June 30, 2013, http://www.lawg.org/action-center/lawg-blog/69-general/1219-mexicos-law-to-protect-journalists-and-human-rights-activists-remains-ineffective.

federal authorities to ensure that protection is effectively extended to those under threat; as of April 2013, 27 of Mexico's 32 states had signed agreements to this effect.[55] While the legislation is promising in that it establishes a legal basis for protection and suggests an end to impunity for attackers, to date, capacity to actualize the law has been lacking. As of March 2013, PEN International noted that since 2006, Mexican authorities have "failed to successfully prosecute 90 percent of cases."[56] Media and human rights advocates are hopeful that the new legislation will shift this troubling dynamic. A separate amendment, predicated on protecting freedom of expression, was passed in the Senate in April 2013. If signed by the president, the amendment will grant authority for prosecution of crimes against journalists to the federal government, marking another positive step in the fight to protect reporters and bloggers.[57]

In January 2013, a coalition of seventeen civil society organizations began mobilizing online to gather the 125,000 signatures required to present new legislation to the government. Following the success of its online initiative, the coalition, know as *Internet para Todos* (internet for all) began lobbying for the inclusion of a universal digital policy guaranteeing access to internet for all Mexicans. The campaign, which was spearheaded by Senator Armando Rios Piter of the Party of the Democratic Revolution (PRD), was intended to extend opportunities for education, information, and work to all Mexicans, while also ensuring the integration of communities previously excluded from the digital sphere due to economic hardship. The government took notice of the coalition's efforts and in April 2013, Article 6 of the constitution was amended to include language that guarantees access to the internet as a civic right. While secondary legislation will be necessary to define precisely how the government will ensure this right, the constitutional amendment is a vital first step in Mexico's digital inclusion policy.[58]

Online tools have gained prominence as crucial sources of public information concerning drug-related violence, which has led local authorities to increase attempts to punish false reports that cause public alarm. In August 2011, amidst a surge of violence in Veracruz, a schoolteacher and a journalist tweeted about an attack on a school. In response to the resulting panic, local authorities arrested the pair on allegations of terrorism and sabotage, which can yield punishments of up to 30 years in prison.[59] A public outcry ensued over due process shortcomings and disproportionate charges for citizens who may have been negligent in publishing unconfirmed reports but

[55] Peace Brigades International, Proyecto Mexico, "The Implementation of the Law for the Protection of Human Rights Defenders and Journalists," June 26, 2013, http://www.pbi-mexico.org/fileadmin/user_files/projects/mexico/files/Mechanism/130625BriefingMechanismPBI_EN.pdf.
[56] PEN International, "A Year On, PEN International Renews its Call for an End to the War on Mexico's Journalists, Writers, and Bloggers," PEN International, March 11, 2013, http://www.pen-international.org/newsitems/a-year-on-pen-international-renews-its-call-for-an-end-to-the-war-on-mexico%E2%80%99s-journalists-writers-and-bloggers/.
[57] Mike O'Connor, "In Mexico, a Movement and a Bill against Impunity," *CPJ Blog*, April 26, 2013, http://cpj.org/blog/2013/04/in-mexico-a-movement-and-law-against-impunity.php; Committee to Protect Journalists, "CPJ Commends New Mexican Legislation," press release, April 25, 2013, http://cpj.org/2013/04/cpj-commends-new-mexican-legislation.php.
[58] Ruben Vasquez, "*La Propuesta Internet para Todos*" [Proposed Internet for All], *Forbes Mexico*, August 1, 2013, http://www.forbes.com.mx/sites/la-propuesta-internet-para-todos/.
[59] Daniel Hernandez, "Terrorism Charges for Two in Mexico who Spread Attack Rumor on Twitter, Facebook," *LA Times* (blog), September 1, 2011, http://latimesblogs.latimes.com/laplaza/2011/09/twitter-tweets-veracruz-mexico-terrorism-drug-war-censorship-rumors.html.

demonstrated no malicious intent.[60] In the midst of such controversy, the prosecutor's office subsequently dropped the charges and the two were released.

During the same month, several state congresses made changes to laws pertaining to "public order disturbances."[61] In Veracruz, the approval of Ley de Perturbación ("The Disturbance Act") has criminalized the spreading of false alarms via mobile phones or social media such that the offense may now carry criminal charges ranging from prison terms of six months to four years and fines equivalent to 1,000 days of wages.[62] Although local attorneys raised concerns that such provisions could be used to unnecessarily restrict freedom of expression, as of May 2013, there were no known instances of such an occurrence.

In late 2012 and early 2013, several state governments either planned or initiated legal proceedings against journalists and bloggers who had written critical statements about state officials. In one case, a list was leaked to the press of journalists that were likely to be sued by the governor of Puebla; in another instance, several online journalists were arrested for defamation. The first instance occurred in October 2012, when a document was publicized naming nineteen journalists and bloggers that Governor Moreno Valle's administration planned to sue. Of the nineteen named reporters allegedly guilty of "engaging in an excess of freedom of expression" which resulted in "moral damage" to government officials, seven were online writers.[63]

In April 2013, Martin Ruiz Rodriguez, editor of digital newspaper *e-consulta*, was arrested by police in Tlaxaca, Mexico's smallest state, and one of 13 that penalizes defamation.[64] The order for arrest came at the behest of Ubaldo Velasco, the chief clerk of Tlaxcala, who Ruiz had called mediocre in a handful of posts on his controversial political blog.[65] Ruiz is one of five contributors to *e-consulta* charged with defamation, a crime punishable in Tlaxcala with fines and up to two years in prison.

---

[60] Local media reported that the pair was subject to psychological pressure to plead guilty. According to Amnesty International, they were also denied access to a lawyer for 60 hours. See: Javier Duarte Ochoa, "*Personas en Riesgo de Prision en Mexico tras Publicaciones en Twitter y Facebook*" [People at Risk of Prison in Mexico after Publications on Twitter and Facebook], Amnesty International, August 31, 2011, http://amnistia.org.mx/nuevo/2011/09/01/personas-en-riesgo-de-prision-en-mexico-tras-publicaciones-en-twitter-y-facebook/.

[61] Reporters Without Borders, "After Wasted Month in Prison, Two Social Network Users Freed, Charges Dropped," September 22, 2011, http://en.rsf.org/mexico-two-social-network-users-held-on-02-09-2011,40907.html.

[62] H. Congreso del Estado de Tabasco, "Constitución de la Estado de Tobasco" [Constitution of the State of Tabasco], http://www.congresotabasco.gob.mx/60legislatura/trabajo_legislativo/pdfs/decretos/Decreto%20125.pdf; See also: Leobardo Perez Marin, "*Aprueban Ley Contra 'Rumor'; Coartara Libertades*" [Law Approved Against 'Rumor'; Freedoms Abridged], *Tabasco Hoy*, August 31, 2011, http://www.tabascohoy.com/noticia.php?id_nota=220149 (account suspended).

[63] Alvaro Delgado, "*Gobernador de Puebla Presenta Doe de 19 Demandas contra Periodistas*" [Governor of Puebla Presents Two of Nineteen Lawsuits against Journalists," *Proces*, October 23, 2013, http://www.proceso.com.mx/?p=323287.

[64] Sin Embargo, "*Atentados a la Libertad de Expresión Aumentaron 46% con EPN: Artículo 19; Registra 32 Agresiones a Periodistas*" [Attacks on Freedom of Expression Increased 46% with EPN: Article 19; Recorded 32 Attacks on Journalists], July 1, 2013, http://www.sinembargo.mx/01-07-2013/672263; Article 19, *"Segundo Informe Trimestral: Reprimir la Protesta* [Second Quarterly Report: Suppress the Protest], Article 19, May 2013, http://articulo19.org/segundo-informe-trimestral-reprimir-la-protesta/.

[65] Elvia Cruz, "*Un Periodista de Tlaxcala va a Juicio por Llamar a un Oficial 'Mediocre'*" [A Journalist from Tlaxcala goes on Trial for Calling an Officer 'Mediocre'], CNN Mexico, April 11, 2013, http://mexico.cnn.com/nacional/2013/04/11/un-periodista-de-tlaxcala-va-a-juicio-por-llamar-a-un-oficial-mediocre; SDP Noticias, "*Detienen a Martín Ruiz, Director de Portal e-consulta Tlaxcala por "Difamación contra Funcionarios" [Arrest of Martin Ruiq, Director of e-consulta Tlaxcala, for "Defamation against Officials"*], April 7, 2013, http://www.sdpnoticias.com/estados/2013/04/07/detienen-a-martin-ruiz-director-de-portal-e-consulta-tlaxcala-por-difamacion-contra-funcionarios.

Although he was released hours after being detained, Ruiz will stand trial for the charges leveled against him, which include emotional and psychological damage, at a future date.[66]

Four other journalists and managers of *e-consulta* have also been charged with defamation by state cabinet officials in Tlaxcala: Ruiz' brother, Rodolfo, Roberto Nava Briones, Gerardo Santillan, and Arturo Tecuatl. As of May 2013, it was unclear whether criminal proceedings would be upheld or whether the charges would be dropped.[67] A few days after Ruiz' arrest, Aurora Aguilar Rodriguez, deputy general of the National Action Party (PAN), publicly denounced the efforts of the Tlaxcala state government to censor criticism by filing criminal charges against journalists. It remains to be seen whether Aguilar's comments will influence the state government.[68]

This is not the first time that contributors to *e-consulta* have been harassed. In October 2012, Gerardo Rojas and Jesse Brena, journalists with the digital newspaper were kidnapped by state police in Puebla and held captive in the trunk of a police car for three hours. After taking all of their personal belongings, including the cash they carried, they were abandoned in an empty lot in Ciudad Judicial.[69] Although such intimidation was presumably meant to inspire fear in *e-consulta* reporters, the digital news outlet continued operations unabated.

Apart from a 2008 requirement that cell phone users register with the government (revoked in 2012) there are no official provisions regarding anonymity. The only regulation currently in practice is unofficial and pertains to the safety of informants writing online about drug cartel activity. Moderators of forums disseminating user-generated safety updates on local websites urge writers to publish their comments anonymously in order to ensure their safety.

Despite a constitutional requirement that any interception of personal communications be accompanied by a judicial warrant—a well as the 2010 passage of a law expanding the oversight powers of the data protection authority[70]—reports published in 2012 allege that secret surveillance of private citizens is widespread in Mexico.[71] In July 2012, evidence was leaked (and later

---

[66] "*Pidió Oficial Mayor de Tlaxcala detención de Director de e-Consulta*" [Mayor of Tlaxcala Called for Detention of Director of e-Consulta], *e-consulta*, April 7, 2013, http://archivo.e-consulta.com/2013/index.php/2012-06-13-18-40-00/politica/item/pidio-oficial-mayor-de-tlaxcala-detencion-de-director-de-e-consulta; Juana Osorno Xochipa, "*Liberan a Periodista Detenido por PGJE de Tlaxcala*" [Free Journalist Arrested for PGJE in Tlaxcala], April 7, 2013, http://www.eluniversal.com.mx/notas/915260.html; "Daily Digest: Mexican State Blocks Access to Police, Court Information," Knight Center for Journalism in the Americas, April 12, 2013, https://knightcenter.utexas.edu/en/blog/00-13521-daily-digest-mexican-state-blocks-access-police-court-information.

[67] Article 19, "*Alerta: Oficial Mayor Intenta Meter a la Carcel a Periodista por Difamacion*" [Alert: Mayor Tries to Send Journalist to Jail for Defamation], April 8, 2013, http://articulo19.org/mexico-criminalizacion-al-director-de-periodico-digital-e-consulta-en-tlaxcala-es-una-agresion-a-la-libertad-de-expresion/.

[68] Gerardo Santillan, "Pide PAN en San Lazaro Cesse Persecucion a la Prense en Tlaxcala" [In San Lazaro, PAN Asks for Persecution of the Press to Cease in Tlaxcala] *e-consulta*, April 11, 2013, http://archivo.e-consulta.com/2013/index.php/2012-06-13-18-40-00/nacion/item/pide-pan-en-san-lazaro-cese-persecucion-a-la-prensa-en-tlaxcala.

[69] Víctor Gutiérrez, "*Dos Reporteros, Víctimas de Policías Delincuentes*" [Two Reporters, Victims of Police Offense], *El Sol de Puebla*, October 22, 2012, http://www.oem.com.mx/elsoldepuebla/notas/n2742106.htm.

[70] Jeremy Mittman, "Mexico Passes Sweeping New Law on Data Protection," Proskauer Rose LLP, May 11, 2010, http://privacylaw.proskauer.com/2010/05/articles/international/mexico-passes-sweeping-new-law-on-data-protection/.

[71] Bob Brewin, "State Department to Provide Mexican Security Agency with Surveillance Apparatus," *NextGov*, April 30, 2012, http://www.nextgov.com/technology-news/2012/04/state-department-provide-mexican-security-agency-surveillance-apparatus/55490/.

confirmed by the Mexican army[72]) pertaining to the secret purchase of approximately $4.6 billion pesos ($355 million) of "spyware" engineered to intercept online and mobile phone communications. Such technology, which has been funded in large part by the U.S. State Department's Bureau of International Narcotics and Law Enforcement Affairs, facilitates the real-time geolocation of callers, the storage of up to 25,000 hours of conversation, and the real-time monitoring of packet data.[73] In addition to recording conversations and gathering text messages, email, internet navigation history, contact lists, and background sound, the surveillance software is also capable of activating the microphone on a user's cell phone in order to eavesdrop on the surrounding environment.[74]

The website of the Mexican Access to Information agency (IFAI) makes no mention of this expenditure — or of the U.S. State Department's alleged assistance in the tripling of Mexico's surveillance capacity.[75] In March 2012, the Geolocalization Law, which allows the government "warrantless access to real time user location data," was passed nearly unanimously with 315 votes in favor, 6 opposed, and 7 abstentions.[76] Such opacity, which renders Mexicans unaware of the extent to which they are being surveilled and unable to contribute to discussions concerning the legality of using such technology on private citizens, is deeply concerning. Critics of the law warn that it is unconstitutional and sets a worrisome precedent of warrantless surveillance.[77] Corruption and weak rule of law among state governments—including the infiltration of law enforcement agencies by organized crime—also leave room for abuse should private communications fall into the wrong hands.

Mexico continues to be one of the most dangerous countries in the world for journalists, who are subject to violence (often from drug cartels) for investigating a range of issues, notably those involving the drug trade, from trafficking to corruption. This phenomenon has been exacerbated by widespread impunity for those carrying out such attacks.[78] While such violence has historically been targeted at traditional, rather than online media, in 2011, bloggers and journalists posting information about sensitive topics online became victims of cartel-related violence for the first time, a worrisome trend that has continued to plague online writers.

Although online writers have attempted to protect themselves, they continued to be the target of intimidation and violence in 2012 and 2013. In September 2012, Ruy Salgado aka "El 5anto"

[72]Ryan Gallagher, "Mexico Turns to Surveillance Technology to Fight Drug War," *Slate*, August 3, 2012, http://www.slate.com/blogs/future_tense/2012/08/03/surveillance_technology_in_mexico_s_drug_war_.html.
[73] Robert Beckhusen, "U.S. Looks to Re-Up its Mexican Surveillance System," *Wired*, May 1, 2013, http://www.wired.com/dangerroom/2013/05/mexico-surveillance-system/.
[74] Katitza Rodriguez, "Mexicans Need Transparency on Secret Surveillance," Electronic Frontier Foundation, July 24, 2012, https://www.eff.org/deeplinks/2012/07/mexicans-need-transparency-secret-surveillance-contracts; Cryptome, *U.S. Department of State Contract 58, Communications Intercept System Mexico*, http://cryptome.org/2012/06/us-mx-spy.pdf.
[75]Robert Beckhusen, "U.S. Looks to Re-Up its Mexican Surveillance System," *Wired*, May 1, 2013, http;Katitza Rodriguez, "Mexicans Need Transparency on Secret Surveillance," Electronic Frontier Foundation, July 24, 2012.
[76] Katitza Rodriguez, "Mexico Adopts Alarming Surveillance Legislation," Electronic Frontier Foundation, March 2, 2012, https://www.eff.org/deeplinks/2012/03/mexico-adopts-surveillance-legislation.
[77] Cyrus Farivar, "Mexican 'Geolocalization Law' Draws Ire of Privacy Activists," *ArsTechnica*, April 24, 2012, http://arstechnica.com/tech-policy/2012/04/mexican-geolocalization-law-draws-ire-of-privacy-activists/.
[78] Committee to Protect Journalists, "28 Journalists Killed in Mexico since 1992/Motive Confirmed," accessed January 12, 2013, https://www.cpj.org/killed/americas/mexico/.

(@5anto), a prominent blogger reporting on corruption and electoral fraud, went missing.[79] Forty-two days later, Salgado resurfaced to announce that despite multiple death threats, he was alive. In a video post, Salgado explained that he had been subject to a forced disappearance, the details of which he was afraid to reveal. Citing fear for the safety of his family, Salgado announced that he would no longer be writing, but urged others to be brave—and careful—in their reporting.[80]

Although widely reported in international media, conflicting reports have emerged about a February 2013 campaign by an organized crime group to identify the administrator of *Valor por Tamaulipas*, a site issuing reports on security risks in the cartel-dominated state. Although the crime group allegedly offered a reward of 600,000 pesos ($47,000) for information leading to the identification of the site's owner or his family,[81] residents of the area say they never saw flyers with such an offer.[82] Following reports of additional threats in April 2013, the site announced the shutdown of both its Twitter and Facebook accounts.[83] As of May, 2013, however, the Facebook and Twitter pages associated with *Valor por Tamaulipas* —which have nearly 215,0000 likes and 33,800 followers, respectively—were back up and running. Conflicting reports alternately claim that the sites are clones or that the administrator changed his mind about closing the sites.[84]

In February 2013, death threats were issued against members of an informal network of Twitter users sharing information about drug violence in Mante, Tamaulipas under the hashtag #vigilantesmante. The threats, which were transmitted from accounts using the name #ManteZeta (the Zeta cartel is active in the area) via YouTube and Twitter, linked to a video depicting the murder of three people. Accompanying the link to the video, which was originally published by *Blog del Narco*, a site reporting on cartel-related violence, were threats stating that the same fate would befall those tweeting about security risks in Tamaulipas.[85]

Murders of online journalists are no longer rare in Mexico. Between September and November 2011, four people were brutally murdered in connection with their online writings. In each case, the bodies, often bearing signs of torture, were displayed publicly and accompanied by notes

[79] Lisa Goldman, "A Prominent Mexican Anti-Corruption Blogger Has Gone Missing, *TechPresident*, Spetmeber 17, 2012, http://techpresident.com/news/wegov/22862/prominent-mexican-anti-corruption-blogger-has-gone-missing.
[80] Arjan Shahani, "Censorship in Mexico: The Case of Ruy Salgado, *Americas Quarterly* (blog), October 29, 2012, http://www.americasquarterly.org/node/4077.
[81] Daniel Hernandez, "Facebook Page in Mexico Draws Attention for Posts on Security Risks, *Los Angeles Times*, February 9, 2013, http://articles.latimes.com/2013/feb/19/world/la-fg-wn-mexico-facebook-page-security-20130218.
[82] #Reynosafollow, "Observaciones en el Caso Valor por Tamaulipas" [Observations in the Case of Valor por Tamaulipas], *Del Twitter al Blog*, April 12, 2013, http://chuynews.blogspot.com/2013/04/observaciones-en-el-caso-valor-por_12.html.
[83] Sin Embargo, "'*Valor por Tamaulipas,' Que Operaba Bajo Amenaza del Narco, Cierra sus Cuentas de Twitter y Facebook*," ['Valor por Tamaulipas,' Which Operated Under Threats from Drug Cartels, Closes its Twitter and Facebook Accounts] SinEmbargo.mx, April 1, 2013, http://www.sinembargo.mx/01-04-2013/576396.
[84] "Valor por Tamaulipas Official Facebook Back Online but Will Cease Operations in Eight Days," *Hispanic News Network USA* (blog), April 7, 2013, http://hispanicnewsnetwork.blogspot.com/2013/04/valor-por-tamaulipas-official-facebook.html; "Valor por Tamaulipas Facebook Page to Remain, but Less Active," *Hispanic News Network USA* (blog), April 14, 2013, http://hispanicnewsnetwork.blogspot.com/2013/04/valor-por-tamaulipas-facebook-page-to.html.
[85] Periodistas en Riesgo, Crowdmap, "*Amenaza de Muerte contra Tuitero de Tamaulipas*" [Death Threat against Twitterers in Tamaulipas], ICFJ and Freedom House, February 21, 2013, https://periodistasenriesgo.crowdmap.com/reports/view/45.

explicitly stating that the murders were retribution for the victims' posts on popular websites and narcoblogs. At least one of the messages was signed "Z" for Zeta.[86]

Echoing the fears of website moderators, who have implored contributors to continue reporting but to do so anonymously, such targeted killings of website contributors were also carried out in 2012 and 2013.[87] In June 2012, Victor Manuel Baez Chino, a journalist who reported on crime for the digital edition of weekly newspaper *Mileno* and also edited the crime reporters' website *Reporteros Policiaos*, was kidnapped and murdered. In a note accompanying his body, the Zeta drug cartel claimed responsibility for Chino's killing.[88] In November 2012, Adrián Silva Moreno**,** a journalist in Tehuacán Puebla working for the online newspaper *Glob@l México,* was shot to death while covering an army raid on a warehouse filled with stolen fuel.[89] Having been warned to leave by a soldier, Silva was in the process of driving away when trucks arrived and began firing on his car, killing him and his companion, Misray López González, a former policeman.

In March 2013, journalist Jaime Guadalupe González Domínguez, editor of the online news portal *Ojinaga Noticias*, was murdered in broad daylight in Chihuahua, a state reportedly run by organized crime. A group of men shot González 18 times before absconding with his camera. González's murder, which was foreshadowed by written threats warning him to avoid covering certain topics, led to the closure of his online news portal, *Ojinaga Noticias,* which reported on local news, crime, sports, and politics.[90]

Hate campaigns against journalists also marred Mexican reporting in 2012 and 2013, bringing attacks against traditional journalists into the domain of the internet. The state Social Communication General Coordination Office in San Luis Potosi made use of both Twitter and Wordpress blogs in December 2012 and February 2013 to denigrate several journalists writing for daily newspaper *Pulso*. After a video was leaked of the Office's director, Juan Antonio Hernandez Varela, ordering subordinates to create fake social networking accounts for the sole purpose of discrediting government critics, Hernandez Varela resigned without explanation. It remains to be seen whether such attacks will continue under the new director.[91]

---

[86] Robert Beckhusen, "Mexican Man Decapitated in Cartel Warning to Social Media," *Wired*, November 9, 2011, http://www.wired.com/dangerroom/2011/11/mexican-blogger-decapitated/.

[87] Sarah Kessler, "Mexican Blog Wars: Fourth Blogger Murdered for Reporting on Cartel," *Mashable*, November 10, 2011, http://mashable.com/2011/11/10/mexico-blogger/.

[88] UNESCO Press, "Director-General Condemns Murder of Mexican Journalist Victor Manuel Baez Chino," July 11, 2012, http://bit.ly/18eVyRR.

[89] Reporters Without Borders, "*Un Periodista Asesinado a Balas en Tehuacán: "'Cuándo se Acabará la Violencia y la Impunidad?'*[Journalist Murdered in Tehuacan Bales: 'When Will the Violence and Impunity End?], November 19, 2012, http://es.rsf.org/mexico-un-periodista-asesinado-a-balas-en-19-11-2012,43695.html.

[90] Committee to Protect Journalists, "*Editor de Sitio Web de Noticias Asesinado a Balazos en México*" [Editor of News Site Murdered by Gunshot in Mexico], March 5, 2013, http://cpj.org/es/2013/03/editor-de-sitio-web-de-noticias-asesinado-a-balazo.php; UNESCO Press, "Director-General Voices Deep Concern over the Killing of Mexican Journalist Jaime Gonzalez Dominguez," March 11, 2013, http://bit.ly/14Twxex; Reporters Without Borders, "Self-Censorship: Newspapers in Northern Border States Forced to Censor Themselves?," March 12, 2013, http://bit.ly/ZlfI6x.

[91] Reporters Without Borders, "The Dangers of Reporting: Organized Crime, Local Authorities Threaten Reporters and Netizens," March 4, 2013, http://en.rsf.org/mexico-organized-crime-local-authorities-04-03-2013,44161.html; Eduardo Delgado, "*Gobierno Estatal Cambia de Vocero*" [State Government Spokesman Changes], *Pulso*, March 5, 2013, http://pulsoslp.com.mx/2013/03/05/gobierno-estatal-cambia-de-vocero/.

Cyberattacks have become an issue in Mexico in recent years, and pose a growing threat to critical news sites. In September 2011, three online outlets known for critical coverage of state government—Expediente Quintana Roo, Noticaribe, and Cuarto Poder—were temporarily disabled by cyberattacks. Personal information and reporters' notes were also stolen from their servers.[92] In November 2011, weekly newspaper *Riodoce* was informed by its host provider that the website had been the target of a large distributed denial of service (DDoS) attack. Widely suspected to be a reprisal for the publication's aggressive reporting on crime and drug trafficking, the cyberattack resulted in the website being inaccessible for several days.[93] Sporadic cyberattacks continued to be reported in 2012 and early 2013. Vincente Carrera, director of online newspaper Noticaribe, which was temporarily paralyzed by DDoS attacks in late 2011 and early 2013, stated that recent attacks, which disabled the site for weeks, were likely government retaliation for the outlet's coverage of electoral violations and state debt.[94]

One notable case of repeated DDoS attacks targeted rompeviento.tv, an independent, left-leaning internet television site intended to present the public with an alternate perspective on news. Rompviento, which counts an audience of 600,000 visitors per month, was disabled by continuous cyberattacks after it aired contentious political content.[95] During the broadcast of a debate organized by YoSoy132, Rompviento lost broadband access and its webpage subsequently vanished. Despite multiple attempts to recover content, the original website appears to have been deleted permanently. Administrators of the host platform, mydomain, were unable to provide explanation or assistance with the issue. As of May 2013, however, the new rompeviento.tv website was accessible both from within Mexico and from outside the country.

[92] Monica Medel, "Three News Websites Hacked in Mexico," Knight Center for Journalism in the Americas (blog), July 15, 2011, https://knightcenter.utexas.edu/blog/three-news-websites-hacked-mexico.

[93] International Freedom of Expression eXchange, "Weekly Goes Offline after Cyber Attack," news release, November 28, 2011, http://ifex.org/mexico/2011/11/30/riodoce_cyberattack/.

[94] Tania Lara, "Mexican Digital Newspaper Disabled by Frequent Cyberattacks," Knight Center for Journalism in the Americas (blog), April 20, 2012, http://knightcenter.utexas.edu/blog/00-9806-mexican-digital-newspaper-disabled-frequent-cyberattacks.

[95] In a recent interview, Ernesto Ledesma, Director General of Rompeviento (www.rompeviento.tv) stated that the company has identified a pattern of disruptions. Although the signal is steady for cultural programs, when the company attempts to broadcast critical political programs, the signal is lost. While Rompviento cannot prove government interference, a pattern has emerged in which disruptions seem to be tied to the airing of political content.

MOROCCO

	2012	2013
INTERNET FREEDOM STATUS	N/A	PARTLY FREE
Obstacles to Access (0-25)	n/a	11
Limits on Content (0-35)	n/a	7
Violations of User Rights (0-40)	n/a	24
Total (0-100)	**n/a**	**42**

* 0=most free, 100=least free

POPULATION: 32.6 million
INTERNET PENETRATION 2012: 55 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Blocking orders on numerous websites and online tools were lifted as the government introduced a series of liberalizing measures to counter rising discontent heightened by the events of the Arab Spring (see **LIMITS ON CONTENT**).
- Despite constitutional reforms introduced in 2011, restrictive press and national security laws continued to plague the online media landscape and induce a spirit of self-censorship (see **VIOLATIONS OF USER RIGHTS**).
- Several online users were arrested under these laws for comments and videos they posted to Facebook, YouTube, and blogs (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Research universities led the development of the internet in Morocco from the early 1990s, with internet access extended to the general public in 1996. Initially, the internet's diffusion was slow in Morocco due primarily to the high cost of computers and poor infrastructure.[1] Under the combined impact of the liberalization, deregulation, and privatization of the telecommunications sector, as well as the legal and technological modernization of Moroccan broadcasting media, a growing and dynamic digital media market has emerged. This phenomenon has been furthered by the recent opening of the political system.

Social media has triggered a revival of the media's traditional function as a watchdog, acting as a check on the misconduct of the political regime. It has also been used as a tool for nascent political movements to organize and mobilize supporters across the country, particularly in the context of the Arab Spring. The February 20th Movement, which started on Facebook and relies heavily on digital media for communication, has held rallies throughout the country demanding democratic reforms, a parliamentary monarchy, social justice, greater economic opportunities, and more effective anticorruption measures. Two weeks after the first demonstrations, King Mohamed VI responded by announcing new constitutional reforms in which he promised to devolve limited aspects of his wide-ranging powers to the elected head of government and the parliament. Included in this reform package were provisions to grant greater independence to the judiciary and an expansion of civil liberties. The king's proposals were approved by 98.5 percent of Moroccan voters in a popular referendum held on July 1, 2011, for which voter turnout was 84 percent. The measures resulted in a lifting of all politically-motivated filtering.

The most remarkable change in internet use among Moroccans is the growing interest in social media and user-generated content, as well as domestic news portals. In 2010, the top ten most visited websites did not include any Moroccan news website.[2] By 2012, the sixth most visited site was Hespress.com, the most popular online news and information website in Morocco with estimated 400,000 unique visitors per day. Besides Hespress, the sports website Koora.com is the only other Arabic-language site in the Top 10.[3] Before the Arab Spring, government intervention to block and delete online content was relatively common. Today, the state no longer engages in technical filtering; it uses the existing laws to limit freedom of speech for online users. As a result, several online users were arrested over the past year.

[1] Ibahrine, M. (2007). The Internet and Politics in Morocco: The Political Use of the Internet by Islam Oriented Political Movements. Berlin: VDM Verlag.
[2] Bouziane Zaid and Mohamed Ibahrine, Mapping Digital Media: Morocco, available at, http://www.opensocietyfoundations.org/reports/mapping-digital-media-morocco, (accessed February 24 2013).
[3] Facebook, Google, YouTube, Google Morocco, and Blogspot were the five most visited sites in 2012. See "Top Sites in Morocco," Alexa, http://www.alexa.com/topsites/countries/MA (accessed January 14 2013).

OBSTACLES TO ACCESS

Internet access in Morocco has increased steadily in recent years, although obstacles remain in place in certain areas of the country. The internet penetration rate grew from just over 21 percent of the population in 2007 to 55 percent in 2012, according to the International Telecommunication Union (ITU).[4] By end of 2012, roughly 2 in 100 inhabitants possessed a fixed-broad subscription, or around 17.8 percent of all subscribers.[5] The remaining 82.2 percent of all subscriptions are through 3G devices, including both data-only and voice-and-data connections.[6] By December 2012, mobile phone penetration reached a rate of 119.7 percent, a rise of almost 20 percentage points compared to 2010.[7]

Internet access is currently limited to educated and urban segments of Morocco's population. There is a major discrepancy in terms of network coverage between urban and rural areas. Telecommunications companies do not abide by the ITU principle of telecommunications as a public service, instead preferring to invest in more lucrative urban areas. Rural inhabitants constitute 37.1 percent of the overall population and while many have access to electricity, television, and radio, most do not have access to phone lines and high speed internet. The high rate of illiteracy is another obstacle (43 percent of Moroccans aged 10 and above are illiterate). Most Moroccan households are not prepared to access content provided by digital media, but recent developments in the telecoms sector show that this situation is likely to change in the near future.

The Moroccan government has undertaken several programs aimed at improving the country's ICT sector. Launched in March 2005, the GENIE project (the French acronym for "Generalization of ICTs in Education") aims to extend the use of ICTs throughout the public education system.[8] Owing to positive results, another round of implementation was launched for the period of 2009-2013 to improve the training and professional development of teachers and encourage the adoption of ICTs by public school students. PACTE (French for "Program of Generalized Access to Telecommunications") was launched in 2008 to provide 9,263 communities, or 2 million Moroccans, with telecoms services by 2010.[9] Financing for the project came from Morocco's Universal Service Fund for Telecommunications. The fund was created in 2005 using contributions from the three major telecoms operators: Maroc Telecom, Medi Telecom, and INWI. More recently, in 2009, authorities established the national strategy "*Maroc Numérique 2013*" (Digital Morocco 2013).[10] The strategy aims to achieve nationwide access to high-speed internet by 2013

[4] "Percentage of individuals using the internet," ITU, 2000-2012, available at http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[5] "Fixed (wired-)broadband subscriptions," ITU, 2000-2012, available at http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[6] "Internet Market in Morocco: Quarterly Observatory" Agence Nationale de Réglementation des Télécommunications, March 2013, http://www.anrt.ma/sites/default/files/2013_T1_TB_Internet_en.pdf.
[7] "Mobile-cellular subscriptions," ITU, 2012, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[8] ANRT, *Rapport Annuel* (Annual Report), 2008, available at http://www.anrt.net.ma/fr/admin/download/upload/file_fr1702.pdf, (accessed 5 January 2013) (hereafter ANRT, Rapport Annuel, 2008).
[9] ANRT, Rapport Annuel, 2008.
[10] "HM the King chairs presentation ceremony of national strategy 'Maroc Numeric 2013'," available at

and to develop e-government programs to bring the administration closer to its citizens, while encouraging small and medium-sized enterprises to adopt ICTs into their business practices. It has a budget of MAD 5.2 billion (around $520 million).

Perhaps as a result of these efforts, internet use remains relatively affordable. For a 3G prepaid connection of up to 7.2 Mbps, customers pay MAD 223 ($26) for initial connectivity fees and then MAD 10 per day ($0.82) or MAD 200 per month ($23.6). Internet users pay on average MAD 3 ($0.35) for one hour of connection in cybercafés.

In the post-Arab Spring era, the government no longer blocks Web 2.0 applications, anonymous proxy tools, and Voice over Internet Protocol (VoIP) services. However, in February 2012 there was a report that Maroc Telecom briefly disrupted VoIP services such as Skype, TeamSpeak, and Viber in order to tamper with the quality of the calls. Some speculated that the actions were motivated by financial concerns over competition to traditional fixed-line services provided by the telecommunications company.[11]

Service providers such as ISPs, cybercafes, and mobile phone companies do not face any major legal, regulatory, or economic obstacles.[12] The allocation of digital resources, such as domain names or IP addresses, is carried out by organizations in a non-discriminatory manner.[13] According to the Network Information Centre, which manages the ".ma" domain, there were 43,354 registered Moroccan domain names in 2012.[14]

The National Agency for the Regulation of Telecommunications (ANRT) is an independent government body created in 1998 to regulate and liberalize the telecommunications sector. The founding law of the ANRT considers the telecommunications sector as a driving force for Morocco's social and economic development and the agency is meant to create an efficient and transparent regulatory framework that favors competition among operators.[15] A liberalization of the telecoms sector aims to achieve the long-term goals of increasing GDP, creating jobs, supporting the private sector, and encouraging internet-based businesses, among others. While Maroc Telecom, the oldest telecoms provider, effectively controls the telephone cable infrastructure, the ANRT is tasked to settle the prices at which the company's rivals (such as Medi-

---

http://www.maroc.ma/PortailInst/An/Actualites/HM+the+King+chairs+presentation+ceremony+of+national+strategy+Maroc+Numeric+2013.htm (accessed 24 February 2013).

[11] Hisham Almiraat, "Morocco: Historic Telecom Operator Blocks Skype," available at, http://globalvoicesonline.org/2012/02/19/morocco-historic-telecom-operator-blocks-skype/ (accessed 24 February 2013). See also, Brahim Oubahouman, "Maroc Télécom interdit Skype et d'autres services VoIP", available at, http://www.moroccangeeks.com/maroc-telecom-interdit-skype-et-autres-services-voip/ (accessed 24 February 2013).

[12] Interviews conducted on 20 February 2013, with Dr. Hamid Harroud and Dr. Tajjedine Rachdi, respectively director and former director of Information Technologies services of Al Akhawayn University in Ifrane.

[13] Network Information Centre, the service that manages the domain .ma, is owned by Maroc Telecom. There are calls for domain.ma to be managed by an independent entity, not a commercial telecoms company.

[14] Network Information Centre, available at http://www.nic.ma/statistiques.asp (accessed 18 February 2013). This service is owned by Maroc Telecom.

[15] Lois régissant la poste et les télécommunications (Laws governing the post and telecommunications), available online at http://www.anrt.ma/fr/admin/download/upload/file_fr1825.pdf (accessed 11 February 2013).

Telecom and INWI) can access those cables. Thus the ANRT makes sure competition in the telecoms market is fair and leads to affordable services for Moroccan consumers.[16]

Some journalists argue that the ANRT is a politicized body lacking independence, citing the fact that its director and administrative board are appointed by a *Dahir* (Royal Decree). However, international organizations such as the World Bank and the ITU have not expressed any major criticism about the ANRT's neutrality.[17]

As mentioned, Maroc Telecom, Medi Telecom, and INWI are the three ISPs and mobile phone companies in Morocco. Maroc Telecom (*Ittissalat Al Maghrib*, IAM) is a former state company that held a monopoly over the telecoms sector until 1999.[18] That year, the ANRT granted licenses for Medi Telecom and INWI. Medi Telecom is a private consortium led by Spain's Telefonica, while INWI (formerly WANA, Maroc Connect) is a subsidiary of Ominum North Africa (ONA), the leading Moroccan industrial conglomerate also owned by the royal family.

LIMITS ON CONTENT

Given the high rate of illiteracy and the many obstacles to access in parts of the country, online media do not enjoy the same popularity and influence as television and radio. For this reason, there are fewer instances of government intervention in the online sphere, even if much more controversial statements are made on the web. The state does not appear to currently block or filter internet sites.[19] Nonetheless, fears over intermediary liability and the prosecution of users have underscored an environment of continued self-censorship, particularly regarding so-called "sacred" issues such as the monarchy and Islam.

Before the Arab Spring, government intervention to block or delete online content was relatively common. While ISPs rarely, if ever, blocked Web 2.0 applications such as YouTube, Facebook, or Twitter,[20] websites advocating controversial views or minority causes were systematically blocked.[21] However, owing to the post-Arab Spring environment, the government has made a concerted effort to show that it is implementing democratic reforms, rather than restricting access

[16] ANRT, Lois régissant la poste et les télécommunications.
[17] Caroline Simard, "Morocco's ANRT Guidelines Project Related to Fundamental Regulatory Aspects," available at http://www.itu.int/ITU-D/treg/Newsletters/Research%20Material/MAR_Projetlignesdirectrices.pdf (accessed 31 January 2013); BjörnWellenius and Carlo Maria Rossotto, "Introducing Telecommunications Competition through a Wireless License: Lessons from Morocco," 1999, available at http://rru.worldbank.org/documents/publicpolicyjournal/199welle.pdf
[18] The State owns 30% of Maroc Telecom shares, 53% owned by the French telecoms company Vivendi, and 17% is public, available online at http://www.iam.ma/Groupe/Institutionnel/Qui-Sommes-nous/Pages/StructureDu Capital.aspx.
[19] Interviews with Hisham Almiraat on February 13, 2013, with Aboubakr Jamai on February 11, 2013, and two other interviews conducted during February 2013 with online activists who want to remain anonymous. Hereafter, Interviews with digital activists and online journalists.
[20] RSF reported one incident where Maroc Telecom blocked YouTube on 25 May 2007 for a few hours. Maroc Telecom reportedly said that it was a "technical problem." RSF speculated that Maroc Telecom may have blocked access to YouTube after videos "were posted on it of pro-independence Saharan demonstrations."Other Moroccan users of the other two ISPs, Medi Telecom and Wana, continued having access to YouTube during that day.
[21] Reporters Without Borders Annual Report 2007 – Morocco, available at, http://www.unhcr.org/refworld/type,ANNUALREPORT,RSF,MAR,46e692cbc,0.html, (accessed 29 March 2013).

to information. As such, sites related to the disputed territory of Western Sahara, the Amazigh minority, or Islamist groups are no longer blocked.[22] In addition, YouTube, Facebook, Twitter, and international blog-hosting services are freely available. Despite numerous reports to the contrary, Google Earth was found to be accessible in tests conducted by Freedom House in several cities and on a range of different devices by mid-2013. The service had been reportedly blocked in August 2009.[23]

Although technical methods to filter websites are no longer utilized, the government still controls the online information landscape through a series of restrictive laws that can be manipulated to serve political purposes. Under the 2002 Press Law, the government has the right to shut down any publication "prejudicial to Islam, the monarchy, territorial integrity, or public order," and it maintains prison sentences and heavy fines for the publication of offensive content (see "Violations of User Rights").

The Anti-Terrorism Bill, passed in 2003 after the May 16, 2003 terrorist attacks in Casablanca,[24] gives the government sweeping legal powers to filter and delete content that is deemed to "disrupt public order by intimidation, force, violence, fear or terror."[25] According to this law, legal liability rests jointly with the author, the site owner, and ISPs. Intermediaries must block or delete infringing content when made aware of it or upon receipt of a court order. While the law was ostensibly designed to combat terrorism, the authorities retain the right to define vague terms such as "national security" and "public order" as they please, thus opening the door for abuse. Although ISPs have not conducted any significant blocking since 2011, many opposition news websites are hosted on servers outside of the country for security reasons, such as Lakome.com, Mamfakinsh.com, and Febrayer.com.

Given the history of media repression in Morocco, many internet users and cyber activists engage in self-censorship. Although activists and journalists face little constraints in voicing their opinions, harsh legal consequences for online speech ultimately deter freedom of expression.[26] According to Aboubakr Jamai, a prominent Moroccan journalist, many website owners continue to censor comments related to the royal family in order to avoid legal problems.[27] In a state that punishes investigative reporting and whistleblowing, people with sensitive information tend to stay quiet to avoid possible retribution.

---

[22] For example, sites such as arso.org, spsrasd.info, cahiersdusahara.com, wsahara.net, and even LiveJournal were blocked for promoting the independence of Western Sahara.

[23] For more, see "Current disruptions of traffic to Google products and services," Google Transparency Report, accessed August 9, 2013, http://www.google.com/transparencyreport/traffic/#expand=TJ,MA.

[24] On 16 May 2003, Morocco was subject to the deadliest terrorist attacks in the country's history. Five explosions occurred within thirty minutes of each other, killing 43 people and injuring more than 100 in suicide bomb attacks in Morocco's largest city, Casablanca. Morocco has been a staunch ally of the U.S. The 14 suicide bombers all originated from a poor suburban neighborhood in the outskirts of Casablanca.

[25] Open Net Initiative, "Internet Filtering in Morocco. 2009," available online at, http://bit.ly/18GiHgW

[26] Interviews with digital activists and online journalists.

[27] Interview with Aboubakr Jamai conducted on 11 February 2013. Jamai is a Moroccan journalist who founded some of the most progressive magazines such as *Le Journal Hebdomadaire* and *Assahifa al-Ousbouiya*. In 2003, he was awarded the International Press Freedom Award of the Committee to Protect Journalists.

In addition to state-run and opposition news outlets, the Moroccan media contains a variety of "shadow publications," nominally-independent but editorially-supportive of the state.[28] The news outlets exist primarily to divert airtime from serious and more engaging news portals and to compete over online advertising money and audience share. There is no evidence to link these publications to a larger state strategy to counter the growth of voices of dissent. However, it is important to note that these shadow publications receive large amounts of advertising, possibly in return for their progovernment bias.

The government also uses financial pressure to push the most outspoken print media publications into closure or bankruptcy. Advertising revenue provided by the government or government-linked companies is not split fairly between independent and progovernment publications.[29] Powerful business entities, such as the three telecommunication companies, are known to adhere to state pressure to withdraw advertising money from news outlets that run counter to the state-owned media narrative.[30] The state, however, does not limit the ability of online media to accept advertising or investment from foreign sources, crucial to maintaining a profitable business and ensuring that citizens can access a range of different opinions and news sources. In addition, webhosting and free blogging services are freely accessible. ISPs are not known to employ bandwidth availability to discriminate on the basis of content.

Internet users take advantage of various social media tools to educate, organize, and mobilize people around a wide variety of issues. Facebook and mobile phones were used very effectively during the 2011 street protests. Facebook users grew by 490 percent from 860,000 to more than 5 million over the period of 2009 to 2012 and the social network is the most visited website in the country.[31] Bloggers were instrumental in disseminating their political views and managed to reach out to large numbers of protesters. Activists used mobile phones and cameras to present their versions of street events in a bid to counter the censored news coverage of state-controlled broadcasting.

The first widely-covered instance of online activism occurred in the summer of 2008, when an amateur cameraman in the northern Morocco area of Targuist filmed traffic police officers taking bribes from drivers. The "Targuist Sniper" video circulated widely on YouTube and Facebook, resulting in a police investigation that led to the arrest of the several police officers. The video served as a model of cyber-activism against daily and mundane corruption in other Moroccan cities. Nevertheless, the effects on corruption and accountability remained short-term as the government eventually stopped responding to such videos.

---

[28] Interview with Aboubakr Jamai conducted on February 11, 2013.
[29] Interview with Aboubakr Jamai conducted on February 11, 2013.
[30] According to *The Report: Emerging Morocco 2007* by Oxford Business Group, Maroc Telecom and Medi Telecom accounted for 16% of the total advertising market. In 2011, according to l'Economiste.ma, telecommunications advertising spending represents 23% of the total advertising market share, available at, http://www.leconomiste.com/article/889132-investissements-publicitairesbrla-tele-en-perte-de-marche, (accessed 29 march 2013)
[31] "Internet users, population and Facebook statistics for Africa 2012 Q2: Facebook 31-Dec-2012," Internet World Stats, http://www.internetworldstats.com/stats1.htm (accessed 14 January 2013)

More recently, online activism led to a national debate on Article 475 of the Moroccan penal code, which allows rapists to avoid prosecution if they agree to marry their victims. Events were sparked in March 2012, when a 16-year-old girl committed suicide after a seven month ordeal in which she was forced to wed her alleged rapist. Women's rights activists successfully used social media and online news platforms to counter arguments made by state-controlled radio and television outlets, rallying popular support for changes to the law. In January 2013, the government officially announced plans to revise the controversial article.[32]

VIOLATIONS OF USER RIGHTS

The Moroccan constitution of 2011 recognizes all Moroccan citizens as equals before the law.[33] Article 25 provides that the constitution guarantees all citizens "freedom of opinion and expression in all its forms." However, prior to the 2011 constitution, the Moroccan legislature adopted an array of laws that limited freedom of expression, such as the 2002 Press Code and the 2003 Anti-Terrorism Law. These provided legal sanctions against any criticism of "sacred" issues such as the monarchy, Islam, and territorial integrity. Crucially, these laws continue to be applied to online activity, resulting in the prosecution of several users for content posted online.

Article 27 of the 2011 constitution states that Moroccan citizens have the right to access information held by the government, elected institutions, and all public service institutions, except in cases in which doing so would violate national security, the privacy of individuals, or constitutional freedoms. For this constitutional right to become reality, a series of public policy debates are taking place to devise policies that would guarantee citizens access to information. However, given the authoritarian nature of the state, many activists are pessimistic and believe the end result will most likely lead to a stifling of internet freedom under the guise of privacy, national security, and counterterrorism.

Although the 2011 constitution strengthened the judiciary as a separate branch of government, the judiciary system in Morocco is far from independent. The king chairs the High Council of Judicial Power and appoints its members. As such, the courts often fail to produce fair and balanced rulings, frequently basing their decisions on recommendations from security forces.[34]

Articles 45, 46, and 47 of the 2002 Press Code stipulate that defamation against the courts, the military, public administrations, members of the government, and any public person are punishable by a prison term of one month to one year. Similarly, Article 52 outlaws criticism of foreign heads of state, foreign ministers, and diplomatic envoys residing in Morocco by stipulating punishments of one month to one year imprisonment and a fine of MAD 10,000 to MAD 100,000 ($800 to

[32] Smail Bellaouli, "Morocco to change law that allowed rapists to avoid punishment by marrying their victims", available at, http://www.huffingtonpost.com/2013/01/23/morocco-rape-marriage-law_n_2532259.html, (accessed 1 April 2013).
[33] Moroccan Constitution 2011, available at http://www.maroc.ma/NR/rdonlyres/B4E91D55-9F14-4526-94A6-2665F12C9B54/0/BO_5964BIS_Fr.pdf, (accessed 22 February 2013).
[34] Huffington Post, "Morocco Justice System: Justice Can Be Bought," available at, http://www.huffingtonpost.com/2011/12/08/moroccan-justice-sold-to_n_1135895.html (accessed 22 February 2013)

$8,000). Judges often apply these vague and oppressive laws to the online domain. In one case from October 2012, the head of the Council for the Moroccan Community Abroad sued the news portal Yabiladi.com for defamation over an article detailing his travel expenses.[35]

When prosecuting online activists, the state strategically avoids arresting the sort of high-profile leaders that would lead to significant media coverage. For instance, members of the February 20th Movement that were arrested did not possess leadership roles, but were well-respected local actors key to mobilizing support in their communities. Meanwhile, prominent online public figures such as Aboubakr Jamai or Ali Lamrabet remain free from prosecution, even if they are harassed or intimidated through more extralegal means.[36]

In one of the most well-documented cases related to online freedom of expression, rap artist Mouad Belghouat (known as *al-Haqed* or "the spiteful") was sentenced to one year in jail on May 11, 2012 for "insulting the police" in a music video that denounced police corruption and brutality.[37] The title of the song was "Kilab ed-Dowla" (Dogs of the State). His defense lawyer had argued that there was no evidence to link Belghouat to the uploading of the video. In another case, Walid Bahomane, an 18-year-old student, was sentenced to 18 months in prison for "attacking the nation's sacred values" after he allegedly ridiculed the king in a post he published on Facebook.[38] The 25-year-old activist Abdelsamad Haydour was also sentenced to three years in prison in February 2012 over a YouTube video in which he allegedly criticized the king.[39]

The blogger Mohamed Sokrate was controversially sentenced to three years in jail and a fine of MAD 5,000 ($590) by a Marrakech court in June 2012. The charges were drug-related, which his defense adamantly denied. Reporters Without Borders argued that his conviction was instead based on his online activism, in which he promoted secularism, defended civil liberties, and criticized the government.[40]

Ali Lmrabet, the well-known progressive journalist, has been the target of constant violent and nonviolent harassment by the security and intelligence services in the northern city of Tetouan.[41] Lmrabet runs the website *Demainonline*, which is openly critical of the monarchy and politicians in Morocco. However, in 2005 he was banned from publishing in Morocco for a period of 10 years, and some believe the state has not arrested him given the negative media coverage it may generate.

---

[35] Reporters without Borders, "Hazards mount for freedom of information in Morocco," available at, http://en.rsf.org/morocco-hazards-mount-for-freedom-of-08-10-2012,43499.html, (accessed 29 March 2013).
[36] Reporters without Borders, "Hazards mount for freedom of information in Morocco."
[37] Human Rights Watch, "Rapper sentenced to one year in prison for criticising police," available at, http://www.ifex.org/morocco/2012/05/14/alhaqed_sentenced/, (accessed 29 March 2013).
[38] Reporters without Borders, "Appeal court extends online critic's sentence," available at, http://www.ifex.org/morocco/2012/03/28/bahomane_haydour_sentences_confirmed/, (accessed 29 March 2013).
[39] Reporters without Borders, "Appeal court extends online critic's sentence."
[40] Reporters without Borders, "Blogger gets two-year jail sentence on trumped-up drug charges," available at, http://en.rsf.org/morocco-blogger-gets-two-year-jail-15-06-2012,42803.html, (accessed 29 March 2013).
[41] Reporters Without Borders, "Journalists targeted for criticising Moroccan officials," available at, http://www.ifex.org/morocco/2012/10/10/journalists_targeted/, (accessed on 29 March 2013).

Following street protests in January and February 2012 in the northeast city of Taza, Mohamed El Boukili, Abdul-Samad and Essam Morsi, and 18 other activists from the February 20th Movement were sentenced to jail terms and steep fines on various charges ranging from "insulting to the sanctities of the state," "disobedience," "insulting public officials while performing their duties," and "insulting to the sanctities of the King."[42] These online activists participated in street protests and posted content on YouTube that criticized the government and called for political reform.

While users are punished for content they post online, Moroccan citizens can create websites and write for blogs without any registration requirements imposed by the government. Mobile phones and SIM cards may also be purchased anonymously. In addition, customers do not need to register or provide any kind of identification at cybercafés. There are no indications that the purchase and use of encryption software by private citizens or companies is restricted.[43]

Nonetheless, activists who openly criticize government policies, particularly online opinion makers, receive personal attacks and derogatory comments from other users on their Facebook walls and Twitter accounts.[44] New accounts are created every day for the sole purpose of attacking digital activists. There is no clear indication regarding the identity behind the accounts and whether they are state-sponsored or simply overzealous private individuals. However, due to the amount of time and energy needed to engage in such activity, there are serious doubts that these are private citizens acting on their own personal resolve.

Some activists have voiced their suspicion that, given their docile nature, telecommunication companies may be cooperating with government authorities by passing on swathes of user data to security forces to conduct widespread surveillance. For example, there are suspicions that Maroc Telecom, through its subsidiary in Mali, performed intelligence gathering for French authorities prior to the recent military intervention in that country by French troops.[45] Many activists have questioned whether the company performs similar actions in Morocco.

In December 2011, Reflets.info, a French news site, published an investigation on the purchase of spyware from the French company Amesys.[46] The article refers to an investigation carried out by journalists from the Wall Street Journal who found that Amesys sold spyware to the former Qadhafi regime in Libya. [47] Reflets.info argues that the same spyware was sold to the Moroccan government and that engineers from Amesys spent time in the country training government

[42] Arabic Network for Human Rights Information, "Activist sentenced for 'insulting' the king", available at, http://www.ifex.org/morocco/2012/02/15/alhaidour_sentenced/, (accessed 20 February 2013).
[43] Interviews conducted on 29 March 2013 with Dr. Fouad Abbou, full professor of computer Science and Telecommunications and Dr. Hamid Harroud, director of the Information Technologies Services of Al Akhawayn University in Ifrane.
[44] Interviews with digital activists and online journalists.
[45] Fouad Harit, "Charlie Hebdo confirme: Vivendi est un acteur majeur de la guerre au Mali," February 11, 2013, available at http://www.afrik.com/charlie-hebdo-confirme-vivendi-est-un-acteur-majeur-de-la-guerre-au-mali (accessed 6 March 2013), and Mustapha May, "Charlie Hebdo: Maroc Telecom, big ears of France in Mali," available at, http://www.moroccomirror.com/index.php/politics-news/item/167-charlie-hebdo-maroc-telecom-big-ears-of-france-in-mali?tmpl=component&print=1, (21 February 2013).
[46] Reflets.com, "Amesys: un Finger de Pop Corn pour le Croco," available at http://reflets.info/amesys-un-finger-de-pop-corn-pour-le-croco/ (accessed 20 February 2013).
[47] Paul Sonne And Margaret Coker, "Firms Aided Libyan Spies," available at, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html (accessed 20 February 2013).

personnel for the use of such sophisticated spyware. The software, called Pop Corn, is used to monitor emails, Skype conversations, and other kinds of encrypted materials.

In addition to surveillance and malware attacks, online news portals that express dissenting voices are subject to continuous cyberattacks. Activists have admitted that, in order to maintain a functional news website, they must pay a substantial amount of money to maintain guards against cyberattacks. For example, Hisham Almiraat,[48] the co-founder of Mamfakinsh.com and one of the leaders of the February 20th Movement, stated that in July 2011 his website was subjected to a cyberattack by a sophisticated computer virus. The site administrator had received an e-mail through the page's contact form that seemed to contain promising journalistic leads, such as videos of police scandals. An investigation into the source and nature of the virus revealed that it was a Trojan Horse developed by a company in Milan, Italy. The virus downloads itself and hides among files, reading keystrokes and taking control of the keyboard and webcam at will.

The company refused to disclose its list of clients and there is no direct evidence that can link the state to such a purchase. However, prices for this type of software range in the hundreds of thousands of dollars, thereby ruling out private individuals. "There is only circumstantial evidence," Almiraat said in an interview, "but it leads to one and only one conclusion; the state is the only entity that has the financial power and the political motivation to target websites who publish dissenting content."

[48] Interview with Hisham Almiraat, conducted February 13, 2013. Almiraat, a medical doctor by profession, is the advocacy director for Global Voices, and a prominent digital activist in Morocco and abroad.

NIGERIA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	12	10
Limits on Content (0-35)	9	8
Violations of User Rights (0-40)	12	13
Total (0-100)	**33**	**31**

* 0=most free, 100=least free

POPULATION: 170 million
INTERNET PENETRATION 2012: 33 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Access to ICTs improved notably thanks to increasing investments in ICT infrastructure and growing competition between telecom service providers (see **OBSTACLES TO ACCESS**).
- Stakeholders regarded recent GSM license auctions as fair, transparent, and uninfluenced by political interference (see **OBSTACLES TO ACCESS**).
- Online self-censorship declined markedly after January 2012 Occupy Nigeria protests, and criticism of the government on social media increased (see **LIMITS ON CONTENT**).
- A draft Lawful Interception of Communications Regulation, introduced in February 2013, was criticized for potentially infringing on citizens' constitutional right to privacy and lacking safeguards or redress in case of abuse (see **VIOLATIONS OF USER RIGHTS**).
- An early 2013 news report said the federal government had contracted an Israeli company to help monitor internet communications; the 2013 budget also contained provisions to purchase monitoring and surveillance systems (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Access to the internet and other digital technologies is still limited for many Nigerians, though information communication technologies (ICTs) and internet penetration have continued to spread across the country due to the growth of mobile phone usage and data services over the past few years. Greater private sector and government investments in ICT infrastructure and increased competition between service providers have also played a key role, while stakeholders regarded recent GSM license auctions as fair, transparent, and uninfluenced by political cronyism. In 2012, the Ministry of Communication Technology set up a presidential committee tasked with the development of a National Broadband Plan that seeks to increase Nigeria's broadband penetration five-fold by 2018.[1]

Compared to the traditional media sphere in Nigeria, online media is relatively free from restrictions, and there were no known incidents of government filtering or interference with online content in the past year. Self-censorship has notably reduced since the January 2012 Occupy Nigeria protests, and people now freely discuss issues that were previously unpopular or taboo, such as gay rights. However, in January 2013, the Blue Coat PacketShaper appliance—a device that can help control undesirable traffic—was discovered on several private ISP's in Nigeria, though the details of why the technology is being deployed and by whom are unknown.

Nigerian users became increasingly suspicious of online censorship and surveillance during the coverage period, even as the government continued its push to make ICT tools more available to citizens. Suspicions of government intentions to monitor ICTs were confirmed in April 2013 when the online newspaper, *Premium Times*, published a news report revealing that the federal government had awarded a secret contract to Israel-based Elbit Systems to help monitor internet communications in Nigeria.[2] Citizen Lab research also found a FinFisher command and server, which communicates with malware that can be used for surveillance, located on a private ISP in April 2013.

During the coverage period, the government increased its criticism of published materials online and social media discourse through dedicated staff monitors and commentators. Legislative discussions on cybercrime also expanded in 2012 to reflect the country's heightened security threats, and a draft law now focuses on cyber security. Proposed legislation with possible clauses that may affect internet freedom in Nigeria—such as the draft 2011 Cybersecurity Bill and a new Draft Lawful Interception of Communications Regulation introduced in February 2013—were still under discussion at the National Assembly as of mid-2013.

[1] "Nigeria's National Broadband Plan 2013 – 2018," accessed June 15, 2013, http://bit.ly/18DUPsQ.
[2] Ogala Emmanuel, "EXCLUSIVE: Jonathan Awards $40 Million Contract to Israeli Company to Monitor Computer, Internet Communication by Nigerians," *Premium Times*, April 25, 2013, http://bit.ly/12K1rUR.

OBSTACLES TO ACCESS

Internet access in Nigeria has grown exponentially in recent years, particularly after the introduction of mobile phone data and Fixed Wireless Access (FWA) services in July 2007.[3] In 2012, internet penetration stood at 33 percent, up from 28 percent in 2011, according to the International Telecommunications Union (ITU).[4] The number of active mobile phone subscribers also increased from almost zero in 2000 to over 117 million subscribers or 84 percent penetration in March 2013, as reported by the Nigerian Communications Commission (NCC).[5] The latest ITU data notes nearly 113 million mobile phone subscriptions and a mobile phone penetration rate of 68 percent in 2012, up from 57 percent in 2011.[6]

Mobile internet subscriptions have also steadily increased in the past few years, reaching a penetration rate of 26 percent in 2012, according to an October 2012 report published by iHub Research.[7] This growth has been enabled by specific handsets such as Nokia's range of smartphones and BlackBerry devices that provide bundled data services to mobile subscribers. The number of BlackBerry users appears to be growing, particularly among young Nigerians, as service prices have dropped to about US$17 a month as of January 2013. Competition, helped by the Mobile Number Portability initiative launched in April 2013, has forced service providers to offer cheaper plans based on time (daily, weekly, or monthly) or use (social media-focused or messaging). Nevertheless, the quality of service remains poor, with users frequently complaining about their inability to enjoy data services.

Although many providers use the word "broadband" in their promotional materials, in practice there is limited broadband service available in Nigeria. The latest statistics reported by the Ministry of Communication Technology cite a broadband penetration rate of 6 percent as of December 2012,[8] with average broadband download speeds of 2.26 Mbps and upload speeds of 1.57 Mbps.[9] Recognizing the importance of ICTs for economic development, the communication ministry set up a presidential committee in September 2012 tasked with the creation of a national ICT policy and broadband plan that aims to increase Nigeria's broadband penetration five-fold by 2018.[10]

---

[3] Fixed Wire Access (FWA) is a type of high-speed internet access that uses radio signals as a connection to service providers instead of cables, enabling areas that lack fiber optic cables or DSL to access broadband internet.
[4] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[5] "Subscriber Data – Monthly Subscriber Data," Nigerian Communications Commission, accessed June 13, 2013, http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125&Itemid=73.
[6] International Telecommunication Union,"Mobile-cellular Telephone Subscriptions, 2000-2012."
[7] "An Analysis Mobile Technology in West Africa: The Case of Nigeria, Ghana and Cote D'Ivoire," iHub Research, October 2012, http://www.research.ihub.co.ke/uploads/2012/october/1351001605_819_249.pdf.
[8] Emma Okonji, "Nigeria Targets 20% Broadband Penetration in 2013," *This Day Live*, December 17, 2012, http://www.thisdaylive.com/articles/nigeria-targets-20-broadband-penetration-in-2013/133769/.
[9] "Nigeria," Net Index, accessed February 16, 2013, http://www.netindex.com/download/2,59/Nigeria.
[10] Olubunmi Adeniyi, "Nigeria to Yield Dividends of Broadband 'Within Shortest Possible Time,' Co-Chair of Presidential Broadband Team Assures," *Technology Times*, December 18, 2012, http://bit.ly/18Gnjl4.

Nevertheless, access to ICTs is characterized by a large urban-rural divide. According to a Gallup poll published in August 2012, 39 percent of urban Nigerians said they had used the internet in the last week, compared to 16 percent of those living in rural areas.[11] Low literacy rates are also an obstacle to access, with 28 percent of the population illiterate in English, the main language used by Nigerian online news outlets and blogs.[12]

High costs are another major impediment to internet access. While increased competition among service providers has made the cost of access more affordable for many Nigerians, the country's average minimum wage still stands at about US$115 per month.[13] FWA services cost an average of $65 per month (a decrease from $80 in 2010), and only about 9 percent of the Nigerian population reported having a computer in the household.[14] As of January 2013, the price for internet use in a cybercafe cost about $0.64 per hour, down from $1 in 2011, though cybercafes have seen a sharp decline in patronage in recent years due to expanding mobile internet usage enabled by the decreasing cost of data plans on GSM network. In 2012, the average cost of a GSM plan dropped from $1 per megabyte of data in 2011 to $0.30, and 26 percent of individuals surveyed in a 2012 Gallup poll who had used a mobile phone in the week prior had used it to access the internet.[15]

In addition to cost, power cuts continue to disrupt service and access, with many users reporting the need to use private generators to stay online during outages. While the country's electricity supply improved notably in 2012, it saw a huge decline in 2013 and Nigeria is still reportedly the largest importer of private power generators in Africa, despite the country's status as an oil-rich country.[16] Telecommunication companies also depend on diesel-powered generators to maintain consistent service amid sporadic power cuts, spending an estimated NGN 177 billion ($1.14 billion) annually on fuel for the generators needed to provide back-up power for the country's 22,000 base stations.[17] Moreover, the need to pay for expensive backup power generators has accelerated the closure of cybercafes that were already struggling with competition against the growing popularity of internet access via mobile devices.

In March 2007, the government established the Nigerian Internet Exchange Point as a means of connecting internet service providers (ISPs) to one another; it had 38 members as of December 2012.[18] Several telecommunications companies have also migrated to private fiber-optic cable projects, such as Glo-1 and MainOne, the latter of which provides connectivity for 21 ISPs,

---

[11] Broadcasting Board of Governors, "New BBG Gallup Data Shows Dramatic Rise In Mobile Use In Nigera," video, August 20, 2012, http://www.bbg.gov/press-release/new-bbg-gallup-data-shows-dramatic-rise-in-mobile-use-in-nigeria/.
[12] "At a Glance: Nigeria—Statistics," United Nations Children's Fund (UNICEF), last modified March 2, 2010, accessed June 29, 2012, http://www.unicef.org/infobycountry/nigeria_statistics.html.
[13] Minimum Wage, "Nigeria Minimum Wage, Labor Law, and Employment Data Sheet," International Minimum Wage Rates 2013, accessed January 31, 2013, http://www.minimum-wage.org/international/en/Nigeria.
[14] Broadcasting Board of Governors, "New BBG Gallup Data Shows Dramatic Rise In Mobile Use In Nigeria ."
[15] Broadcasting Board of Governors, "New BBG Gallup Data Shows Dramatic Rise In Mobile Use In Nigeria ."
[16] Clara Nwachukwu, "Nigeria Maintains Lead in Generator Imports in Africa…," *Vanguard*, January 10, 2011, http://www.vanguardngr.com/2011/01/nigeria-maintains-lead-in-generator-imports-in-africa-%E2%80%A6/.
[17] Amaka Eze, "Base Stations Gulp N178bn Worth of Diesel Annually," *This Day Live*, August 27, 2012, http://www.thisdaylive.com/articles/base-stations-gulp-n178bn-worth-of-diesel-annually/123273/.
[18] Internet Exchange Point of Nigeria, "Our Members," accessed December 13, 2012, http://www.nixp.net/index.php?option=com_content&view=article&id=13&Itemid=13.

telecommunication companies, banks and other corporate entities in Nigeria and Ghana.[19] However, the reduced cost of a cable connection over satellite has yet to be passed on to consumers.

The ICT market in Nigeria has expanded considerably over the past decade, with the number of licensed ISPs rising from 18 in 2000 to 139 (28 of which have licenses in need of renewal[20]) by the end of 2012. There are also 11 FWA providers,[21] and four GSM mobile phone operators that provide internet access to their subscribers.[22] Nevertheless, the growth of ISPs and FWA providers has slowed in recent years with the rise in mobile access. As of March 2013, the four privately-owned GSM companies had a total of 114 million subscribers between them, MTN with 51 million, compared to Globacom's 24 million, Airtel's 24 million, and Etisalat's 15 million.[23] Furthermore, the process of issuing GSM licenses has been very transparent. Unlike similar auctions that have been subject to political interference, most stakeholders regarded the first and subsequent GSM license auctions as fair, and friends of prominent politicians, who are usually recipients of such licenses, lost out in the process.

The only government-owned firm in the market, NITEL, is now inactive, with 58,750 landlines and 258,520 mobile lines. It has remained on the government's privatization list for several years following multiple attempts to sell it. In February 2009, Transcorp, a local conglomerate with strong ties to the government, relinquished the 51 percent stake that it had acquired in 2006,[24] and in February 2010, New Generation Telecoms, a consortium that includes China Unicom, won a controversial bid to purchase the company.[25] The president initiated an investigation in response to allegations of corruption surrounding the purchase, but the findings have not yet been published.[26] As of 2013, NITEL remained on the government's list of to-be-sold companies.

Internet services are governed by the Nigerian Telecommunications Act, which vests regulatory responsibilities in the NCC. All ISPs must obtain a license from the NCC to operate, and there have been no reports of any ISP being denied a license or registration renewal. However, new ISPs

---

[19] "Our Clients," Main One Cable Company, accessed December 23, 2012, http://www.mainonecable.com/our-clients.

[20] All 11 FWA providers have expired licenses according to the NCC website, which could mean that renewed license details have yet to be uploaded to the website, or that the regulator is in the process of renewing licenses. See: Nigerian Communications Commission, "Internet Services," accessed December 31, 2012, http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=326&Itemid=.

[21] Nigerian Communications Commission, "Fixed Wireless Access," accessed December 31, 2012, http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=4&Itemid=53.

[22] Nigerian Communications Commission, "Digital Mobile License," accessed December 31, 2012, http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=2&Itemid=53.

[23] Nigerian Communications Commission, "Operator Data," accessed December 31, 2012. http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=70&Itemid=76.

[24] "NITEL Board Ratifies Appointment of Chairman: About NITEL," Transcorp, September 24, 2008, http://www.transcorpnigeria.com/corporatecom/archives.php?page=fullstory&nid=60; Betrand Nwankwo and Juliet Alohan, "Nigeria: Transcorp Relinquishes 51 Percent Equity Share in Nitel/Mtel," *Leadership* via *All Africa*, February 26, 2009, http://allafrica.com/stories/200902260498.html.

[25] Camillus Eboh, "New Generation Telecoms Acquires NITEL," Reuters, February 16, 2010, http://234next.com/csp/cms/sites/Next/Home/5527697-146/new_generation_telecoms_acquires_nitel_.csp.

[26] Camillus Eboh, "Nigeria Cabinet Sacking Delays Nitel sale," Reuters, March 19, 2010, http://www.reuters.com/article/idUSLDE62I0WS20100319.

seeking to enter the market have faced challenges in their operations due to competition from larger ISPs and investor focus on the mobile sector.

Although the government nominates the NCC's nine-member board of commissioners, the regulator's decisions have been viewed as relatively independent. Nevertheless, in November 2012, the NCC executive commissioner Dr. Bashir Gwandu was removed from the board under controversial circumstances after he revealed the details of an alleged frequency racketeering scheme that involved the sale of a frequency slot belonging to the Nigeria Police to a private firm. The federal government commissioned a joint NCC board and Ministry of Communication Technology investigation, which declared Gwandu's claims as unfounded.[27] According to the government, the executive commissioner was removed from his post for "insubordination to the current leadership of the nation's telecoms regulatory agency."[28]

LIMITS ON CONTENT

No blocking or filtering of online content was reported during the coverage period, though evidence surfaced in the government's proposed 2013 budget indicated its potential desire to manipulate the online communications landscape. Calls to clampdown on the use of social media made by government officials in mid-2012 also increased fears of impending internet censorship.

Online media has been relatively free from restrictions in Nigeria, and to date, the authorities have not carried out any blocking or filtering of content, mainly due to the complex nature of Nigeria's internet framework, which makes it difficult to carry out systematic filtering or censorship.[29] Nevertheless, in January 2013, the Citizen Lab internet research group discovered evidence of the Blue Coat PacketShaper appliance—a device that can help control undesirable traffic sent via online applications by filtering according to content category—in Nigeria alongside 18 other countries around the world, including China, Bahrain, and Russia. While the device was traced to a private suburban network,[30] its discovery in Nigeria is disconcerting given recent revelations of the government's intent to install a monitoring and surveillance system (see "Violations of User Rights").

Otherwise, the last report of ICT disruption occurred on May 29, 2011, when residents of the capital city, Abuja, reported that telecommunication services were inaccessible in certain areas.[31]

---

[27] "Interview: I Blew Whistle on Frequency Racketeering in NCC, Gwandu Says," *Technology Times*, October 14, 2012, http://www.technologytimesng.com/news/2012/10/6951/.

[28] "Federal Government fires Gwandu from NCC," *Technology Times*, November 28, 2012, http://www.technologytimesng.com/news/2012/11/federal-government-fires-gwandu-from-ncc/.

[29] According to the last study by the OpenNet Initiative (ONI) conducted in 2007, several websites were inaccessible surrounding the 2007 presidential elections due to technical problems, not government intervention. OpenNet Initiative, "Internet Filtering in Nigeria," October 1, 2009, http://opennet.net/research/profiles/nigeria; OpenNet Initiative, "Internet Watch Report: The 2007 Presidential Elections in Nigeria," November 2007, http://opennet.net/research/bulletins/014.

[30] Discussion between a Freedom House consultant and Citizen Lab.

[31] While the incident was not confirmed or reported by the mainstream media, various blogs covered the story, with a blog post by *IT News Africa* reporting quotes from NCC representatives and the Visaphone service provider that cited security reasons behind the isolated telecom shutdown. The reported shutdown coincided with the inauguration of the president, and there

Some ISPs have been known to block access when users infringe on laws by downloading copyrighted content, but this has often been done to manage network traffic rather than to protect intellectual property.

The video-sharing website YouTube, social-networking site Facebook, microblogging application Twitter, and various international blog-hosting services are freely available and among the most popular websites in the country. According to the website rating company Alexa, the ten most popular websites in Nigeria in 2012 were Facebook,[32] Google Nigeria, Google, Yahoo, YouTube, Twitter, Blogspot, Twitter, Nairaland, an online discussion forum, the 302 Found web search service, and the *Vanguard*.[33] Three other Nigerian websites were cited in the top 20—*Punch* newspaper at number 13, GTBank at number 15, and *LindaIkeji*, (a gossip news site) at number 20.

Government manipulation of online content has not been a huge issue in Nigeria, though in June 2009, reports emerged that the Nigerian government planned to invest in sponsoring pro-government websites and blogs.[34] In practice, it has been difficult to confirm whether the plan has been implemented; however, a sharp increase in the volume of government responses to citizen comments, participation in debates, and opinion pieces on government positions through online media was observed in 2012. In addition, the government seems intent on creating its own social media tools, as indicated by Nigeria's 2013 budget proposal,[35] in which the information ministry had made provisions to spend 100 million naira ($623,000) for "developing social media platforms and networking with other platforms."[36]

Meanwhile, websites, blogs, and commentators are generally divided among those with antigovernment, progovernment, and neutral leanings. Web commentary appeared to tilt against the government in January 2012 during the Occupy Nigeria demonstrations, but there has been a more balanced set of discussions since then, with many online commentators moving the conversation towards socioeconomic issues in place of polarized debates. Furthermore, online self-censorship has reduced notably since the January 2012 protests, and people now freely discuss issues that were previously unpopular or taboo, such as gay rights. Criticism of the government on social media has also increased, as have responses from government representatives.

Nevertheless, there is some indication that the government is beginning to feel threatened by critical online commentary. On July 26, 2012, the President of the Senate of the Federal Republic

---

were claims of a possible bomb explosion following a similar event during the country's independence anniversary celebration in October 2010. See, Charlie Fripp, "Nigerians Angry Over Abuja Telecom Shutdown," *IT News Africa*, May 31, 2011, http://www.itnewsafrica.com/2011/05/nigeria-angry-over-abuja-mobile-shutdown.

[32] As of December 2012, there were over six million Facebook users. "Nigeria Facebook Statistics," Socialbakers, accessed December 29, 2012, http://www.socialbakers.com/facebook-statistics/nigeria.

[33] "Top Sites in Nigeria," Alexa, accessed January 4, 2013, http://www.alexa.com/topsites/countries/NG.

[34] Sokari Ekine, "Nigeria Government Launches Attack Against Bloggers," *Global Voices*, June 25, 2009, http://advocacy.globalvoicesonline.org/2009/06/25/nigeria-government-launches-attack-against-bloggers/; "Umaru Yar'adua Regime Launches $5 Million Online War," *Sahara Reporters*, June 16, 2009, http://www.saharareporters.com/news-page/umaru-yar%E2%80%99adua-regime-launches-5-million-online-war.

[35] "New Projects," in Ministry of Information 2013 Budget (Appropriation), Federal Republic of Nigeria, accessed June 29, 2013: 10, http://www.budgetoffice.gov.ng/2013%20appropriation/Copy%20of%2018.%20Summary_Information.pdf.

[36] Tolu Ogunlesi, "Social Media Lessons for Govts and Businesses," *Punch*, February 12, 2013, http://www.punchng.com/opinion/social-media-lessons-for-govts-and-businesses/.

of Nigeria, third in command after the president and vice president, called for a clampdown on the use of social media in Nigeria while speaking at a media retreat.[37] Government representatives from the Oyo State House of Assembly made similar declarations in 2012. These statements drew reactions from citizens who viewed these statements as signs of impending online censorship,[38] leading the director general of Nigeria's National Orientation Agency to publicly announce in January 2013 that the government would not restrict social media.[39]

There has also been some government interference in the economic aspects of online news publishing. For example, in 2011, the leading critical online newspaper, *234Next*, folded in part due to a refusal to provide advertising by government or progovernment businesses. In 2013, government patronage is still evident and is reputed to be the largest source of business contracts that companies depend for financial sustainability.

Nigeria is home to a diverse blogosphere, with entertainment blogs drawing the most readers and a growing number of Nigerians blogging about their personal lives or social issues. Blogs have gradually emerged as an important platform for discussion and a source of reliable news for many users, providing a space for lengthy debate among online commentators. Readers often leave comments on popular news-oriented blogs to express frustration with societal issues. The Nigerian blogosphere includes both expatriates and locally-based writers, and the popular platforms on which Nigerian bloggers interact and learn from one another include *Global Voices*, Blogger, Afrigator, and WordPress. The president's Facebook page has also become a major avenue through which citizens comment on public issues, and Twitter plays a prominent role in debates around events as they happen, with government ministers often hosting Twitter chats with the public.[40]

In addition, ICTs are playing an increasingly important role in mobilizing people for real life protests and providing updates on unfolding events. Online citizen activism in Nigeria was particularly evident in December 2012 when the Nigerian Youth Climate Action Network and Human Rights Watch released a joint statement announcing that the "Nigerian government's failure to produce promised funding to address the worst lead poisoning outbreak in modern history is leaving thousands of children to die or face lifelong disability."[41] The statement was intended to hold the government accountable to its May 2012 pledge of $4 million to clean up locations in Zamfara state that had been contaminated with lead during gold mining operations. The groups initiated a social media campaign, asking Nigerians to sign a petition and leave comments on the president's Facebook page,[42] while also using Twitter to demand that the government release the

[37] Leke Baiyewu, "Social Media Users Carpet Mark on Call for Censorship," *Punch*, July 29, 2012, www.punchng.com/news/social-media-users-carpet-mark-on-call-for-censorship/.
[38] Akinwale Aboluwade, "Assembly Seeks Law Against Abuse of Social Media," November 2, 2012, *Punch*, http://www.punchng.com/news/assembly-seeks-law-against-abuse-of-social-media/.
[39] Paul Adepoju, "Government Will Not Restrict Social Media in Nigeria – National Orientation Agency," *Humanipo*, January 11, 2013, http://bit.ly/11m3uz0.
[40] "[Town Hall Chat] Nigerian Youth Minister On Twitter @ 3-5pm Today," *Tekedia*, September 8, 2011, http://tekedia.com/21375/town-hall-chat-nigerian-youth-minister-twitter-35pm-today/.
[41] Human Rights Watch, "Nigeria: Death Stalking Lead-Poisoned Children," news release, December 6, 2013, http://www.hrw.org/news/2012/12/06/nigeria-death-stalking-lead-poisoned-children.
[42] Human Rights Watch, "Ask Nigeria's President What Happened to $4 Million," December 6, 2012, http://www.hrw.org/news/2012/12/06/ask-nigeria-s-president-what-happened-4-million.

promised funds.[43] These campaigns caught the attention of the Senate Committee Chair on Ecology and Environment who visited the contaminated community himself and used his Twitter platform to add further pressure on the government to take action. The government released the funds two days after the campaign was launched, demonstrating the potential power of social media in Nigeria.

VIOLATIONS OF USER RIGHTS

Legislative discussions on cybercrime were expanded in 2012 to reflect the country's heightened security threats, and proposals were drafted to deal with cybersecurity and lawful interception. Still under discussion as of mid-2013, the draft laws have elicited concerns over how they may limit internet freedom in Nigeria. The most concerning development in the past year involved revelations in April 2013 that the government had invested in monitoring and surveillance technology and the discovery of a FinFisher command server located on a private ISP.

Nigeria's 1999 constitution guarantees freedom of expression and of the press, and the lack of internet-specific legislation has generally fostered an open environment for online activities. Nonetheless, the country's legal framework was revised in 2011 to reflect the use of new media technologies through Section 84(1) of the 2011 Evidence Act, which provides for the admission of statements in documents produced by computers and electronic signatures as evidence in court. [44] Libel also remains a criminal offense in Nigeria, with the burden of proof resting on the defendant. Journalists covering sensitive issues such as official corruption, the president's health, and communal violence are regularly subjected to criminal prosecution, though such cases have yet to arise for online expression. Furthermore, the implementation of Sharia or Islamic law in 12 northern states has not affected internet freedom to date.

In November 2011, the office of the National Security Advisor and the Attorney General drafted the Cybersecurity Bill, revising the earlier Cyber Security and Information Protection Agency Bill, which had provisions that could restrict users' rights to free expression and privacy by allowing security officials to apprehend and prosecute users based on suspicion and without a court order. Taking into account feedback from citizens and stakeholders in the Nigerian ICT sector, the revised bill reduced the powers granted to security officers by requiring a court order for the seizure of any equipment and for arrests based on suspicion. The draft bill passed a second reading in the House of Representatives in November 2012.[45]

[43] Japheth Omojuwa, "#SaveBagega: President Jonathan has Moved, Time for Dr. Okonjo-Iweala to Shake Things," *YNaija*, January 30, 2013, http://www.ynaija.com/japheth-omojuwa-jonathan-has-moved-time-for-okonjo-iweala-to-shake-things-savebagega-y-frontpage/.
[44] Evidence Act, 2011, National Assembly, Federal Republic of Nigeria, accessed January 14, 2013, http://www.scribd.com/doc/86359478/Evidence-Act-2011
[45] Paul Adepoju, "Nigerian Cybercrime Bill Passed for Second Reading," *Humanipo*, November 29, 2012, http://www.humanipo.com/news/2618/Nigerian-cybercrime-bill-passed-for-second-reading.

Meanwhile, many fear that the draft 2010 Lawful Interception of Information Bill,[46] which was still being deliberated in the National Assembly as of May 2013, may include provisions that will allow voice and data monitoring. In February 2013, the NCC introduced a new draft Lawful Interception of Communications Regulation,[47] which seeks to accomplish through secondary legislation what the 2010 bill has been slow to achieve. Still under discussion in May 2013, the regulation was criticized for potentially infringing on the constitutional right to privacy, in addition to a lack of safeguards against abuse or opportunities for redress, and unclear supervisory and reporting provisions.[48]

There are no restrictions on anonymous communication online in Nigeria, though SIM card registration with service providers has been required since June 2009.[49] The process of registering existing SIM cards extended through mid-2012, after which point service providers were required to cut off unregistered users. Cybercafes, on the other hand, do not require customers to register or present any form of identification to go online, and monitoring software installed on their computers is used only for billing purposes.

Thus far, the Nigerian security services have not appeared to proactively monitor internet and mobile phone communications, but many online journalists have long suspected that they are being monitored by the state. Suspicions of government intentions to monitor ICT communications were confirmed in April 2013 when the online newspaper, *Premium Times*, published a news report revealing that the federal government had awarded a secret contract to Israel-based Elbit Systems to help monitor internet communications in Nigeria.[50] This finding was further corroborated by publicly available details of Nigeria's 2013 budget, in which the Office of the National Security Adviser requested $61 million for a "wise intelligence network harvest analyzer system, open source internet monitoring system, personal internet surveillance system" and "encrypted communication equipment."[51] Citizen Lab research also found a FinFisher "Command and Control" server, which communicates with malware that can be used for surveillance, located on a private ISP in April 2013.[52] Nevertheless, the extent to which such surveillance systems have been implemented have yet to be established in May 2013.

---

[46] International Law Office, "Intercepting Private Communications," March 7, 0212, http://www.internationallawoffice.com/newsletters/detail.aspx?g=b24e48af-d424-4bd4-b526-52278a2e6d34#proposed.

[47] Nigeria Communications Commission, "Draft Lawful Interception of Communication Regulations," accessed February 10, 2013, http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=328&Itemid; Ojo Madueke, "Revealed: SSS, Police Have Powers to Tap Phone Lines," *This Day Live*, January 30, 2013, http://www.thisdaylive.com/articles/revealed-sss-police-have-powers-to-tap-phone-lines/137851/; "Mind That Conversation: Security Operatives To Tap Phones, Track E-mail," *Naij*, February 5, 2013, http://m.naij.com/news/22640.html; Ken Nwogbo, "SSS, Police Get Powers to Tap Phones," *Nigeria Communications Week*, January 29, 2013, http://www.nigeriacommunicationsweek.com.ng/telecom/sss-police-get-powers-to-tap-phones.

[48] Kunle Azeez, "Concerns Over Proposed Lawful Interception Law," *National Mirror Online*, May 23, 2013, http://nationalmirroronline.net/new/concerns-over-proposed-lawful-interception-law/.

[49] Nigerian Communications Commission and National Identity Management Commission, "Design, Development and Delivery of SIM Card Registration Solution," June 15, 2009, http://www.ncc.gov.ng/Archive/Headlines/SIM_Registration_RFP.pdf.

[50] Ogala Emmanuel, "EXCLUSIVE: Jonathan awards $40 Million Contract."

[51] "Research and Development/Ongoing Projects," in Office of the National Security Adviser 2013 Budget (Appropriation), Federal Republic of Nigeria, accessed June 29, 2013: 10, http://www.budgetoffice.gov.ng/2013%20appropriation/37.%20Summary_ONSA.pdf.

[52] Morgan Marquis-Boire et al., "For Their Eyes Only: The Commercialization of Digital Spying," Citizen Lab, May 1, 2013, https://citizenlab.org/2013/04/for-their-eyes-only-2/.

Meanwhile, according to the "Guidelines for the Provision of Internet Service" published by the NCC, ISPs are required to cooperate with law enforcement and regulatory agencies in providing "any service related information… including information regarding particular users and the content of their communications" during investigations of cybercrime or other illegal activity.[53] No details are provided in the guidelines regarding the oversight mechanisms required to prevent government authorities from acquiring free access to user information. The guidelines also stipulate that ISPs must retain user data and "the content of user messages or routing data" for at least 12 months.[54] There are no clear provisions on what the NCC expects of mobile phone companies.

While the constitution protects freedom of expression and of the press, the state often uses arbitrary and extralegal measures to suppress political criticism in the traditional media. The Nigerian authorities have a history of arresting and intimidating traditional media workers, and at least ten journalists have been killed in connection with their work since 1998.[55] In addition, there is a culture of impunity for crimes against media workers, though there have been no reports of individuals being sentenced to prison or physically attacked for their online activities.

Cyberattacks have increased in Nigeria, though most of the attacks have been against government websites and carried out by the Naija Cyber Hacktivists,[56] a group that has claimed responsibility for almost all cyberattacks to date. In 2012, cyberattacks against government websites reportedly increased by 60 percent, up from 10 percent in 2010,[57] with a total of 38 websites defaced by hackers.[58] Private sector websites such as those of an airline, a sugar processing company, and the Labour Union were also hacked in 2012,[59] with most of the messages left on the defaced websites aligning with citizen protests.

In response to growing instances of cybercrime in Nigeria, the government has increased its measures to crackdown against criminal activity online. A 2011 Ernst & Young report found that the country's unchecked cybercrime imposes costs on the Nigerian economy to the tune of $200 million per year from cyberattacks alone.[60] In February 2013, the Nigerian House of Representatives put forth a proposal to amend the 2004 criminal and penal codes to place strict penalties on cybercrime, prescribing fines ranging from 5 to 25 million naira for offenders and jail

---

[53] "Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission," accessed June 27, 2013; 2 http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=62&Itemid=53.
[54] "Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission," 3.
[55] Committee to Project Journalists, "10 Journalists Killed in Nigeria since 1992/Motive Confirmed," accessed January 30, 2013, https://www.cpj.org/africa/nigeria/.
[56] Richard Essien, "EFCC & NCC Websites Hacked," *Daily Times*, October 29, 2011, http://dailytimes.com.ng/article/efcc-ncc-websites-hacked.
[57] "Cyber Attacks At Nigerian Government Websites Increased By 60% In 2012," *TechLoy*, January 17, 2013. http://techloy.com/2013/01/17/nigerian-government-websites-cyber-attack-report.
[58] The hacked websites included those of Ministry of Transport, National Agency for Food and Drug Administration and Control, Economic and Financial Crimes Commission, Nigerian Army Education Corp, Central Bank of Nigeria, Nigeria Police, Ministry of Science & Technology, Navy, Defense Headquarters, State Security Service, News Agency of Nigeria and National Examinations Council.
[59] "NLC Website Hacked over Botched Occupy Nigeria Protest," *Ogala*, January 27, 2012, http://ogala.wordpress.com/2012/01/27/nlc-website-hacked-over/.
[60] Ben Uzor Jr, "Nigeria Now Attractive to Cyber Criminals – Ernst & Young," *Business Day*, September 27, 2011, http://bit.ly/nPlzg7.

terms between 2 and 15 years.[61] The Ministry of Justice resisted the proposed amendments, advising that a "comprehensive executive bill on cybercrimes" would be a better approach than amending the criminal and penal codes.[62] Meanwhile, broader conversations on issues of cyber-security have also focused on how to protect internet freedom.

Nevertheless, at the ITU's World Conference on International Communications in Dubai in December 2012, Nigeria joined countries such as Russia, China, and the United Arab Emirates in signing a proposal that sought to extend the International Telecommunication Regulations to give national governments regulatory jurisdiction over the internet.[63] The proposal was not adopted due to opposition from countries such as the United States, United Kingdom, Egypt, and Kenya out of concern that that the regulations would threaten internet freedom.[64]

[61] "Reps Propose N25 Million Fine And 15-Year Jail Term For Yahoo Boys," *Naij*, February 9, 2013, http://www.talkofnaija.com/news/132343_reps-propose-n25-million-fine-and-15-year-jail-term-for-yahoo-yahoo-boys
[62] John Ameh, "Reps Block Bid to Stop Criminal Code Hearing," *Punch*, February 12, 2013, http://www.punchng.com/news/reps-block-bid-to-stop-criminal-code-hearing/.
[63] "Who Signed The ITU WCIT Treaty... And Who Didn't," *TechDirt*, December 14, 2012, https://www.techdirt.com/articles/20121214/14133321389/who-signed-itu-wcit-treaty-who-didnt.shtml.
[64] Charles Arthur, "Internet Remains Unregulated After UN Treaty Blocked," *Guardian*, December 14, 2012, http://www.guardian.co.uk/technology/2012/dec/14/telecoms-treaty-internet-unregulated.

PAKISTAN

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	19	20
Limits on Content (0-35)	18	20
Violations of User Rights (0-40)	26	27
Total (0-100)	**63**	**67**

* 0=most free, 100=least free

POPULATION: 180 million
INTERNET PENETRATION 2012: 10 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- In 2013, officials sought to systematize nationwide online content filtering, an effort that was supposedly quashed in March 2012 (see **LIMITS ON CONTENT**).
- Information authorities blocked YouTube and 20,000 other websites for anti-Islamic content in 2012 (see **LIMITS ON CONTENT**).
- The Pakistani Taliban claimed responsibility for critically wounding 15-year-old blogger and activist Malala Yousufzai in October 2012 (see **VIOLATIONS OF USER RIGHTS**).
- Islamist activists bombed at least three cybercafés or mobile phone stores on moral grounds in 2013 (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Pakistan has seen an increase in citizen journalism and online activism in recent years, despite numerous social and political obstacles to internet access. Successive military and civilian governments have adopted various measures to control the internet in Pakistan, which they frame as necessary for combatting terrorism and the preservation of Islam. However, censorship decisions often reflect political motives—as coverage of political independence movements are consistently censored—or the influence of religious extremists who believe information and communications technologies (ICTs) spread obscenity. While internet penetration continued to improve in 2012 and early 2013, internet freedom in Pakistan looks increasingly precarious, a trend that could have significant consequences for the country's socioeconomic development.

Long-awaited general elections to the country's national assembly took place just outside the coverage period of this report on May 11, 2013, unseating the coalition led by the Pakistan People's Party and its co-chair, President Zardari, who will remain in office until his term expires in September 2013.[1] The Pakistan Muslim League under Nawaz Sharif, a former prime minister, formed the next government in June.

In the run-up to the polls, information restrictions were focused on maintaining security. An anti-Islamic video on YouTube that sparked unrest around the Muslim world caused the government to block access to the entire site in September 2012, followed by an additional 20,000 websites deemed to contain offensive content. Authorities also blocked mobile phone networks throughout major urban centers during many religious or national holidays. These supposed security measures, while restricting ICT usage for hundreds of thousands of users, failed to curb the rate of violent, often fatal attacks on journalists and internet users. Islamic militant groups targeted internet cafés and mobile phone stores with explosive devices, and the Pakistani Taliban claimed responsibility for the shooting of 15-year-old blogger and rights activist Malala Yousufzai in Swat, launching a worldwide social media campaign of support for the teenager, who survived skull surgery and now lives in the United Kingdom.

Legal measures also threatened digital rights, particularly over sensitive religious issues. At least two of the 23 criminal investigations launched in 2012 under Pakistan's strict blasphemy laws—which carry the death penalty—involved content sent by mobile phone. A Twitter spat escalated into a defamation suit after a political website accused a religious leader of inciting hatred. And in January 2013, the regulatory authority chairman Farooq Ahmed Khan announced that a blocking mechanism to filter un-Islamic, pornographic, and blasphemous material from websites would be activated in Pakistan within 60 days. Whether such technology is now in place, however, and how closely it relates to a 2012 proposal by the National ICT Research and Development Fund for a national internet firewall which was ostensibly scrapped due to public opposition, is unclear—as are the surveillance implications of the mechanism for private communications sent via ICTs. In

[1] Moeen Cheema, "Pakistan Elections and the Challenges Facing the New Government," Al Jazeera, May 13, 2013, http://www.aljazeera.com/indepth/opinion/2013/05/201351355212336147.html.

February 2013, the upper house of parliament passed the counter-terrorist Fair Trial Act 2012, which allows security agencies to monitor electronic communications; though the surveillance requires a judicial warrant, some fear the Act's broad wording leaves it open to abuse.

Despite a proactive defense of internet freedom by engaged civil society groups and their embrace of online tools to promote electoral transparency,[2] recent developments indicate a worrisome movement from ad hoc censorship towards systematized filtering and monitoring that the authorities preferred not to acknowledge before the international community. Subsequent to a Universal Periodic Review of its human rights practices in late 2012, Pakistan was elected a member of the United Nations Human Rights Council for 2013-2015.[3] While its pledge to the council supporting its candidacy referenced Pakistan's "free media" and "vibrant civil society," the country's UN mission made no mention of the internet at all, or its recent moves to curtail citizens' digital rights.[4]

OBSTACLES TO ACCESS

Internet penetration in Pakistan stood at 10 percent in 2012, according to the International Telecommunications Union.[5] A local report put the figure at 16 percent in mid-2013.[6] Mobile penetration was at 67 percent.[7] Low literacy, difficult economic conditions, and cultural resistance have limited the proliferation of ICTs in Pakistan.[8] Poor copper wire infrastructure and inadequate monitoring of service quality by the Pakistan Telecommunication Authority (PTA) have historically stymied the expansion of broadband internet.[9] While the cost of internet use has fallen considerably in the last few years,[10] access remains out of reach for the majority of people in Pakistan, and most users go online at their workplace or school. Cybercafes are largely limited to major cities, and recent news reports about employees stealing data to harass female clients online have contributed to public perceptions that they are unsafe.

Better quality broadband services remain concentrated in urban areas like Karachi, Lahore, Peshawar, Hyderabad, Faisalabad, and Islamabad. According to 2012 data, there are 50 operational internet service providers (ISPs) throughout Pakistan, along with ten broadband service providers

[2] Faisal Kapadia, "Watchdog Social Media Monitor Pakistan's Historic Elections," *Global Voices,* May 9, 2013, http://globalvoicesonline.org/2013/05/09/watchdog-social-media-monitor-pakistans-historic-elections/.
[3] "UN HRC Membership Elections: Clean Slates Permitted Empty Pledges by Asian State," Forum-Asia, November 13, 2012, http://www.forum-asia.org/?p=15587.
[4] United Nations General Assembly, "Note Verbale Dated 28 September 2012 from the Permanent Mission of Pakistan to the United Nations addressed to the Secretariat," October 2, 2012, http://www.un.org/ga/search/view_doc.asp?symbol=A/67/486.
[5] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. In 2010, the ITU indicated an internet penetration rate of 17 percent based on estimates by the PTA; they subsequently revised it to 8 percent.
[6] "30m Internet Users in Pakistan, Half on Mobile: Report," *Express Tribune,* June 24, 2013, http://bit.ly/1cdIifE.
[7] International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2012."
[8] A. Khan, *Gender Dimensions of the Information Communication Technologies for Development* (Karlstad: University of Karlstad Press, 2011). Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1829989.
[9] Muhammad Jamil Bhatti, "Broadband Faces Obstacles in Pakistan," *Oh My News*, December 20, 2006, http://english.ohmynews.com/articleview/article_view.asp?at_code=381272.
[10] "Incentive Package," Knowledge Management, accessed August 2012, http://bit.ly/19Ke7fX.

and five hybrid fiber-coaxial operators providing broadband internet.[11] All ISPs are controlled by the government through the PTA. For its backbone, the country is connected via the government-controlled Pakistan Internet Exchange with the SEA-ME-WE 3 and 4 cables,[12] along with backup bandwidth provided by TransWorld Associates.[13] Local media reported under-sea fiber optic cables sustaining damage in two separate incidents in March 2013, disrupting to up to 50 percent of the country's connections.[14]

Most remote areas lack broadband, while slow, intermittent connections render any meaningful online activities—such as multimedia training for students and entrepreneurs—challenging. Conflict-stricken areas like Khyber Pakhtunkhwa (formerly North West Frontier Province) and the Federally Administered Tribal Areas (FATA) have significantly reduced internet access.[15] Pakistan faced frequent electricity shortfalls throughout 2012,[16] resulting in outages lasting several hours across the country. The situation was particularly grim in rural areas where rolling blackouts extended to as many as 20 hours a day.

In 2006, the government of Pakistan initiated the Universal Service Fund to promote access to ICT services and broadband across the country.[17] One of its core projects is the establishment of universal telecenters in rural areas with populations above 5,000 that offer access to health, education, and employment opportunities. However, contracts for building the centers were cancelled without public explanation in 2012 and now are being re-auctioned, a sign that bureaucracy is further slowing the rate of development.[18]

Bureaucratic hurdles have also slowed the development of 3G or 4G networks,[19] and wireless service providers using the high-capacity data network WiMax or high-speed broadband technology EVDO, along with mobile operators Mobilink, Ufone, Telenor, Warid, and Zong have struggled to attract consumers due to high prices and poor coverage. In late 2012, a National Assembly standing committee declared the PTA had violated rules in auctioning 3G licenses.[20] The prime minister approved a new 3G policy for Pakistan and began auctioning contracts to service providers in January 2013.[21]

The PTA is responsible for issuing licenses to telecommunications companies and internet and mobile service providers through a bureaucratic process that includes hefty licensing fees.[22] By

[11] "Internet Facts," Internet Service Providers Association of Pakistan, last updated April 26, 2012, www.ispak.pk.
[12] SEA-ME-WE is the "South-East Asia – Middle East – Western Europe" fiber-optic submarine telecommunications cable connects those regions. SEA-WE-ME 4 was completed in 2005; SEA-WE-ME 3 in 2000.
[13] "Cable and Wireless Worldwide Wins New Contract from Transworld Associates for International Data Services," Cable and Wireless Worldwide, press release, July 21, 2010, http://bit.ly/14TbEjq.
[14] Farooq Baloch, "Undersea Cable Cut Affects 50% of Pakistan's Internet Traffic," March 27, 2013, http://bit.ly/14nTQ0q.
[15] Tayyeb Afridi, "Radio in FATA: A Foreign Voice for Local Problems," *Express Tribune* (blog), June 3, 2012, http://bit.ly/L9N3wy.
[16] "Khawaja Asif Urges People to Bear Load Shedding with Patience," *Pakistan Today*, June 30, 2013, http://bit.ly/17MtdoR.
[17] Ministry of Information Technology, "Universal Service Fund," accessed July 2013, http://www.usf.org.pk/.
[18] Ministry of Information Technology, "Universal Telecentres—Pilot Project," accessed July 2013, http://bit.ly/19Ke4k8.
[19] Dr. Basit Riaz Sheikh, "Bringing 3G to a City Near You," *Express Tribune*, November 22, 2012, http://bit.ly/R1NKgX.
[20] "3G Licenses Auction: NA Committee Holds PTA Responsible for Rules' Violation," *Dawn News*, December 31, 2012, http://dawn.com/2012/12/31/3g-licenses-auction-na-committee-holds-pta-responsible-for-rules-violation/.
[21] Fawad Khan, "3G in Pakistan to be Launched in January," Aaj TV, November 16, 2012, http://bit.ly/WdjXmS.
[22] Pakistan Telecommunications Authority, "Functions and Responsibilities," December 24, 2004, http://bit.ly/1bRmTNN.

contrast, internet cafes do not require a license to operate, and opening an internet cafe is relatively easy.[23] However, in January 2012, the provincial cabinet in Punjab approved a Net Cafe Regulations Act (Punjab Cyber & Gaming Cafe Regulation Act 2012),[24] which some analysts noted would oblige cafe owners to register their businesses, among other requirements that could potentially restrict user anonymity.[25] The document was never made public, and after provincial elections in May 2013 reshuffled the local administration, it was unclear when the regulations would be implemented, or if other provinces would follow suit.

Pakistani authorities often deliberately obstruct ICT access in the southern province of Balochistan, where a conflict between Baloch nationalists and state security forces or anti-separatist militias has persisted since 1948. During the national March 25 Pakistan Day celebrations in 2012, mobile service was cut in the entire province based on Interior Minister Rehman Malik's "order to implement national security policy," according to the chairman of the PTA.[26] At least one local official denied security concerns and characterized the shutdown as routine maintenance,[27] but many Baloch people saw the move as discriminatory.[28]

The same tactic was used throughout the year in cities facing possible security threats. PTA and security officials partially suspended mobile networks in urban areas around the country for a religious holiday in November 2012,[29] during a religious procession in January 2013,[30] to thwart attacks on a political march on Pakistan's capital city led by a reformist cleric, [31]and on New Year's Eve and Eid-ul-Fitr.[32] Civil society groups consider these actions an attack on citizens' freedom of expression, and an international service provider is seeking damages from the PTA and the information ministry for loss of revenue.[33]

The prime minister appoints the chair and members of the PTA, which reports to the ministry of information technology and telecommunication.[34] International free expression groups and experts have serious reservations about the PTA's openness and independence as a regulatory body.[35]

---

[23] Sehrish Wasif, "Dens of Sleaze," *Express Tribune*, July 22, 2010, http://tribune.com.pk/story/29455/dens-of-sleaze/.
[24] Office of the Chief Minister of Punjab, "Provincial Cabinet Sanctions Net Café Regulations Act," January 14, 2012, http://chiefminister.punjab.gov.pk/index.php?q=node/1228.
[25] Mehwish Shan, "Punjab to Regulate Internet Cafes," *Pro Pakistani*, December 21, 2011, http://bit.ly/HbLsGf.
[26] Zahid Gishkori, "Security: Cell Phone Services in Balochistan Suspended on Pakistan Day," *Express Tribune*, March 23, 2012, http://tribune.com.pk/story/354095/security-cellphone-services-in-balochistan-suspended-on-pakistan-day/.
[27] "Security concerns': On Pakistan Day, Balochistan blacked out," *Express Tribune*, March 24, 2012, http://bit.ly/GKtgnQ.
[28] "Baluchistan: Access Should Not Be A Victim To National Security," *Bolo Bhi*, August 14, 2012, http://bit.ly/1fyLidq.
[29] "Mobile Phone Services to be Partially Suspended During Ashura Holiday," *Dawn,* November 23, 2012, http://bit.ly/10nP53k.
[30] "Mobile Phone Services to Remain Suspended on Thursday," *Dawn*, January 2, 2013, http://bit.ly/UbcrJx.
[31] Asad Kharal and Zahid Gishkori, "Long March: In the Name of Security, Mobile Services Suspended," January 13, 2013, http://tribune.com.pk/story/493420/long-march-in-the-name-of-security-mobile-services-suspended/.
[32] "Cell Phone Service Ban on New Year Eve Sought," *Dawn*, December 30, 2012, http://dawn.com/2012/12/30/cellphone-service-ban-on-new-year-eve-sought/."Eid-ul-Fitr Security: Cellphone Services Blocked in Major Cities," *Express Tribune*, August 20, 2012, http://tribune.com.pk/story/424463/eidul-fitr-security-cellphone-services-blocked-in-major-cities/.
[33] "Mobile Suspension Case: SHC Issues Notices to PTA, Interior Ministry," *Express Tribune*, November 22, 2013, http://tribune.com.pk/story/469691/mobile-suspension-case-shc-issues-notices-to-pta-interior-ministry/.
[34] Pakistan Telecommunications Authority, "Pakistan Telecommunication (Re-organization) Act 1996," October 17, 1996, http://www.pta.gov.pk/media/telecom_act_170510.pdf.
[35] Article 19, "Legal Analysis – Pakistan: Telecommunications (Re-organization) Act," February 2, 2012, http://bit.ly/xQC5ra.

LIMITS ON CONTENT

The government's efforts to systematize website blocking by creating and installing new equipment for nationwide content filtering were among the most concerning developments of 2012 and 2013. While the first attempt was supposedly quashed in March 2012, PTA officials were still voicing their intent to implement new blocking technology in 2013. They received an unexpected boost by the battle over YouTube, which was unilaterally blocked in Pakistan in the wake of an offensive, anti-Islamic upload. Since Google declined to remove the video, the government refused to restore access to its video-sharing platform until it could block the unwanted content directly. In May 2013, the status of the new firewall remained unclear.

Since January 2003, the government of Pakistan has taken steps to censor some online content, and the system for doing so has become increasingly sophisticated.[36] A wide variety of government agencies are involved in the censorship of online content, but the PTA is the main one. Authorities can block URLs at the internet exchange point through the PIE, and individual ISPs are required to carry out content-related directives issued by the PTA or have their license suspended. Individuals or groups also play a role, petitioning courts to order the ministry to enact moral bans on online or traditional media content.[37] Presumably, the PTA maintains the list of sites to filter, but the details are not known. There are no published guidelines outlining how or why content is blocked or what mechanisms are available to challenge it. Error messages seen by users trying to access blocked websites usually refer to the censored content as "blasphemous" or state that the "site is restricted."

Censorship targets some content, such as pornography, on moral grounds and can be inconsistent across ISPs, according to an August 2012 OpenNet Initiative report.[38] A range of provisions in the 1996 Pakistan Telecommunications Act support censorship for the protection of national security and Islam.[39] Authorities also cite Section 99 of the penal code, which allows the government to restrict information that might be prejudicial to the national interest, to justify filtering anti-military, blasphemous, or anti-state content.[40] Critics believe these issues can serve as a cover for politically motivated censorship of dissenting voices. Information disseminated by Balochi and Sindhi political dissidents, for example, is among the nation's most systematically censored content.[41] In 2010, authorities blocked the region's first English-language news website *The Baloch Hal* a year after its launch.[42]

Information perceived as damaging to the image of the military or top politicians is also targeted, such as a satirical music video about military generals, which was replaced on video-sharing site

[36] OpenNet Initiative, "Country Profile—Pakistan," December 26, 2010, http://opennet.net/research/profiles/pakistan.
[37] "Internet censorship: Court Asked to Ban Inappropriate Content," *Express Tribune*, June 14, 2011, http://bit.ly/jOCZFP.
[38] OpenNet Initiative, "Country Profile—Pakistan," August 6, 2012, http://opennet.net/research/profiles/pakistan.
[39] Article 19, "Legal Analysis – Pakistan."
[40] "Pakistan: Code of Criminal Procedure," available at the Organization for Economic Co-operation and Development website, accessed August 2013, http://www.oecd.org/site/adboecdanti-corruptioninitiative/39849781.pdf.
[41] Pakistan Telecommunication Authority, "Blocking of Websites Access," letter, April 25, 2006, http://bit.ly/17d2EXs.
[42] "The Baloch Hal Banned," *Baloch Hal,* November 9, 2010, http://www.thebalochhal.com/2010/11/the-baloch-hal-banned/.

Vimeo by a page telling viewers it was "prohibited" within Pakistan in mid-2013.[43] The website of the Lal-Masjid mosque in Islamabad has been blocked since 2007 when it became the center of a government stand-off with conservative clerics.[44] In July 2011, the website of the popular American music magazine *Rolling Stone* was blocked by at least 13 ISPs after the site published a blog post discussing Pakistan's "insane military spending."[45] Rollingstone.com remains blocked as of February 2013 along with the website of the *Toronto Sun* newspaper, supposedly because it published articles by Canada-based secularist and journalist Tarek Fateh criticizing the Pakistani military.[46]

Since website blocking was first observed in Pakistan, much of it has targeted social media and communication apps. In 2006, the PTA—responding to widespread public pressure—instructed ISPs to block websites displaying controversial cartoon images of the prophet Mohammed, many on Google's blog hosting platform Blogger.[47] In 2010, over 10,500 websites were blocked,[48] including many on Facebook, YouTube, Flickr and Wikipedia, after the Lahore High Court ruled in favor of a legal appeal made by the Islamic Lawyers Movement over the Facebook page, "Everybody Draw Mohammed Day."[49] Mobile phone providers also completely halted Blackberry services; functionality was only gradually restored, though web-browsing functions remained restricted for longer.[50] While most social-networking and blog-hosting platforms were available and widely used throughout 2012 and early 2013, there were several temporary disruptions of Facebook and Twitter services, and different religious groups persistently exerted pressure on the Pakistani courts to ban Facebook completely.[51] Groups and individuals affiliated with political and religious parties have also filed court petitions against YouTube.[52]

The most wide-reaching ban in 2012 was imposed after a Californian internet user uploaded a 14-minute video to YouTube ostensibly promoting a movie he had created to denounce Islam titled "The Innocence of Muslims."[53] In September, the clip was dubbed into other languages, garnering hundreds of thousands of views and sparking violent anti-American protests in several Muslim

---

[43] "Song Critical of Pakistani Generals is Blocked Online, With No Official Explanation," *New York Times,* May 4, 2013, http://www.nytimes.com/2013/05/05/world/asia/satirical-song-blocked-in-pakistan-but-no-reason-is-given.html?_r=0.
[44] "Lal Masjid Issue and its Blocked Website," *Teeth Maestro*, April 12, 2007, http://bit.ly/5ayFuP.
[45] Jillian York, "Pakistan Escalates its Internet Censorship," Al Jazeera, July 26, 2011, http://aje.me/nuirDk; "Pakistan Blocks Sex, Drugs AND Rock and Roll," Association for Progressive Communications (blog), http://bit.ly/o2WMUw.
[46] "Toronto Sun Website Blocked in Pakistan: Report," *Express Tribune*, February 8, 2013, http://bit.ly/11UCR4P.
[47] Jefferson Morley, "Pakistan's Blog Blockade," *Washington Post* (blog), March 8, 2006, http://bit.ly/14TdwIY; PTA Unblocks Blogspot," *Teeth Maestro*, May 3, 2006, http://teeth.com.pk/blog/2006/05/03/pta-unblocks-blogspot.
[48] "The Shameful Saga of the Internet Ban in Pakistan," Association for Progressive Communication, July 22, 2010, http://www.apc.org/en/node/10786/.
[49] Islamic tradition forbids the depiction of Allah or Mohamed. "Pakistan Court Orders Facebook Ban," Al Jazeera, May 20, 2010, http://www.aljazeera.com/news/2010/05/201051994155758717.html.
[50] Aamir Attaa, "Blackberry Services Go Offline in Pakistan," *Pro Pakistani*, May 20, 2010, http://bit.ly/b5Dzth; Aamir Attaa, "Blackberry Services Yet to be Fully Restored," *Pro Pakistani*, June 4, 2010, http://propakistani.pk/2010/06/04/blackberry-services-yet-to-be-fully-restored/. Full Blackberry services were accessible in 2013.
[51] "Permanently Banning Facebook: Court Seeks Record of Previous Petitions," *Express Tribune*, May 6, 2011, http://tribune.com.pk/story/162801/permanently-banning-facebook-court-seeks-record-of-previous-petitions/.
[52] "Access Denied: As YouTube Remains Blocked, SHC Dismisses Plea for Ban," *Express Tribune*, March 29, 2013, http://tribune.com.pk/story/527923/access-denied-as-youtube-remains-blocked-shc-dismisses-plea-for-ban/.
[53] Ian Lovett, "Man Linked to Film in Protests Is Questioned," *New York Times*, September 15, 2012, http://nyti.ms/16JNAfz; Michael Joseph Gross, "Disaster Movie," *Vanity Fair*, December 27, 2012, http://vnty.fr/W3sPpO.

countries. In Pakistan, they resulted in at least 19 deaths.[54] Google, which owns YouTube, temporarily blocked versions of the video in some countries but declined to remove it altogether, and it remained accessible in Pakistan, despite Prime Minister Raja Pervez Ashraf's request that it be taken down.[55] News reports in Pakistan attributed this to the lack of a Mutual Legal Assistance Treaty with the U.S.—a legal agreement through with countries can negotiate over companies' compliance with local laws[56]—but how far this affected Google's decision is unclear. In response, the information ministry instituted a site-wide block on YouTube on September 17, 2012.[57] By October 9, another 20,000 websites were blocked, not just for featuring the anti-Islamic movie, but also for hosting material that the PTA characterized as "objectionable."[58]

Prior to this incident, many blocks were implemented on a temporary basis to calm protests against online content. In 2012, however, civil society groups protested against the ban—which affected more than seven million users of the service in Pakistan[59]—to no avail, and it continued almost uninterrupted through May 2013. The civil society organization Bytes for All filed a petition against the block in the Lahore High Court in January; hearings are ongoing.[60] Students who frequently refer to YouTube online lectures were particularly affected, and one institution, Pakistan's Virtual University, moved all educational material formerly hosted on YouTube to its own servers. In early 2013, Pakistani officials stated that the ban would stay in place until Google removed the content or until a nationwide filtering mechanism was in place, allowing them to control what YouTube content is available for themselves.[61]

The government set out to acquire such a mechanism in February 2012 on grounds that ISPs and backbone providers were unable to manage the volume of blacklisted sites manually.[62] The National ICT Research and Development Fund invited ICT companies to submit proposals to develop and operate a "national level URL Filtering and Blocking System,"[63] preferably one able to "handle a block list of up to 50 million URLs with a processing delay of not more than 1 millisecond."[64] Websites with "blasphemous, un-Islamic, offensive, objectionable, unethical, and immoral material" would be targeted, according to the notice.[65] After widespread protest from civil society,

[54] "'Innocence of Muslims' Protests: Death Toll Rising In Pakistan", *International Business Times*, September 21, 2012, http://www.ibtimes.com/%E2%80%98innocence-muslims%E2%80%99-protests-death-toll-rising-pakistan-794296.
[55] Lawrence Latif, "Pakistan and Bangladesh Block YouTube Over Innocence of Muslims Trailer," *The Inquirer*, September 19, 2012, http://bit.ly/164gJGP.
[56] Huma Imtiaz, "Pakistan Renewed its Ban on YouTube this Week. Could the Entire Internet be Far Behind?," February 15, 2013, http://qz.com/54618/pakistan-renewed-its-ban-on-youtube-this-week-could-the-entire-internet-be-far-behind/.
[57] "YouTube blocked in Pakistan," *The News International,* September 17, 2012, http://bit.ly/OxLpn5.
[58] "In Massive Censorship Move, Pakistan Blocks 20,000 "Objectionable" Sites," *The Daily Dot*, October 9, 2012, http://www.dailydot.com/news/pakistan-twenty-thousand-sites-blocked/.
[59] "Excessive Internet Bans Worrisome for Pakistan," *Dawn,* November 5, 2012, http://bit.ly/YHXwVp.
[60] Bytes for All, "Bytes for All vs. Federation of Pakistan – Updates on our Net Freedom Petition," April 14, 2013, http://content.bytesforall.pk/node/96.
[61] Andrew Webster, "Pakistan Will Lift Ban on YouTube After Building Filter for 'Blasphemous Material,'" *The Verge,* January 9, 2013, http://www.theverge.com/2013/1/9/3854816/pakistan-lift-youtube-ban-content-filter.
[62] Danny O'Brien, "Pakistan's Excessive Internet Censorship Plans," *CPJ Internet Channel*, March 1, 2012, http://bit.ly/yW8kb9.
[63] National ICT Research and Development Fund, "Request for Proposal: National URL Filtering and Blocking System," accessed August 2012, http://ictrdf.org.pk/RFP-%20URL%20Filtering%20%26%20Blocking.pdf.
[64] National ICT Research and Development Fund, "Request for Proposal."
[65] "PTA Determined to Block Websites with 'Objectionable' Content," *Express Tribune*, March 9, 2012, http://bit.ly/xEND9P.

the request for proposals was apparently shelved,[66] although that change was announced in the media rather than an official press release. In January 2013, PTA Chairman Farooq Ahmed Khan announced that an apparently unrelated "new mechanism" for blocking un-Islamic, pornographic, and blasphemous material from websites would be activated in Pakistan within 60 days, according to the *Pakistan Today* newspaper.[67] Other news reports were less clear about the timing for implementing new filtering devices,[68] possibly reflecting internal disputes between the PTA and the information ministry over costs and responsibility for the project.[69]

Authorities also target users seeking to access blocked content. In August 2011, the PTA sent a legal notice to all ISPs in the country urging them to report customers using encryption and virtual private networks (VPNs)[70]—technology that allows internet users to go online undetected, access blocked websites, and conceal communications from government monitoring—on grounds of curbing communication between terrorists.[71] International and civil society organizations in Pakistan raised effective voice against this repressive development;[72] however, the order still stands as of early 2013.

Despite existing limitations on online content—and looming new ones—Pakistanis have relatively open access to international news organizations and other independent media, as well as a range of websites representing Pakistani political parties, local civil society groups, and international human rights organizations.[73] ICTs, particularly mobile phones, promote social mobilization, including on free expression issues. The 2010 floods in Pakistan, for example, inspired many Pakistani citizens and members of the diaspora to mobilize and raise funds online.[74] Nevertheless, most online commentators exercise a degree of self-censorship when writing on topics such as religion, blasphemy, separatist movements, and women's and LGBT rights.

The relationship between citizen journalism and traditional media in Pakistan is mutually reinforcing. In 2013, reports of election rigging spread via Facebook and Twitter, prompting traditional media coverage.[75] Social media advocacy also advanced a police investigation into the shooting murder of 20-year old uptown Karachi resident Shahzeb Khan in December 2012.[76] The mainstream media and police initially responded with apathy to news of the attack, perhaps because

---

[66] Shahbaz Rana, "IT Ministry Shelves Plan to Install Massive URL Blocking System," *Express Tribune*, March 19, 2012, http://tribune.com.pk/story/352172/it-ministry-shelves-plan-to-install-massive-url-blocking-system/.
[67] Anwer Abbas, "PTA, IT Ministry at Odds Over Internet Censorship System," January 3, 2013, http://bit.ly/12Znc2Q.
[68] Apurva Chaudhary, "Pakistan To Unblock YouTube After Building Filtering Mechanism," *Medianama,* January 10, 2013, http://bit.ly/TMmcvh; Pakistan Press Foundation, "The Saga of YouTube Ban," January 2, 2013, http://bit.ly/1bhpMEP.
[69] "Ministry Wants Treaty, Law to Block Blasphemous Content," *The News International*, March 28, 2013, http://bit.ly/16JP6yo.
[70] Josh Halliday and Saeed Shah, "Pakistan to Ban Encryption Software," *Guardian*, August 30, 2011, http://bit.ly/outDAD.
[71] Nighat Dad, "Pakistan Needs Comms Security Not Restrictions," Privacy International (blog), September 12, 2011, https://www.privacyinternational.org/blog/pakistan-needs-comms-security-not-restrictions.
[72] Barbora Bukovska, "Pakistan: Ban on Internet Encryption a Violation of Freedom of Expression," Article 19, September 2, 2011, http://www.article19.org/resources.php/resource/2719/en/index.php?lang=en.
[73] OpenNet Initiative, "Country Profile—Pakistan" (2012).
[74] Issam Ahmed, "Pakistan Floods: How New Networks of Pakistanis are Mobilizing to Help," *Christian Science Monitor,* August 19, 2010, http://bit.ly/95cXzo.
[75] Mehwish Khan, "15 Election Rigging Videos From Pakistan That Went Viral on Social Media!," *Pro Pakistani,* May 11, 2013, http://propakistani.pk/2013/05/11/election-rigging-videos-and-images-go-viral-on-social-media/.
[76] "Full coverage: Shahzeb Khan Case," Geo TV, accessed February 2013, http://www.geo.tv/Trending.aspx?ID=126

one of his alleged assailants was well-connected.[77] However, a cameraman uploaded footage of the incident to YouTube for users still accessing the banned service via proxy servers. Thousands subsequently expressed concern for Shahzeb on Twitter and Facebook until the chief justice of the Supreme Court directed Karachi police to expedite the investigation. A court sentenced two perpetrators to death and their accomplices to life imprisonment in June.[78]

VIOLATIONS OF USER RIGHTS

In February 2013, the upper house of parliament granted security agencies permission to monitor private e-mails and mobile phone communications collect evidence of terrorist activity when they passed a piece of 2012 legislation governing trials. Other legal challenges faced by ICT users included a defamation suit stemming from comments made via Twitter, and of the 23-odd blasphemy cases reported in 2012, at least two involved text messages, causing one family to flee their home and one arrest. Though attacks on journalists from traditional media far outstripped those on bloggers and internet users, both groups received threats. In a case which resounded around the world, insurgents shot and seriously injured Malala Yousufzai for creating online content for the BBC about her life as a school-girl in a Taliban-controlled region of Pakistan.

Article 19 of the Pakistani constitution establishes freedom of speech as a fundamental right, although it is subject to several restrictions.[79] Pakistan also became a signatory to the International Covenant on Civil and Political Rights in 2010.[80] In 2011, Pakistan People's Party lawmaker Sherry Rehman, now ambassador to the United States, introduced the Right to Information Bill in the National Assembly, a law that would prevent all public bodies from blocking a requester's access to public records.[81] A Senate sub-committee reviewed the draft in June 2013 in preparation for tabling it for parliament to pass.[82]

Section 124 of the Pakistan penal code on sedition "by words" or "visible representation" is broadly worded, though it has been used infrequently to punish journalists and online speech.[83] However, Section 295(c), which covers blasphemy, has been invoked to limit freedom of expression and has featured in most recent cases concerning internet speech. In 2010, police initiated legal proceedings against Facebook founder Mark Zuckerberg over the page titled, "Everyone Draw Mohammad Day."[84] The maximum punishment for blasphemy is life imprisonment or the death

[77] Sana Jamal, "Shahzeb Khan – Symbol of Hope Against Pakistan's Powerful Feudals," *Global Voices*, December 31, 2012, http://globalvoicesonline.org/2012/12/31/shahzeb-khan-symbol-of-hope-against-pakistans-powerful-feudals/.
[78] "Shahzeb Khan's Murder: Shahrukh Jatoi, Siraj Talpur Get Death Penalty," *Express Tribune,* June 8, 2013, http://tribune.com.pk/story/560586/shahzeb-khans-murder-shahrukh-jatoi-siraj-talpur-get-death-penalty/.
[79] "The Constitution of Pakistan," available at *Pakistani,* accessed September 2012, http://bit.ly/pQqk0.
[80] "President Signs Convention on Civil, Political Rights," *Daily Times*, June 4, 2010, http://bit.ly/1fyK9Tl.
[81] Maha Mussadaq, "Sherry Rehman's Bill: Public May Eventually Access Organisations' Official Records," *Express Tribune*, October 17, 2011, http://bit.ly/qvS2G6.
[82] "Right to Information Act 2013 : Draft of law at final stage," *Daily Times,* June 14, 2013, http://bit.ly/16A1TKt.
[83] "Pakistan Penal Code," available at *Pakistani,* accessed August 2013, http://bit.ly/98T1L8; Karin Deutsch Karlekar, ed., "Pakistan," in *Freedom of the Press 2011* (New York: Freedom House, 2011), http://bit.ly/1biVaqb.
[84] Maija Palmer, "Facebook Founder Faces Pakistan Probe," *Financial Times*, June 17, 2010, http://on.ft.com/9583eo.

penalty, though the charges against Zuckerberg appear to have been quietly dropped after they were ridiculed in the press.

At least 23 blasphemy cases involving 27 defendants were reported in 2012, according to the Human Rights Commission of Pakistan.[85] Some of these involved electronic media. In October 2012, for example, neighbors filed a police complaint against a 16-year-old Christian boy in Karachi for allegedly sending them a blasphemous text message.[86] Reflecting the difficulty of proving intent in such cases, media reports published conflicting accounts of the message, some reporting that the unnamed boy acknowledged forwarding a message but denied creating it, and others saying the message was sent when his mobile phone was commandeered by friends. His family fled the area and neighbors ransacked their house. A second text message resulted in the arrest of the sender, even though he claimed to have circulated the blasphemous content to resolve a dispute with a customer.[87]

Accusing someone of blasphemy leaves them vulnerable to attack, regardless of whether it has foundation, while attempts to reform the punitive laws leave even politicians vulnerable. In January 2013, the Supreme Court ordered an investigation into Ambassador Sherry Rehman after a businessman accused her of blaspheming the Prophet during an October 2010 television talk show appearance to defend proposed changes to the blasphemy laws; police and lower courts had refused to consider the case.[88] Three months after that TV appearance, Salman Taseer, the governor of Punjab, was murdered by his own bodyguard for criticizing the same laws.

The 2004 Defamation Act allows for imprisonment of up to five years, and observers fear a chilling effect if it is used to launch court cases for online expression, particularly since internet users are already seeking to prosecute their rivals**.** In January 2013, a Twitter feud escalated into a defamation suit when Tahir Ashrafi, head of the Pakistan Ulema Council of Muslim clerics and scholars, announced that he would initiate civil proceedings against Let Us Build Pakistan, a political website, for allegedly inciting sectarian violence.[89] A writer on the site—which critics censure for spreading hate speech—had accused Ashrafi of forming alliances with banned extremist groups.

Government surveillance is a concern for activists, bloggers, and media representatives in Balochistan, as well as ordinary internet users wishing to comment openly on the state or religion, notably atheist groups. Pakistani authorities, particularly intelligence agencies, appear to have been expanding their monitoring activities in recent years, while provincial officials have been exerting pressure on the central government to grant local police forces greater surveillance powers and location tracking abilities, ostensibly to curb terrorism and violent crimes.[90] ISPs,

[85] Human Rights Commission of Pakistan, *State of Human Rights in 2012*, (Lahore: HRCP, 2013), http://bit.ly/183cVXq.
[86] "Teenage Christian boy booked for blasphemy," *Dawn*, October 11, 2012, http://bit.ly/SRWNBs.
[87] Faraz Khan, "Printer Texts Blasphemy to Get Customer to Pay," *Express Tribune*, January 9, 2012, http://bit.ly/A68hQl.
[88] "SC Admits Petition Against Sherry Rehman," *The News International*, January 17, 2013, http://bit.ly/15BOhh6; Christopher Dickey, "Pakistan's Woman Warrior," *Daily Beast*, March 25, 2013, http://thebea.st/YuVXbL.
[89] "Legal First: Twitter Feud Turned Defamation Suit," *Express Tribune*, January 22, 2013, http://bit.ly/10BNUiE.
[90] Masroor Afzal Pasha, "Sindh Police To Get Mobile Tracking Technology," *Daily Times,* October 29, 2010, http://bit.ly/16TKfLY; "Punjab Police Lack Facility of 'Phone Locator', PA Told," *The News International,* January 12, 2011, http://bit.ly/1bRl6bx.

telecommunications companies, and SIM card vendors are required to authenticate the National Identity Card details of prospective customers with the National Database Registration Authority before providing service.[91] Furthermore, under the Prevention of Electronic Crimes Ordinance—a 2007 bill that required ISPs to retain traffic data for a minimum of 90 days, among other regulations[92]—telecommunications companies were required to keep logs of customer communications and pass them to security agencies when directed by the PTA. While the bill officially expired in 2009, the practice is reportedly still active.

In February 2013, the upper house of parliament passed the Fair Trial Act 2012, which had been approved by the National Assembly in December.[93] The legislation allows security agencies to seek a judicial warrant to monitor private communications "to neutralize and prevent [a] threat or any attempt to carry out scheduled offenses;" and covers information sent from or received in Pakistan or between Pakistani citizens whether they are resident in the country or not.[94] The bill was proposed by Law Minister Farooq Hamid Naek to thwart terrorism, but its critics counter that the act's wording leaves it open to abuse, and that it grants powers to a broad range of agencies.[95] Under the law, service providers face a one-year jail term or a fine of up to PKR 10 million ($103,000) for failing to cooperate with the warrant.

In 2013, a report by Citizen Lab indicated that Pakistani citizens may be vulnerable to oversight through a software tool present in the country. The "Governmental IT Intrusion and Remote Monitoring Solutions" known as FinFisher Suite described in the report includes the FinSpy tool, which attacks the victim's machine with malware to collect data including Skype audio, key logs, and screenshots.[96] The analysis found FinFisher's command and control servers in 36 countries globally, including Pakistan, on the PTCL network. This does not confirm that actors in Pakistan are knowingly taking advantage of its capabilities. Nevertheless, civil society organizations called on PTCL to investigate and disable FinFisher tools.[97]

Pakistan is also reported to be a long-time customer of Narus,[98] a U.S.-based firm known for designing technology that allows for monitoring of traffic flows and deep-packet inspection of internet communications, and some media reports say Pakistani authorities have also acquired

[91] National Database Registration Authority, "Verification of CNICs: Nadra Signs Contract with Three Cell Phone Companies," July 29, 2009, http://bit.ly/gNdXsW; Bilal Sarwari, "SIM Activation New Procedure," Pak Telecom, September 3, 2010, http://bit.ly/pqCKJ9.
[92] Kelly O'Connell, "INTERNET LAW – Pakistan's Prevention of Electronic Crimes Ordinance, 2007," Internet Business Law Services, April 14, 2008, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2030.
[93] "Senate Passes 'Fair Trial Bill,'" *Dawn*, February 1, 2013, http://dawn.com/2013/02/01/senate-passes-fair-trial-bill/; The Gazette of Pakistan, "Investigation for Fair Trial Act 2013," February 22, 2013, http://bit.ly/18esYjq.
[94] Yasir Rehman, "Fair Trial Act Gives Pakistan Authorities Wiretapping Powers," *Central Asia Online,* December 28, 2012, http://centralasiaonline.com/en_GB/articles/caii/features/pakistan/main/2012/12/28/feature-01.
[95] The laws covers the Inter-Services Intelligence, the police, Intelligence Bureau and the three military intelligence agencies. See, Digital Rights Foundation, "Fair Trial Bill is an Official Intrusion on Privacy: Digital Rights Foundation," December 22, 2012, http://digitalrightsfoundation.pk/fair-trial-act-official-intrusion-on-privacy/
[96] Morgan Marquis-Boire et al, "For Their Eyes Only," Citizen Lab, May 1, 2013, http://bit.ly/ZVVnrb.
[97] Digital Rights Foundation, "Global Coalition Of NGOs Call To Investigate & Disable FinFisher's Espionage Equipment in Pakistan," May 3, 2013, http://bit.ly/18AvwGb.
[98] Timothy Carr, "One U.S. Corporation's Role in Egypt's Brutal Crackdown," *Huffington Post*, January 28, 2011, http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html; "Narus: Security Through Surveillance," Berkman Center for Internet and Society at Harvard University, November 11, 2008, http://hvrd.me/ewSFSg.

surveillance technology from China. In 2013, when news reports described the possible introduction of new filtering software to address the YouTube crisis, some said the information ministry objected to its additional capacities for monitoring communications. PTA chief Farooq Ahmed Khan denied any intent to use it for surveillance.[99]

Pakistan is one of the world's most dangerous countries for traditional journalists, with seven killed in 2012 alone, either on the job or in reprisal for published reports.[100] Violence has yet to affect online journalists in the same way, though they are equally vulnerable to some attacks, such as double-bombings that target first responders at the scene of one blast with a second, delayed detonation. In January 2013, twin blasts hit a Shia Muslim community in Quetta, the provincial capital of Balochistan, killing over 100 people, including three media professionals and Irfan Ali, a blogger and human rights activist who was helping survivors at the scene.[101]

In a particularly high-profile case, an unknown gunman shot 15-year-old Malala Yousufzai in the head while she was traveling in a school van in the Taliban-controlled Swat region of Pakistan in October 2012; she had received threats for writing an online diary for the BBC in 2009.[102] Though she used a pseudonym, the diary included personal details about her family; she also appeared in an online video series for *The New York Times,*[103] among other local media appearances, and became an informal spokesperson promoting education for women, which the Taliban had recently banned. The Pakistani Taliban claimed responsibility for the shooting, saying she had "divulged secrets of the mujahideen and Taliban through BBC [sic]."[104] Yousufzai survived the shooting and was flown to the United Kingdom where she was treated for a severe head wound.

Pakistan was shocked by the attack, and social media played a significant role in driving public debate over the case,[105] which criticized military and intelligence leaders for failing to check the Taliban,[106] and prompted a retaliatory online smear campaign accusing Yousufzai of being a U.S. spy.[107] Local journalists reported Taliban spokesmen contacting them by e-mail and text to defend the action and warn against negative coverage.[108]

Several other free expression activists and bloggers have also reported receiving death threats. Many publicize them—and sometimes attract more—on Twitter. Most are sent via text message from untraceable, unregistered mobile phone connections, often originating from the tribal areas of the country, and several include specific details from the recipient's social media profiles or other

[99] "PTA and MoIT has No Set Plan of Action over the Internet Censorship," *Green and White* (blog), January 10, 2013, http://bit.ly/10nnhOt; Anwer Abbas, "PTA, IT Ministry at odds."
[100] Committee to Protect Journalists, "Journalists Killed in Pakistan," accessed February 2013, http://bit.ly/9YP7fx.
[101] Michael Ross, "Pakistani Activist Killed in Quetta Attacks," The World, PRI, January 11, 2013, http://bit.ly/ZDXGeY.
[102] "Diary of a Pakistani School Girl," BBC News, February 9, 2009, http://news.bbc.co.uk/2/hi/south_asia/7889120.stm.
[103] Adam B. Ellick, "Class Dismissed: Malala's Story," *New York Times*, October 9, 2012, http://nyti.ms/Tf3CaH.
[104] Marie Brenner, "The Target," *Vanity Fair*, April 2013, http://vnty.fr/109Ff7x.
[105] "Pakistan Media Condemn Attack on Malala Yousafzai," BBC News, October 9, 2012, http://bbc.in/VL9AGh.
[106] Talat Farooq, "Malala is a Mirror," *The News International*, October 17, 2012, http://bit.ly/Xlj3CE.
[107] Electron Libre, "Pakistan: Smear Campaign Against Malala on Social Media," France 24, October 18, 2012, http://www.france24.com/en/20121017-2012-10-17-2050-wb-en-webnews.
[108] Sumit Galhotra and Bob Dietz, "After Malala Shooting, Taliban Goes After Media Critics," *CPJ Blog*, October 17, 2012, http://www.cpj.org/blog/2012/10/after-malala-shooting-taliban-goes-after-media-cri.php.

online activity. In addition, some militant Islamic groups in Khyber Pakhtunkhwa and FATA attack cybercafés, which they consider sites of moral degradation. In January 2012, an explosion outside an internet cafe in Peshawar, provincial capital of Khyber Pakhtunkhwa, killed two people;[109] at least three more attacks on cybercafés or mobile phone stores were reported in different areas of the country in the first half of 2013.[110]

Technical attacks against the websites of NGO's, opposition groups, and activists are common in Pakistan but typically go unreported due to self-censorship. Minority organizations such as the Catholic-run human rights advocacy group National Commission for Justice and Peace have also been subject to technical attacks. The websites of government agencies are also commonly attacked, often by ideological hackers attempting to make a political statement. In March 2013, an unidentified hacker defaced the electoral commission's website in advance of elections.[111] Hackers defaced websites belonging to the Supreme Court and the PTA in October 2011 demanding stricter controls for online pornography.[112] Hackers have also infiltrated Pakistan's internet registry PKNIC, which manages the country's top level domains, including major news websites and Microsoft and Google regional homepages. The first attack came on November 24, 2012 and resulted in several sites being defaced, including Google's search engine, which was replaced with an image of penguins and a Turkish-language message reading "Pakistan Downed."[113] The PKNIC failed to adjust its security and was infiltrated again on February 4, 2013, apparently to highlight ongoing vulnerabilities.[114]

[109] "Bomb Blasts in Pakistan Kill Six, Wound 29," UPI, January 3, 2012, http://bit.ly/vNBddl.
[110] "Blast in Nowshera Destroys Internet Cafe, Music Store," *Dawn*, February 2, 2013, http://bit.ly/X1XVk8; "Fresh Bomb Attacks Kill 2 Shias, Wound 20 in Pakistan," Press TV, January 13, 2013, http://bit.ly/Ssoth2; Police: Bomb Blast at Mall in Northwestern Pakistan Kills 1 Person, Wounds 12," The Associated Press via Fox News, February 21, 2013, http://fxn.ws/YI5QCq.
[111] Hisham Almiraat, "Cyber Attack on Pakistan's Electoral Commission Website," *Global Voices Advocacy*, April 1, 2013, http://advocacy.globalvoicesonline.org/2013/04/01/cyber-attack-on-pakistans-electoral-commission-website/.
[112] Shaheryar Popalzai, "Compromised: Official Website of the SC Hacked," *Express Tribune*, September 27, 2011, http://tribune.com.pk/story/261497/hacker-defaces-supreme-court-website/; Jahanzaib Haque, "Ban Porn or Else: Hacker Penetrates PTA Site," *Express Tribune*, October 10, 2011, http://bit.ly/pLS7cC.
[113] "Cyber Vandalism: Hackers Deface Google Pakistan," *Express Tribune*, November 25, 2012, http://bit.ly/SlFhlE.
[114] "Pakistani Hackers Expose PKNIC Vulnerabilities that Caused Defacements of .PK Domains," *Pro Pakistani*, November 26, 2012, http://propakistani.pk/2012/11/26/pakistani-hackers-expose-pknic-vulnerabilities-defacements-of-pk-domains/.

THE PHILIPPINES

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	10	10
Limits on Content (0-35)	5	5
Violations of User Rights (0-40)	8	10
Total (0-100)	23	25

* 0=most free, 100=least free

POPULATION: 96 million
INTERNET PENETRATION 2012: 36 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The Cybercrime Prevention Act of 2012, currently suspended by the Supreme Court, would allow authorities to block online content without a warrant, facilitate government surveillance, and punish online libel with up to 12 years' imprisonment (see **LIMITS ON CONTENT** and **VIOLATIONS OF USER RIGHTS**);
- Civil society activism fuelled 15 petitions to the Supreme Court to suspend the new Cybercrime law; its status going forward is unclear (see **LIMITS ON CONTENT**).
- As of March 2013, there were eight proposed bills in the Senate calling for regulation of online child pornography, gambling, and phishing, which could add to overbroad restrictions on cybercrime (see **LIMITS ON CONTENT**).

INTRODUCTION

People in the Philippines enjoy nearly unrestricted access to the internet. There have not been any reports of the government systematically blocking access to online content. This excellent record was marred in September 2012 by the passage of an anti-cybercrime law boosting official powers to censor and monitor internet users without judicial oversight.

The Philippines first connected to the internet almost twenty years ago via the Philippine Internet Foundation, but experienced very low penetration until the government deregulated the industry in the 1990s, allowing new players to compete with the dominant Philippine Long Distance Telephone Company (PLDT). Recent mergers and acquisitions, however, mean PLDT controls 70 percent of the market and still lacks the kind of competition that would spur it to innovate or become more efficient for the end user. In addition to this the de facto monopoly, lack of infrastructure and bureaucratic government regulation continue to slow penetration. Mobile phone use is more widespread, though this has yet to result in higher mobile internet use.

During the coverage period for this report, the senate approved the notorious Cybercrime Prevention Act, which President Benigno Aquino Jr. signed into law in September. Civil society groups and lawyers immediately petitioned the Supreme Court to issue a restraining order against it, particularly provisions that allow the government to block content without a court order, monitor online activities with the help of service providers, and classify libel—already criminalized under the penal code to the detriment of free expression—as a cybercrime punishable by harsher jail terms than the same offence committed offline. The court, under newly-appointed Chief Justice Maria Sereno, suspended the law's implementation indefinitely on grounds that it may be unconstitutional. Sereno's predecessor was unseated in an impeachment trial related to corruption allegations in May 2012.

This suspension, while positive, left the status of the law ambiguous, and drew attention to its creators' intent in ways that are already chilling online expression. In oral arguments defending it, a government lawyer warned that "liking" a defamatory Facebook post is tantamount to committing libel. A libel complaint over a YouTube video is pending, since the investigation cannot continue until the status of the law is clarified. Meanwhile, the Philippine National Police formed an Anti-Cybercrime Group based on one of the act's provisions in early 2013; it is unclear how the law's suspension will affect the group's activities.

OBSTACLES TO ACCESS

Internet penetration in the Philippines stood at 36 percent in 2012.[1] Usage is concentrated in urban areas, with rural areas largely underserved.[2] A significant number of users still rely on dial-up connections, as just two percent of the population had fixed broadband subscriptions in 2012.[3]

Mobile phone subscriptions, on the other hand, have increased significantly in recent years, with penetration reaching 107 percent in 2012, indicating that some users have more than one device.[4] SMS has been hugely popular for 2G cell phone users since the mid-2000s. Penetration of 3G devices enabling internet access remained comparatively low, at 11 percent, at the end of 2012.[5] In the first quarter of 2013, leading mobile service providers Globe Telecommunications and PLDT wireless subsidiary Smart Communications began expanding 4G LTE coverage outside the metropolitan area surrounding the capital, Manila.[6] Smart was also reportedly testing to improve mobile data speeds.[7]

The government does not place any known restrictions on internet connectivity. Indeed, bridging the digital divide through development of ICT infrastructure is one of the goals of the government's Philippine Digital Strategy for 2011 to 2016. As a result, it is now testing TV White Space technologies—which tap previously unused frequencies and overcome physical obstacles like concrete or dense foliage—to increase connectivity in poor rural areas.[8] However, steep broadband subscription fees still stand in the way of higher penetration in a country where 42 percent of the population lives on US$2 a day.[9] In 2013, even as legislators urged telecoms to cut rates by 50 percent in order to promote universal access,[10] the average cost of broadband subscriptions remained between $7 and $19 a month.[11]

An industry monopoly has contributed to these inflated costs. In the 1990s, government legislation allowed competitors a foothold in the market, previously dominated by the PLDT, a company that

---

[1] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[2] Tam Noda, "Phl to Test TV White Space Technology in Rural Areas," February 1, 2013, *Philippine Star*, http://www.philstar.com/nation/2013/02/01/903696/phl-test-tv-white-space-technology-rural-areas.
[3] International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2012."
[4] International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2012."
[5] Mary Meeker and Liang Wu, "2012 Internet Trends," Kleiner Perkins Caufield and Byers, http://kpcb.com/insights/2012-internet-trends-update.
[6] Marlon C. Magtira, "Globe, Smart Activate New LTE Sites," February 20, 2013, *Manila Standard Today*, http://manilastandardtoday.com/2013/02/20/globe-smart-activate-new-lte-sites/.
[7] "Philippines Network Tests Huawei Supplied TDD-LTE Infrastructure," *Cellular-News,* March 21, 2013, http://www.cellular-news.com/story/59148.php.
[8] Tam Noda, "Phl to Test TV White Space Technology in Rural Areas."
[9] Oxford Poverty and Human Development Initiative, "Philippines Country Briefing," Multidimensional Poverty Index Data Bank, (University of Oxford, 2013) http://www.ophi.org.uk/wp-content/uploads/Philippines-2013.pdf?cda6c1.
[10] Newsbytes.ph, "79% of Philippines Homes no Internet, Telcos Urged to Cut Rates," January 21, 2013, *Digital News Asia*, http://www.digitalnewsasia.com/digital-economy/79percent-of-philippines-homes-no-net-access-telcos-urged-to-lower-rates
[11] Based on current rates published by the three biggest providers: Sun Broadband (owned by Digitel and acquired by PLDT in October 2011), PLDT, and Globe Telecom as of March, 2013.

had been US-owned and Philippine government-owned before its current incarnation as a private entity.[12] However, in the absence of antitrust laws to promote healthy competition between businesses, the PLDT has retained its dominance though a series of mergers and acquisitions. After acquiring majority shares in rival Digitel Telecommunications in 2011, it now controls 70 percent of the country's ICT sector.[13]

Although the industry appears to have diversified, some of these changes are superficial: The most recent government statistics reported 304 registered internet service providers (ISPs) as of 2010,[14] yet most connect to the international internet through the PLDT. The company still owns the majority of fixed-line connections—and consequently the most stable backbone—as well as the 10,000-kilometer domestic fiber optic network that connects to several international networks. It also owns or manages several international cable landings,[15] and offers the highest total bandwidth capacity of 250 Gbps.[16]

By the end of 2012, the only remaining challenger to PLDT's Smart was Globe Telecommunications, which purchased debts amounting to billions of Philippine pesos from struggling competitor Bayan Telecommunications in 2013 with a view to acquiring the company.[17] The rivalry has not resulted in the kind of competition which reduces costs and increases efficiency for the end user. Instead, Smart and Globe have been mired in negotiations over interconnecting their networks for several years, which has also delayed the development of broadband services in many areas.[18] Interconnection allows customers to communicate with users on rival networks without incurring extra costs.

Companies entering the market go through a two-stage process. First, they must obtain a congressional license that involves parliamentary hearings and the approval of both the upper and lower houses. Second, they need to apply for certification from the National Telecommunications Commission, which has regulated the industry with quasi-judicial powers and developed tariff and technical regulations, licensing conditions, and competition and interconnection requirements since its creation in 1979. The constitution limits foreign entities to only 40 percent ownership of a business to be established in the country. Internet service is currently classified as a value-added service and is therefore subject to fewer regulatory requirements than mobile and fixed phone services.

---

[12] Mary Ann Ll. Reyes, "PLDT: From Voice to Multi-Media (First of Two Parts), *Philippine Star,* http://www.philstar.com/business-usual/2012/10/22/859665/pldt-voice-multi-media-first-two-parts.

[13] Winston Castelo, "Controversy on PLDT-Digitel Merger," The Official Website of Congressman Winston "WINNIE" Castelo, November 22, 2011, http://www.winniecastelo.net/controversy-on-pldt-digitel-merger/.

[14] National Statistics Office, "Philippines in Figures 2012," Republic of the Philippines, accessed July 2013, http://www.census.gov.ph/old/data/publications/pif2012_in_CD.pdf.

[15] Erwin A. Alampay, "ICT Sector Performance Review for Philippines," in *Sector Performance Review (SPR)/Telecom Regulatory Environment (TRE) (*LIRNEasia, 2011).

[16] Darwin G. Amojelar, "PLDT says Internet Bandwidth Capacity Up More than Half with Asia Submarine Cable Project," *InterAksyon,* February 22, 2013, http://bit.ly/1bmgY0r.

[17] "Globe Used 'Excess Funds' to Buy Bayan Debt – CFO", January 7, 2013, *Rappler*, http://www.rappler.com/business/19281-globe-used-%E2%80%98excess-funds%E2%80%99-to-buy-bayan-debt-cfo.

[18] Aya Lowe, "NTC to Intervene in PLDT-Globe Interconnection Row," March 6, 2013, *Rappler*, http://www.rappler.com/business/23135-ntc-to-intervene-in-pldt-globe-interconnection-row.

Institutions governing the ICT sector are highly bureaucratic, often with ambiguous or overlapping responsibilities which slow the pace of development. Successive government administrations have modified the structure of official ICT bodies, including President Benigno Aquino. His Executive Order 47 of 2011 established an Information and Communications Technology Office under the Department of Science and Technology (DOST) tasked with conducting research, development, and capacity-building in the ICT industry.[19] However, the division of labor between this office and the Department of Transportation and Communications, which also deals with ICT-related communications, as well as the National Computer Center and the Telecommunications Office, was hard to perceive.

A streamlining process is anticipated. In 2012, Senate Bill No. 50 was passed to create a separate and specialized Department of Information and Communications Technology. The bill is pending before a bicameral conference committee before being transmitted to the president for approval.[20] If authorized, all other ICT-related agencies will be abolished and their powers and personnel transferred to the new department. Some DOST officials challenged the necessity of creating the new department.[21]

All relevant government bodies are headed by presidential appointees. Critics believe this creates a dependence on the incumbent administration and Congress, which determines their budget.[22]

LIMITS ON CONTENT

In the year's most significant development, the 2012 Cybercrime Prevention Act was passed into law in September, threatening to infringe on the Philippines' otherwise open online environment by introducing content restrictions that even a government lawyer admitted are unconstitutional. Under the now-suspended act, the Department of Justice can block online information without a warrant.

While the new anti-cybercrime act remains on hold, there is no systematic government censorship of online content, and internet users in the Philippines enjoy unrestricted access to both domestic and international sources of information. A wide range of Web 2.0 applications, including YouTube, Facebook, Twitter, and international blog-hosting services, are freely accessible. No incidents of politically-motivated website blocking have been reported.[23] The OpenNet Initiative

[19] Executive Order No. 47, June 23, 2011, Official Gazette, http://www.gov.ph/2011/06/23/executive-order-no-47/.
[20] Ricardo Saludo, "Will ICT finally get its own department?," *Manila Times*, April 30, 2012, http://www.manilatimes.net/index.php/opinion/columnist1/21967-will-ict-finally-get-its-own-department.
[21] Patrick Villavicencio, "DOST Withdraws Support for Dept of ICT," August 23, 2012, *InterAksyon*, http://www.interaksyon.com/infotech/dost-withdraws-support-for-dept-of-ict.
[22] Erwin A. Alampay, "ICT Sector Performance Review for Philippines."
[23] Jacques D.M. Gimeno, "Democracy as the Missing Link: Global Rankings of e-Governance in Southeast Asia," in *E-Governance and Civic Engagement: Factors and Determinants of E-Democracy* ed. A. Manoharan and M. Holzer (Hershey, PA: IGI Global, 2012), 561-583.

found no evidence of national filtering,[24] though several organizations reported monitoring and filtering activities in the workplace.[25]

The Cybercrime Prevention Act, signed into law on September 12, 2012, allows the Department of Justice to "restrict or block" content without a court order, including some overly-broad categories like "cybersex," which fails to differentiate between consensual and illegal acts.[26] The law's most troubling provisions introduce punitive jail terms for online libel, outlined in Violations of User Rights.

The reaction to the passing of this punitive piece of legislation was encouraging, if full of apparent contradictions. Before it took effect, the act's own sponsor, Senator Edgardo Angara, stated that he would amend it to require a court order in support of content restrictions: "I'm trying to trace in the record who introduced this kind of provision," he told local journalists.[27] Activists moved quickly to prevent the act's implementation, and different groups and stakeholders had filed 15 petitions with the Supreme Court to question its constitutionality by January 2013.[28] In response, the justices issued a 120-day restraining order to prevent the law from being acted upon, which the court extended indefinitely in February 2013; in oral arguments, the government's lawyer acknowledged that the clauses relating to content restrictions were unconstitutional.[29] Meanwhile, Senator Miriam Defensor Santiago filed a rival bill with congress that, if passed, would repeal the act.[30] Santiago told journalists her Magna Carta for Philippine Internet Freedom bill "provides for court proceedings in cases where websites or networks are to be taken down and prohibits censorship of content without a court order."[31] It is not clear how much support Santiago's bill may attract, and passing a bill in the Philippines can take months or even years.

As of March 2013, there are eight other proposed bills in the Senate calling for regulation of online content pertaining to child pornography, gambling, and phishing, some of which would require ISPs, web hosting services and educational institutions to monitor users and disable access to banned content. The Anti-Child Pornography Act of 2009 also requires ISPs to install unspecified "available technology, program or software" to filter content prohibited by the act.[32]

---

[24] OpenNet Initiative, "Internet Filtering in Asia," 2009, http://opennet.net/research/regions/asia.
[25] Erwin A. Alampay and Regina Hechanova, "Monitoring Employee Use of Internet: Employers' Perspective," *Inquirer*, January 24, 2010, http://business.inquirer.net/money/topstories/view/20100124-249272/Monitoring-employee-use-of-Internet-Employers-perspective.
[26] "Republic Act 10175," Official Gazette, September 12, 2012, http://www.gov.ph/2012/09/12/republic-act-no-10175/.
[27] "Author of Cybercrime Law to File Bill Amending It," *Rappler*, October 3, 2012, http://www.rappler.com/nation/13545-author-of-cybcerime-law-to-file-bill-amending-it.
[28] Mark D. Merueñas, "SC Junks 16th Petition vs. Cybercrime Law," January 24, 2013, http://www.gmanetwork.com/news/story/291825/scitech/technology/sc-junks-16th-petition-vs-cybercrime-law.
[29] Edu Punay, "SC Extends TRO on Cyber Law," *Philippine Star*, February 6, 2013, http://www.philstar.com/headlines/2013/02/06/905368/sc-extends-tro-cyber-law.
[30] "Senate Bill No. 3327," Senate of the Philippines, accessed July, 2013, http://www.senate.gov.ph/lisdata/1446312119!.pdf.
[31] Norman Bordadora, "Santiago Proposes Magna Carta for Internet," *Inquirer*, December 1, 2012, http://technology.inquirer.net/20769/santiago-proposes-magna-carta-for-internet#ixzz2RJNaXMVZ.
[32] "Republic Act No. 9775," November 17, 2009, The LawPhil Project, http://www.lawphil.net/statutes/repacts/ra2009/ra_9775_2009.html.

There have been no reports of officials putting pressure on online journalists or bloggers to delete content when it is critical of the authorities. However, many news websites are online versions of traditional media which self-censor due to the level of violence against journalists in the Philippines. While it is fair to surmise that the same attitude is reflected in their online output, the degree is difficult to establish. Notably, however, one of the Senate's main proponents of the libel clause in the Anti-Cybercrime Act argued that it would instill self-censorship in internet users—the actual phrase was "think before you click," according to local blogger Raïssa Robles.[33]

More generally, the Philippine blogosphere is rich and thriving. Both state and non-state actors actively use the internet as a platform to discuss politics, especially during elections. Online protests against the Cybercrime Prevention Act were common for several months before and after the law was passed, with individuals blacking out their profile pictures on social networks. Many dubbed it Cyber Martial Law after the era of military rule in the 1970s when freedom of expression was seriously threatened.[34] While encouraging, these protests can only be called successful inasmuch as they spurred the filing of the 15 petitions with the Supreme Court, which are to be credited with ultimately suspending the law's implementation.

VIOLATIONS OF USER RIGHTS

The Cybercrime Prevention Act, which passed in 2012 after more than a decade of deliberations,[35] uncritically adopted archaic libel provisions from the penal code—long challenged by local and international human rights groups[36]—and increased the minimum penalty for online violations from six months to a staggering six years in jail, apparently at the last minute and without public discussion.[37] Other provisions require service providers to cooperate with law enforcement in monitoring users suspected of cybercrime, and potentially allow police to monitor online traffic in real time. Despite the Supreme Court's restraining order on the law's implementation, it has already created a chilling effect among internet users. Violence against traditional journalists exerts a negative effect on freedom of expression in the Philippines, but as of 2013, had relatively little impact on online communication.[38]

[33] Raïssa Robles, "Who Inserted that Libel Clause in the Cybercrime Law at the Last Minute?," *RaissaRobles*, September 18, 2012, http://raissarobles.com/2012/09/18/who-inserted-that-libel-clause-in-the-cybercrime-law-at-the-last-minute/.
[34] T.J.D., "Protests Versus Cybercrime Law Rage on Multiple Fronts," October 2, 2012, *GMA News*, http://www.gmanetwork.com/news/story/276448/scitech/technology/protests-vs-cybercrime-law-rage-on-multiple-fronts.
[35] "The Road to the Cybercrime Prevention Act of 2012," *Rappler,* October 9, 2012, http://www.rappler.com/rich-media/13901-the-road-to-the-cybercrime-prevention-act-of-2012.
[36] Human Rights Watch, "Philippines: New 'Cybercrime' Law Will Harm Free Speech," September 28, 2012, http://www.hrw.org/news/2012/09/28/philippines-new-cybercrime-law-will-harm-free-speech.
[37] Jillian C. York, "Philippines' New Cybercrime Prevention Act Troubling for Free Expression," Electronic Freedom Foundation, September 18, 2012, https://www.eff.org/deeplinks/2012/09/philippines-new-cybercrime-prevention-act-troubling-free-expression.
[38] Article 19, "Philippines: ARTICLE 19's Submission to the UN Universal Periodic Review," November 29, 2011, http://www.article19.org/resources.php/resource/2879/en/philippines:-article-19%27s-submission-to-the-un-universal-periodic-review.

The Bill of Rights of the 1987 Constitution protects freedom of expression (Section 4) and privacy of communication (Section 1).[39] However, some laws undermine those protections. Libel is punishable by fines and imprisonment under the Revised Penal Code. This has historically been challenging to prove in online cases which lack a physical place of publication—one of the requirements for an offline prosecution—and in 2007, a Department of Justice resolution established that Articles 353 and 360 of the Revised Penal Code covering libel do not apply to statements posted on websites.[40] This may have discouraged, but did not stop, attempts to prosecute online libel. In 2011, a doctor filed a complaint over an allegedly defamatory statement about him posted in the comments section of their website. In January 2013, the prosecutor dismissed the complaint against the website staffers on the basis that they are not responsible for content they neither edited nor approved. However, charges are still pending against the third respondent who left the comment.[41]

The 2012 cybercrime law not only adopted the penal code's definition of libel, but further classified it as a cybercrime punishable by six to twelve years in prison or a fine determined by the Department of Justice. The identical offense perpetrated offline carries a lesser sentence of six months to four years and two months imprisonment under the Revised Penal Code.[42] A government lawyer warned that liking or sharing a libelous post on Facebook or Twitter could result in imprisonment.[43] Others pointed out that the law could imprison the living for libeling the dead, and that the author of alleged libel could be sued for something written years before the law was passed if the content is still available online.[44] One lawyer reposted content that had sparked a libel suit against him in 2010 to his Facebook page in an attempt to create the kind of judicial controversy that would spur the Supreme Court to intervene over the law.[45]

While the legal challenges to the law have left its future in doubt, a private citizen used it to sue a neighbor for uploading a video to YouTube under an allegedly libelous title in October 2012; the preliminary investigation into the complaint was suspended due to the restraining order issued by

[39] "1987 Philippine Constitution, Article III, Bill of Rights," via Asian Human Rights Commission, accessed July 2013, http://philippines.ahrchk.net/news/mainfile.php/leg_sel/15/.

[40] Department of Justice, Resolution No. 05-1-11895 on Malayan Insurance vs. Philip Piccio, et al., June 20, 2007. Article 353 states that, "libel is committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means." The Department also stated that the accused are not culpable because they cannot be considered as authors, editors, or publishers as provided for in Article 360. Critics have further noted that the Revised Penal Code, which dates from 1932, long predates digital technology, and therefore shouldn't be applied to digital content.

[41] Rene Acosta, "Prosecutor Drops Libel Complaint vs TV Network," January 6, 2013, *Business Mirror*, http://www.businessmirror.com.ph/index.php/news/nation/7273-prosecutor-drops-libel-complaint-vs-tv-network

[42] Purple Romero, "DOJ Holds Dialogue on 'E-Martial Law'," October 9, 2012, Rappler, http://www.rappler.com/nation/13837-it-s-not-e-martial-law.

[43] "SolGen: Netizens Spreading 'Libelous' Posts Criminally Liable," January 29, 2013, *SunStar,* http://www.sunstar.com.ph/breaking-news/2013/01/29/solgen-netizens-spreading-libelous-posts-criminally-liable-265420.

[44] "Digital Martial Law: 10 Scary Things About the Cybercrime Prevention Act of 2012," *Spot*, October 2, 2012, http://www.spot.ph/newsfeatures/52041/digital-martial-law-10-scary-things-about-the-cybercrime-prevention-act-of-2012/1#sthash.4vVhXXNS.dpuf.

[45] Mark Merueñas, "Lawyer Wants Test Case on Cybercrime Law," *GMA News*, October 3, 2012, http://www.gmanetwork.com/news/story/276548/news/nation/lawyer-wants-test-case-on-cybercrime-law.

the Supreme Court against the cybercrime law.[46] Another prominent case did not involve a criminal prosecution. In 2012, a group of nurses said their hospital had fired them for 'liking' a Facebook post criticizing the management.[47] Though the state-run hospital denied Facebook was a factor in the termination, the case evoked the same fear—of authorities taking arbitrary action over ICT content—as the anti-cybercrime law itself.

The cybercrime act would also facilitate government surveillance of online communication, allowing the authorities to monitor online activities, and requiring service providers to assist the government in collecting and storing user data pertaining to acts classified as cybercrimes, including spam and file-sharing.[48] The extent to which they already conduct surveillance is not clear. The government acted on Section 10 of the law to create an anti-cybercrime group within the Philippine police force in March 2013.[49] It is not known whether the team has begun collecting real-time traffic data based on the law's contested section 12.[50]

A Data Privacy Act introduced into law on August 15, 2012 establishes parameters for the collection of personal information and an independent privacy regulator, but only pertaining to data voluntarily provided in private or official transactions, such as credit card information or social security details.[51] While many clauses are ICT-specific, requiring those who control information online to take steps such as assessing reasonably foreseeable vulnerabilities in computer networks, it does not redress the provisions in the Cybercrime Prevention Act that would allow monitoring or collection of personal data in criminal cases with neither the user nor the court's consent.[52]

Other laws with privacy implications include the Anti-Child Pornography Act of 2009 which explicitly states that its section on ISPs may not be "construed to require an ISP to engage in the monitoring of any user,"[53] though it does require them to "obtain" and "preserve" evidence of violations, and threatens to revoke their license for non-compliance; section 12 of the law also authorizes local government units to monitor and regulate commercial establishments that provide internet services. Under the Human Security Act of 2007, law enforcement officials must obtain a

[46] Tricia Aquino, "Cebu Resident Subpoenaed Over 'Cyber-Libelous' YouTube Post", October 27, 2012, *InterAksyon*, http://www.interaksyon.com/article/46643/cebu-resident-subpoenaed-over-cyber-libelous-youtube-post.
[47] Matika Santos, "Audio Recording Bares Nurses Fired Over Facebook 'Like' on Critical Status Update," *Inquirer*, October 10, 2012, http://technology.inquirer.net/18744/audio-recording-bares-nurses-fired-over-facebook-like-on-critical-status-update.
[48] Paul Tassi, "The Philippines Passes a Cybercrime Prevention Act that Makes SOPA Look Reasonable," *Forbes,* October 2, 2012, http://www.forbes.com/sites/insertcoin/2012/10/02/the-philippines-passes-the-cybercrime-prevention-act-that-makes-sopa-look-reasonable/.
[49] Official Homepage of the Philippine National Police, "PNP Activates Anti-Cybercrime Group," press release, March 21, 2013, http://pnp.gov.ph/portal/press-news-releases/latest-news/969-pnp-activates-anti-cybercrime-group.
[50] Tetch Torres, "Gov't Admits Cyberlaw Barely Constitutional," January 29, 2013, *Inquirer*, http://newsinfo.inquirer.net/349173/govt-admits-cyber-law-barely-constitutional.
[51] "Republic Act No. 10173," Official Gazette, August 15, 2012, http://www.gov.ph/2012/08/15/republic-act-no-10173/; Janette Toral, "Salient features of Data Privacy Act of 2012 – Republic Act 10173," *Digital Filipino*, December 17, 2012, http://digitalfilipino.com/salient-features-of-data-privacy-act-of-2012-republic-act-10173/.
[52] Alec Christie and Arthur Cheuk, "Australia: New Tough Privacy Regime in the Philippines Data Privacy Act Signed Into Law," DLA Piper Australia via *Mondaq*, October 27, 2012, http://www.mondaq.com/australia/x/203136/Data+Protection+Privacy/privacy+law+Philippines.
[53] "Implementing Rules and Regulations of the Anti-Child Pornography Act of 2009," via University of Minnesota Human Rights Library, accessed July 2013, http://www1.umn.edu/humanrts/research/Philippines/IRR%20%20of%20the%20Anti%20Child%20Pornography%20Act.pdf.

court order to intercept communications or conduct surveillance activities against individuals or organizations suspected of terrorist activity.[54] To date, no abuse of this law has been reported. Other bills pending in Congress as of March 2013 would potentially add to privacy concerns by requiring ISPs, web-hosts, and educational institutions to monitor users trying to access child pornography, gambling sites, or performing illegal hacking.[55]

Violence against journalists is a significant problem in the Philippines. As of April 30, 2013, the Committee to Protect Journalists reported at least 73 Philippine journalists had been killed in relation to their work—most covering political beats—since the organization started compiling records in 1992.[56] Not one of these murders has been fully prosecuted—meaning that everyone responsible for both ordering and executing the killing have been tried and convicted—creating an entrenched culture of impunity that sends the message that individuals exercising free speech can be attacked at will. This trend has yet to make itself felt among internet users: There have been no prominent cases reported of attacks on bloggers for online expression, though some fear that may change as internet penetration grows and more people turn to web-based news sources.

There are no restrictions on anonymous communication in the Philippines. The government does not require the registration of user information prior to logging online or subscribing to internet and mobile phone services, especially since prepaid services are widely available, even in small neighborhood stores.

There have been no reports of politically-motivated incidents of technical violence or cyberattacks perpetrated by the government towards private individuals. However, in October 2012, the Philippine chapter of the group Anonymous perpetrated a series of cyberattacks against government- and privately-owned websites.[57]

[54] "Republic Act 9372 – Human Security Act of 2011 (full text)," Philippine e-Legal Forum, July 10, 2007, http://jlp-law.com/blog/ra-9327-human-security-act-of-2007-full-text/

[55] For example, "SBN-1710: Safer Net Act," Senate of the Philippines, accessed July, 2013, http://www.senate.gov.ph/lis/bill_res.aspx?congress=15&q=SBN-1710.

[56] The organization documented an additional 37 journalist murders in which the motive was not confirmed. Committee to Protect Journalists, "73 Journalists Murdered in Philippines since 1992," accessed May 2013, http://cpj.org/killed/asia/philippines/.

[57] Camille Diola, "'Anonymous Philippines' Hacks Gov't Websites Anew," *Philippine Star,* January 15, 2013, http://www.philstar.com/cybercrime-law/2013/1/15/897221/anonymous-philippines-hacks-gov-t-websites-anew.

RUSSIA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	11	10
Limits on Content (0-35)	18	19
Violations of User Rights (0-40)	23	25
Total (0-100)	**52**	**54**

* 0=most free, 100=least free

POPULATION: 143.2 million
INTERNET PENETRATION 2012: 53 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The number of websites classified as extremist material and blocked by the Ministry of Justice increased approximately 60 percent from January 2012 to February 2013 (see **LIMITS ON CONTENT**).
- In July 2012, the State Duma passed Federal Law #139-FZ which allows the government to create a list of websites that ISPs must block without any mechanism for judicial oversight. This law is intended to restrict access to sites with illegal content, such as child pornography, drug-related material, or extremist content; however, sites with legitimate content have also been blocked under this law (see **LIMITS ON CONTENT**).
- Internet use continued to be a significant tool for mobilization and communication among civil society and opposition groups (see **LIMITS ON CONTENT**).
- In July 2012, the Russian criminal code was amended to recriminalize defamation in traditional and online media (see **VIOLATIONS OF USER RIGHTS**).
- Cases of criminal prosecution for online activities increased from 38 in 2011 to 103 in 2012 (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Since Vladimir Putin's return to the presidency in May 2012, issues related to internet freedom in Russia have continued to move toward the forefront of social and political concerns. Activists demonstrated the internet's wide-ranging potential for political mobilization and, in so doing, have attracted the close attention of the authorities. Increasingly, the internet is regarded by the Russian state as a realm that requires tighter regulation and restrictions.[1]

The number of active online users continues to grow, particularly in small towns and among older generations.[2] There was a notable increase in the number of websites on the three Russian top-level domains (.ru, .su and .рф), and by the end of 2012, a total of 5,156,504 domain names were registered by 25 accredited registrars.[3] At the same time, many website owners have begun to choose foreign jurisdictions to host their sites; last year showed a rapid growth in Russian demand for renting server equipment outside of the country.[4]

In July 2012, the government passed Federal Law #139-FZ, which allows for the creation of a "blacklist" of websites that internet service providers (ISPs) within Russia are required to block. The law is intended to block access to illegal or otherwise harmful material on the internet, such as child pornography, material related to drug abuse, and so forth. However, there is no judicial approval required to place a website on the blacklist, and many websites with legitimate content have also been blocked in the process. Critics warn that the law is difficult to implement without negatively impacting otherwise legal online activities, and that it could be used to directly censor online content.

The number of legal restrictions against online users also increased over the past year, including an increase in the number of criminal prosecutions against online users, and the recriminalization of defamation through legislation passed by the State Duma. Moreover, well-known bloggers like Aleksei Navalny and Rustem Adagamov,[5] as well as regular users and activists, were subjected to harassment and prosecution. For the first time, internet activists began to flee Russia, seeking asylum in other countries.[6]

---

[1] Elena Milashina, "Russia steps up crackdown on rights groups, Internet," Committee to Protect Journalists, March 26, 2013, http://www.cpj.org/blog/2013/03/russia-steps-up-crackdown-on-rights-groups-interne.php#more.
[2] Anastasia Golitsyna, "Google ускоряет шаг" [Google Speeds Up], Vedomosti.ru, January 29, 2013, http://www.vedomosti.ru/newspaper/article/383941/google_uskoryaet_shag.
[3] "Russian Domains" [in Russian], Statdom.ru, accessed July 30, 2013, http://statdom.ru/.
[4] "Russian Customers Fill Up European Data-Centers" [in Russian], accessed July 30, 2013, http://www.deac.lv/?object_id=16936.
[5] Alan Cullison, "Russia Investigates Allegations Against Opposition Blogger," *Wall Street Journal*, January 11, 2013, http://online.wsj.com/article/SB10001424127887324581504578236031175757590.html?KEYWORDS=Russia
[6] "Estonia Grants Political Asylum to Blogger Who Criticised Russian Orthodox Church," Agora Human Rights Association, October 19, 2012, http://agora.rightsinrussia.info/archive/news/efimov/asylum.

OBSTACLES TO ACCESS

The internet penetration rate in Russia has continued to grow over the past few years.[7] In 2012, the internet penetration rate stood at 53 percent, up from 25 percent in 2007, according to the International Telecommunication Union (ITU).[8] Survey data from the Public Opinion Foundation indicates that the estimated number of people who use the internet on a daily basis increased from 44.3 million users (38 percent of the population) at the end of 2011 to 50.1 million users (43 percent of the population) at the end of 2012.[9] During this time period, the greatest growth in internet use occurred in villages and towns with less than 100,000 inhabitants.[10] The mobile phone penetration rate at the end of 2012 was 161 percent, with approximately 230 million mobile phone subscribers among the top seven Russian mobile service providers.[11]

In early 2013, Prime Minister Dmitry Medvedev commissioned the Ministry of Communications and several other government bodies to develop a series of measures by April 1, 2013 that would reduce the cost of broadband internet access for households.[12] The average monthly cost of a broadband connection with a speed of 1 Mbps is $1.80.[13] Currently, however, it costs service providers RUB 12,000 (approximately US$365) to connect one household to a broadband network.[14] This cost may be one of the determining factors in the persisting gap in internet penetration between large cities and rural areas, and among different regions of the country. For instance, the penetration rate in the Northwestern Federal District reached 62 percent in 2012, whereas in the Volga and North Caucasus regions it did not exceed 49 percent.[15] In part, this gap in internet access is counteracted by the explosive growth of mobile internet access. By the end of 2012, there were approximately 22.5 million mobile internet subscribers, an increase of 88 percent from 2011.[16]

Internet access in schools also varies according to region, with many Russian schools still lacking an internet connection. According to a survey conducted by the National Training Foundation, 70

[7] Public Opinion Foundation, "Интернет в России: динамика проникновения. Осень 2012" [Internet in Russia: Dynamics of Penetration. Fall 2012], December 18, 2012, http://runet.fom.ru/Proniknovenie-interneta/10738.
[8] International Telecommunication Union (ITU), "Percentage of individuals using the Internet," 2007 & 2012, accessed July 13, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[9] Public Opinion Foundation, "Internet in Russia. Report highlights," accessed July 30, 2013, http://www.ewdn.com/wp-content/uploads/2013/03/FOM_Internet_Winter_2012_20131.pdf.
[10] Public Opinion Foundation, "Internet Audience: Yesterday, Today, Tomorrow..." [in Russian], November 29, 2012, http://runet.fom.ru/Proniknovenie-interneta/10714.
[11] Advanced Communications & Media, "Cellular Data," accessed July 30, 2013, http://www.acm-consulting.com/data-downloads/cat_view/7-cellular.html.
[12] "Medvedev Commanded to Decrease the cost of Internet access in Russia" [in Russian], RIA Novosti, January 21, 2013, http://ria.ru/economy/20130121/918943794.html.
[13] Maria Petrova, "Broadband Access to the Internet Must Become Cheaper" [in Russian], Comnews.ru, January 22, 2013, http://www.comnews.ru/node/69851.
[14] "В село проведут инновационную сеть," RBC Daily, January 22, 2013, http://www.rbcdaily.ru/media/562949985558334.
[15] "Dynamics of Internet penetration in Federal Districts and settlements" [in Russian], December 18, 2012, http://runet.fom.ru/Proniknovenie-interneta/10738.
[16] "Mobile Internet Market Review. Use of mobile internet through smartphones and tablet PCs," J'son and Partners Consulting Official Website, January 2013, http://bit.ly/15BZjTz.

percent of schools in cities with more than 1 million inhabitants are connected to the internet, whereas in rural areas, less than 45 percent of schools have internet access.[17]

In May 2012, several Russian ISPs (VimpelCom, Megafon, Mobile TeleSystems and the state-controlled company Rostelecom) announced plans to develop an underwater fiber-optic cable connecting towns on the island of Sakhalin to the Far East regions of Kamchatka and Magadan.[18] The project, which would significantly lower prices of internet access on the island, is expected to take about two years to complete.[19] It should be noted, however, that there have been multiple failed attempts to construct an undersea cable to Sakhalin in the past.[20]

There are no specific legal restrictions on ICT connectivity or limitations on social media and communication apps. However, in September 2012, members of the State Duma issued a proposal that would outlaw the use of anonymizers and circumvention tools that enable users to send and receive encrypted data, access blocked websites, or make their online activities less conspicuous.[21] As of May 2013, this proposal had not been acted upon and the use of these tools is still legal, although in August 2013 the FSB director revived this debate by announcing that his agency would begin working with other Russian law enforcement and security bodies to draft such legislation.[22]

The broadband market in Russia is still highly concentrated. State-owned provider Rostelecom controls 39 percent of the broadband market, while the other five main providers (VimpelCom, ER-Telecom, Mobile TeleSystems, TransTelecom, and AKADO) together control approximately 40 percent.[23] The remaining 21 percent of the market is controlled by smaller ISPs. This data reflects the overall market distribution throughout the country; however, competition is much lower in small towns and regions where only a few service providers operate.[24] Similarly, the Russian mobile communications market is dominated by three leading companies—Mobile TeleSystems, VimpelCom, and Megafon—which together control 82 percent of the market.[25]

---

[17] Компьютерная оснащенность школ. РИАН ["Computer equipment in schools"], RIA Novosti, September 11, 2012, http://ria.ru/ratings/20120911/747679545.html.

[18] «Стартовали проектно-изыскательские работы по строительству подводной ВОЛС «Сахалин-Магадан-Камчатка» ["Ctartovali design work for the construction of underwater fiber-optic 'Sakhalin-Magadan-Kamchatka'"], Corporate website of Rostelecom, June 9, 2012, http://www.kamchatka.rt.ru/press/news/news877.

[19] "Russians to link eastern islands by cable," Global Telecom Business, May 16, 2012, http://www.globaltelecomsbusiness.com/article/3029654/Russians-to-link-eastern-islands-by-cable.html.

[20] "The island of Sakhalin is still very far away," *The Economist*, April 5, 2010, http://www.economist.com/blogs/babbage/2010/04/broadband_prices_russia.

[21] Dmitry Runkevich, Депутаты запретят анонимность в сети [The deputies shall ban anonymity on the Net], Izvesita.ru, September 21, 2012, http://izvestia.ru/news/535724.

[22] "Russia's FSB mulls ban on 'Tor' online anonymity network," RT.com, August 16, 2013, http://rt.com/politics/russia-tor-anonymizer-ban-571/.

[23] Advanced Communications & Media, "Russian Residential Broadband Data 2012," accessed July 30, 2013, http://www.acm-consulting.com/data-downloads/cat_view/16-broadband.html.

[24] Интернет в глубинке: обзор стоимости ШПД в небольших городах [Internet in remote places: overview of broadband access cost in small towns], Telecomza.ru, April 17, 2013, http://telekomza.ru/2013/04/17/internet-v-glubinke-obzor-stoimosti-shpd-v-nebolshix-gorodax/.

[25] Advanced Communications & Media, "Cellular Data 2012," accessed July 30, 2013, http://www.acm-consulting.com/data-downloads/cat_view/7-cellular/19-cellular-2012.html.

The ICT and media sector is regulated by the Federal Service for Supervision in the Sphere of Telecom, Information Technologies, and Mass Communications (Roskomnadzor) under the control of the Ministry of Communications and Mass Media and the Government of the Russian Federation. With the new internet blacklist law (Federal Law #139-FZ) going into effect in November 2012, Roskomnadzor now has the authority to determine if a website should be blocked based on whether or not the site contains material that is restricted by the law; these decisions do not require prior court approval. As a result, Roskomnadzor has become a primary player in the field of controlling and filtering information on the internet. Concerning the technical aspects of access to the internet, the regulatory bodies generally operate fairly. However, their efforts to overcome the digital gap and open up the ICT market to greater competition have been insufficient.

LIMITS ON CONTENT

In 2012–2013, the Russian government ramped up its practice of restricting online content through the blocking of websites. In addition to a 60 percent increase in the number of websites placed on the federal list of extremist materials from January 2012 to February 2013, with the enactment of Federal Law #139-FZ in November 2012, the regulatory authority can now place websites deemed "harmful to the health and development of children" on an internal blacklist of sites that ISPs are required to block, without prior decisions or approval by a court.

Blocking access to information on entire websites, IP addresses, and particular webpages has become the most common means in Russia to restrict user activity on the internet. This control over online content expanded after Federal Law #139-FZ was passed on July 28, 2012. Commonly known as "the internet blacklist law," this law, for the first time in Russian history, legalised the blocking of access to websites without requiring a court ruling. Since the law took effect on November 1, 2012, websites on which experts find pornographic images of minors, information about suicide techniques, or information on preparing or taking drugs can be placed on a special register within two days, and access to these sites can be blocked on the basis of a decision by Roskomnadzor. In addition to the material targeted in the legislation, blocked websites have included Ri-online.ru (the website of *Ingushetia Online,* a local news site), a Jehovah's Witnesses site,[26] websites of Caucasian separatists, blogs on LiveJournal, and an analytical article by the public figure and academic Yuri Afanasyev.[27]

During the first four months of the enforcement of Federal Law #139-FZ (November 1, 2012–February 28, 2013), 309 domain names were banned and 197 IP addresses were blocked, causing approximately 4,000 blockings of those resources that shared IP addresses with banned sites.[28] In November 2012, during the first weeks of the implementation of the new law, dozens of websites

[26] "Jehovah's Witnesses website identified as extremist" [in Russian], SecurityLab.ru, June 15, 2012, http://www.securitylab.ru/news/425840.php.
[27] "Register of extremist materials was replenished with an article by Yuri Afanasyev" [in Russian], Agentura.yu, February 19, 2013, http://www.agentura.ru/news/28138.
[28] "The Register Monitoring" [in Russian], February 27, 2013, http://rublacklist.net/4445/#more-4445.

were blocked for seemingly arbitrary reasons. Among those sites were popular resources such as Lurkmore.to (a wiki-based ironic online encyclopedia for internet subcultures), RuTracker.org (a popular torrent tracker), and Lib.rus.ec (an open library).

In the period from July to December 2012, Google reported that there were 114 requests by the Russian authorities to remove content from various Google platforms, compared to 4 requests during the same period in 2011.[29] These included 111 requests issued by police or executive authorities and 3 court orders. Material related to suicide promotion and drug abuse accounted for the majority of the removal requests (56 requests and 51 requests, respectively), followed by 3 cases related to defamation, 3 related to privacy and security, and 1 related to hate speech. In response to these requests, Google removed content for violating their own product policies in more than half of the cases, and restricted content from local view in about one third of the cases.[30]

In September 2012, there were widespread demands from prosecutors' offices and from Roskomnadzor to block access to sites hosting fragments of the "Innocence of Muslims" video. According to Google's Transparency Report, the company decided to restrict in-country access to the video in eight countries, including Russia.[31] However, prior to this restriction, demands from the General Prosecutor went out to ISPs across the country, instructing the service providers to block access to the content prior to any court decisions. Given the varying nature of each request, some ISPs opted to block the entire YouTube platform, rendering it temporarily inaccessible for users in certain regions, while other ISPs also blocked access to the social network Vkontakte for containing pages with links to the video.[32] In each case, the service providers complied with the request before the court identified the video as containing extremist material.

In late 2011, Roskomnadzor announced that it had installed online software to detect "extremist" material. Under the new system, websites flagged by the software are given three days to take down the allegedly offending content. If a site does not comply, two additional warnings are sent followed by a complete shutdown. The test mode version of the software was to begin operating in December 2011, though its full deployment was indefinitely postponed as of mid-2012. The Ministry of Justice, on the other hand, has invited bids to create its own internet monitoring system, apparently for the purposes of examining content related to the Russian government and justice systems, and to any European Union statement concerning Russia.[33]

The practice of identifying online materials as extremist, which was widespread and used to block websites after the adoption of anti-extremist legislation in 2002, expanded in 2012 when dozens of webpages were added to a federal list of extremist materials, operated by the Ministry of Justice.

[29] "Russia," Google Transparency Report 2012, accessed July 30, 2013, http://www.google.com/transparencyreport/removals/government/RU/?hl=en_GB.
[30] Ibid.
[31] "Google Transparency Report: Russia," July-December, 2012, accessed July 30, 2012, http://www.google.com/transparencyreport/removals/government/RU/.
[32] Maria Kravchenko, "Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2012," edited by Alexander Verhovsky, SOVA Center for Information and Analysis, June 26, 2013, http://www.sova-center.ru/en/misuse/reports-analyses/2013/06/d27382/#_Toc357760970.
[33] "2012 Surveillance: Russia," Reporters Without Borders, March 12, 2012, http://bit.ly/VoO1HS.

The federal list contains details of court decisions that identify any online information materials as extremist. As of February 2013, the list included 1,704 items, compared to 1,066 as of January 2012.[34] According to the law, anyone who disseminates these materials, either offline or online, may be administratively or criminally prosecuted and receive a penalty ranging from a fine of RUB 1,000 (approximately $30) to up to 5 years imprisonment, depending upon the legal treatment.

In total, no less than 608 decisions were made during 2012 to block access to websites, either through court judgments or by service providers, compared to 231 decisions in 2011.[35] This number does not include blockings made under the new "blacklist law." At the end of 2012, Roskomnadzor officials reported that 1206 entries were made on the Unified Register at the site Zapret-info.gov.ru, which means either that the information on these sites was deleted or that the website was blocked completely.[36]

At the end of 2011, new rules for the registration of domain names for the domains ".ru" and ".РФ" were adopted by the Coordination Center for TLD RU/РФ.[37] These rules have given registrars the right to terminate the domain name delegation of a website based on a decision in writing by the head of an agency which exercises operational search actions, such as the police, the Federal Security Service, the drug police, or the customs agency. In accordance to these rules, in February 2012 the domain name registrar Masterhost discontinued its delegation of the Andrei Rylkov Foundation for Health and Social Justice's domain—Rylkov-fond.ru—based on a report by the head of the directorate of the Moscow branch of the Federal Service for Drug Control, which stated that "the office received information that the domain [...] contained materials that propagandised (advertised) the use of narcotics." In reality, the foundation's site contained official documents on replacement therapy from the World Health Organisation and the United Nations Office on Drugs and Crime.[38]

Some actions taken by local prosecutors and regional courts regarding the blocking of online content have been questionable. In August 2012, for example, the Perm City Court forced an ISP to block a free listings website, stating that a search for the phrase "buy marijuana in Perm" using the Yandex search engine provided a link to that website. According to a representative from the company that ran the site, an advertisement for a smoking blend had indeed been placed on the site. However, the government bodies had not contacted the site owner, and instead went straight to court. Although the moderator subsequently deleted the advertisement, the ruling to force the service provider to block the site's IP address had already taken legal effect.

---

[34] "Federal list of extremist materials," Ministry of Justice official website, accessed July 30, 2013, http://minjust.ru/ru/extremist-materials?search.

[35] AGORA Association, Доклад: Россия как глобальная угроза свободному Интернету [Report: Russia - a global threat to Internet freedom], http://eliberator.ru/news/detail.php?ID=21.

[36] Twitter account of the Head of Russian Association for Electronic Communications (RAEC) Sergey Plugotarenko [in Russian], December 21, 2012, https://twitter.com/plugotarenko/status/282014753851854848/photo/1.

[37] "The Terms and Conditions of Domain Names Registration in domains .RU and .РФ," The Coordination Center for TLD RU, accessed July 30, 2013, http://cctld.ru/en/docs/rules.php.

[38] "Rules Governing Registration of Domain Names Allow Law Enforcement to Arbitrarily Block Websites," Agora Human Rights Association, February 7, 2012, http://agora.rightsinrussia.info/archive/news/domains/andrei-rylkov.

In October 2012, the Prosecutor's Office in the Orel region demanded that the court ban the website Orlec.ru, a local "free encyclopedia," based on the claim that the website hosted extremist material. The reason stated by the prosecutor—that the material "undermined the public image of local self-governments and the [Russian Federation] authorities in general"—indicates the political nature of the request.[39] Additionally, there were questions as to whether the material was actually planted on the website for the purpose of such an investigation. In the end, the court ruled that the particular material, which had already been removed, was extremist, but that the website itself was not.

The practice of putting pressure on service providers and content producers by telephone has become increasingly common. Police and representatives of the Prosecutor's Office often call the owners and editors of websites to remove unwanted material. Most providers do not wait for court orders to remove targeted materials, and such pressure encourages self-censorship. As a result, there has been a massive exodus of opposition websites to foreign site-hosting providers, as well as a trend toward greater use of social-networking sites. Additionally, as the blacklist law allows the government to quickly block access to websites that contain information considered to be prohibited, and the evaluation criteria for these decisions is unclear, users and administrators of web resources are forced to practice self-censorship in order to avoid responsibility.

Government attempts to influence the blogosphere and other online sources of information continued from 2012–2013. The Kremlin allegedly influences the blogosphere through media organizations as well as the progovernment youth movements Nashi ("Ours") and Molodaya Gvardiya ("Young Guard").[40] The emergence of competing propaganda websites has led to the creation of a vast amount of content that collectively dominates search results, among other effects.[41] Leaked e-mails allegedly belonging to Nashi leaders revealed that the pro-Kremlin movement had been widely engaging in all kinds of digital activities, including paying commentators to post content, disseminating DDoS attacks, and hijacking blog ratings.[42] Propagandist commentators simultaneously react to discussions of "taboo" topics, including the historical role of Soviet leader Joseph Stalin, political opposition, dissidents like Mikhail Khodorkovsky, murdered journalists, and cases of international conflict or rivalry (with countries such as Estonia, Georgia, and Ukraine, but also with the foreign policies of the United States and the European Union). Furthermore, minority languages are underrepresented in Russia's blogosphere.

There are few specific economic constraints that negatively impact the financial stability of online media. The most common sources of news and information—the federal TV channels—are owned

[39] Roman Zholud, "Labelling [sic] a web publication 'extremist,': how this is done in Oryol," Glasnost Defense Foundation Digest No. 586, Glasnost Defense Foundation, October 8, 2012, http://www.gdf.ru/digest/item/1/1016#ev1.
[40] The Kremlin-affiliated media organizations include the Foundation on Effective Politics, led by Gleb Pavlovsky; New Media Stars, led by Konstantin Rykov; and the Political Climate Center, led by Aleksey Chesnakov.
[41] Ksenia Veretennikova, "'Медведиахолдинг': Единая Россия решила формировать собственное медиапространство" ['Medvediaholding:' United Russia Decided to Form Its Own Media Space], *Vremya*, August 21, 2008, http://www.vremya.ru/2008/152/4/210951.html.
[42] Leaked mailboxes are published at this website: http://slivmail.com/ [in Russian]. Email that contains the plan to paralyze Kommersant newspaper website published at: http://rumol-leaks.livejournal.com/12040.html.

or controlled by the government. In this way, access to opposition and independent sources of information depends on one's access to the internet. On July 23, 2012, amendments to the law "On advertising" entered into force, outlawing the advertisement of alcohol-based products on the internet.[43] This law has had a considerable financial impact on independent internet resources, as advertising is their main source of income.

During 2012 and 2013, the internet, particularly social networks like Twitter, Facebook, and Vkontakte, continued to be a significant tool for mobilization and communication between citizens and activists. In 2011, opposition activists in Moscow used Facebook to organize street protests in reaction to the December 2011 State Duma elections, although local platforms like Vkontakte are more popular tools for political mobilization in other regions.[44] Organizers of subsequent protests, such as those related to Putin's inauguration in May 2012 and the January 2013 "March Against Scoundrels" protesting the bill banning Americans' adoption of Russian children, have also made use of social-networking platforms to call attention to events. Additionally, crowdfunding websites such as RosUznik.org, which raises money for and coordinates the legal defenses of civil activists charged in the Bolotnaya Case, have emerged as a way for opposition activists to organize support efforts online.[45]

VIOLATIONS OF USER RIGHTS

During 2012 and early 2013, government pressure against online users continued to escalate through the use of lawsuits, administrative prosecutions, unlawful criminal prosecution using anti-extremist legislation, and charges for offending government officials. In July 2012, the State Duma introduced legislation that recriminalizes defamation for both online and offline speech. Additionally, the Russian government continues to employ surveillance methods that circumvent proper judicial oversight requirements and which threaten the civil liberties of online users.

Although the constitution grants the right to free speech, this right is routinely violated, and there are no special laws protecting online modes of expression. Online journalists do not possess the same rights as traditional journalists unless they register their websites as mass media. Recently, police have been suppressing online expression through the use of Article 282 of the criminal code, which restricts "extremism." The term is vaguely defined and includes "xenophobia" and "incitement of hatred toward a social group." The phrase "social group" is particularly problematic as the criminal code does not clearly describe what a social group entails, and several extremism cases in 2012 involved broad definitions of the term "social groups" to include the United Russia political party and law enforcement officers.[46]

[43] Законопроект №81110-6 [Draft Bill #81110-6], Official State Duma website, accessed July 30, 2013, http://bit.ly/NlBpxl.
[44] Tom Balmforth, "Russian Opposition 'Likes' Facebook," Radio Free Europe / Radio Liberty, May 18, 2012, http://www.rferl.org/content/russian-opposition-likes-facebook/24585388.html.
[45] "Arrest extension validated for Moscow riot participants," Russian Legal Information Agency, August 8, 2012, http://rapsinews.com/judicial_news/20120806/264133072.html.
[46] Maria Kravchenko, "Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2012," edited by Alexander Verhovsky, SOVA Center for Information and Analysis, June 26, 2013, http://bit.ly/18A40f8.

Despite claims that the State Duma is planning to adopt special legislation establishing criminal and civil liability for internet activities and offenses,[47] existing laws do not differentiate between online and offline activities. In the case of some crimes, such as defamation, slander, or extremism, use of the internet can be considered an aggravating factor.

In July 2012, the State Duma passed amendments to the criminal code that recriminalized defamation, after having just decriminalized it less than a year earlier. The revision of Article 128.1 of the code makes it easier to use this provision arbitrarily with the aim of pursuing those who criticize government policy. Revisions to Article 129 of the code officially make defamation a criminal offense, with applicable punishment including a fine of up to RUB 5 million (approximately $170,000). Previously, when prosecuted for defamation, one could typically expect a suspended sentence, especially as a first offender. Now the maximum possible fine allowed under the criminal law can be applied under section 5, Article 128.1, with no reduction in other negative legal consequences for the person convicted.

A draft law concerning the introduction of criminal liability for publicly insulting the feelings of religious believers was introduced in the State Duma in September 2012.[48] The law, which came into effect on July 1, 2013, establishes fines up to RUB 300,000 (approximately $10,000) or 1 year imprisonment. Critics point out that the law is too vaguely worded and that key terms, such as "worship" or "religious traditions," are not properly defined, making it difficult to predict the ways in which the law will be implemented. It is also unclear in what ways online activities might be prosecuted under this new law.

The practice of criminal prosecution has expanded over the past year: in 2012 there were 103 cases of criminal prosecution against online users, compared to 38 cases in 2011.[49] The majority of these cases were related to incitement of hatred against national and social groups or calls for extremism published on social networks. A few charges for insulting government representatives and inciting riots have been registered as well. In April 2012, blogger Dmitry Shipilov was sentenced to 11 months of correctional labor for his brusque article addressed to the governor of the Kemerovo region, Aman Tuleev.[50] The Investigative Committee of the Russian Federation opened a criminal case in March 2012 against journalist and blogger Arkadiy Babchenko for writing a blog post encouraging an unauthorized protest, with references to using force against police authorities.[51] Additionally, on May 14, 2012, State Duma deputy Aleksandr Khinshtein sent a request to the

[47] Vladimir Bogdanov, Анонимки на просвет [Anonymity on clearance], RG.ru, September 11, 2012, http://www.rg.ru/2012/09/11/anonim.html.
[48] Законопроект №142303-6 [Draft Bill #142303-6], Official State Duma website, accessed July 30, 2013, http://asozd.duma.gov.ru/main.nsf/(SpravkaNew)?OpenAgent&RN=142303-6&02. See also "Analysis on Russia's New Blasphemy Law: 28 February 2013," The Institute on Religion and Public Policy, http://www.religionandpolicy.org/reports/the-institute-country-reports-and-legislative-analysis/europe-and-eurasia/russia/analysis-on-russia-s-new-blasphemy-law-2013/.
[49] "Russia: a global threat to internet freedom," Agora Human Rights Association, February 4, 2013, http://agora.rightsinrussia.info/archive/reports/global-threat.
[50] "Блогер получил 11 месяцев за оскорбление Тулеева" [Blogger received 11 months for insulting Tuleyev], Grani.ru, April 3, 2012, http://grani.ru/Internet/m.196855.html.
[51] "Independent journalist sued for 'extremist' blog entry," Gazeta.ru, March 21, 2012, http://en.gazeta.ru/news/2012/03/21/a_4099301.shtml.

General Prosecutor's Office to open a criminal case against users of Twitter and Facebook who called for participation in public protests in Moscow on May 6, 2012, though it appears that the General Prosecutor has not acted on the request.[52]

Various forms of administrative and legal pressure against online bloggers and activists continued in 2012–2013. In August 2012, Maksim Efimov, the chair of the Karelia Youth Human Rights Group, sought asylum in Estonia after prosecutors requested that he be committed to a psychiatric ward. In April 2012, Efimov was charged with insulting the feelings of Orthodox believers for his critical article entitled "Karelia is tired of priests," which described the close cooperation between the Karelian regional government and representatives of the Russian Orthodox Church.[53] Efimov has been granted political asylum in Estonia, while the criminal case against him remains under investigation by the Karelian Investigative Committee.[54]

In May 2012, a civil activist from Tuymen, Nikolay Lyambin, was arrested on suspicion of drug possession. Lyambin claims that the drugs were planted and relates his detention and prosecution to his activities online, as he was one of the creators of an opposition group on the social network Vkontakte.[55] In February 2013, Pavel Khotulev, who criticized regional standards of education in Tatarstan in his blog post, was sentenced to pay a fine of $3,300 for incitement of hatred against Tatars.[56]

Privacy and anonymity are key concerns for many online users in Russia. There are currently no restrictions on the use of circumvention tools or anonymizers, although such tools may be banned in the near future. Presently, identification is needed for signing a contract for internet access or cellular services. Additionally, owners of public Wi-Fi spots are required to use content filters to protect children from potentially accessing "harmful" information (Article 6.17 of the code of administrative offenses). This requirement may force owners to implement age checks for users. In October 2012, State Duma members from the Liberal Democratic Party of Russia revived the idea of forcing social network users to enter their passport details when registering on these websites.[57] However, later that month the State Duma decided that this proposal was unnecessary.[58]

The extent to which internet users in Russia are subject to extralegal surveillance of their online activities remains unclear; however, recent evidence suggests that the Russian government has significantly increased its surveillance capabilities over the past few years. Since 2000, all ISPs have

[52] "Retweeted to General Prosecutor", Gazeta.ru, May 14, 2012, http://www.gazeta.ru/politics/2012/05/14_a_4583269.shtml.
[53] Vyacheslav Kozlov, "Blogger faces up to 2 years in jail for critising Russian Orthodox church," Gazeta.ru, April 13, 2012, http://en.gazeta.ru/news/2012/04/13/a_4345165.shtml.
[54] "Blogger who Criticized Orthodox Church Seeks Political Asylum in Estonia," Agora Human Rights Association, accessed July 30, 2013, http://agora.rightsinrussia.info/archive/news/efimov/estonia.
[55] "New fraud criminal cases in Tymen" [in Russian], Golosa.info, May 18, 2012, http://www.golosa.info/lambin.
[56] "Pavel Hotulev has been convicted" [in Russian], Evening-Kazan.ru, February 15, 2013, http://www.evening-kazan.ru/news/pavlu-hotulevu-vynesen-obvinitelnyy-prigovor.html.
[57] "В Госдуме рассматривают возможность регистрации в соцсетях по паспорту" [State Duma considering registering social networks with passport], Kommersant-FM, October 11, 2012, http://www.kommersant.ru/doc/2041985.
[58] "MPs oppose passport details for social networks," Russian Legal Information Agency, October 12, 2012, http://rapsinews.com/legislation_news/20121012/264976106.html.

been required to install the "system for operational investigative measures,"[59] or SORM-2, which gives the FSB and police access to internet traffic. The system is analogous to the Carnivore/DCS1000 software used by the U.S. Federal Bureau of Investigation (FBI), and operates as a packet-sniffer that can analyze and log data passing through a digital network.[60] ISPs that do not comply with SORM system requirements are promptly fined, and may have their license revoked if problems persist. Russian authorities are technically required to obtain a court order before accessing an individual's electronic communications data; however, the authorities are not required to show the warrant to ISPs or telecom providers, and FSB officers have direct access to operators' servers through local control centers.[61]

There is increasing evidence that Russian surveillance technology is being used for political purposes, including the targeting of opposition leaders. In a Supreme Court case in November 2012 involving Maxim Petlin, an opposition leader in the city of Yekaterinburg, the court upheld the government's right to eavesdrop on Petlin's phone conversations because he had taken part in so-called "extremist activities," namely antigovernment protests. Online surveillance represents somewhat less of a threat in the major cities of Moscow and Saint Petersburg than in the regions, where almost every significant blog or forum is monitored by the local police and Prosecutor's Office. Most of the harassment suffered by critical bloggers and other online activists in Russia occurs in the regions.

Extralegal intimidation is also used to limit users' abilities to interact and mobilize on the internet. For example, in the fall of 2012, Yuliya Bashinova, a journalist at the internet publication Grani.ru, was summoned for questioning by the Investigative Committee to explain why she had signed a petition on the website of Amnesty International in support of human rights defender Igor Kalyapin.[62] It has been reported that investigators have held talks with citizens who signed the petition in several Russian cities.

Despite the reduction in the severity of violence over the past year, implicit impunity for those who commit violence against bloggers, online journalists, and other online users is common. Information on investigations into crimes committed in previous years is usually not available to citizens. Between 2008 and 2011 there were three internet-related murders and one attempted murder, according to research conducted by the AGORA Association.[63] Only one of these resulted in a prosecution: according to the verdict, the murder of Magomed Evloev, the owner of the

[59] Konstantin Nikashov, "СОРМ для IP-коммуникаций: требуется новая концепция" [SORM for IP-Communications: New Concept Needed], Iksmedia.ru, December 10, 2007, http://www.iksmedia.ru/topics/analytical/effort/261924.html?__pv=1. For more information on SORM, see V.S. Yelagin, "СОРМ-2 история, становление, перспективы" [SORM-2 History, Formation, Prospects], Protei, http://www.sorm-li.ru/sorm2.html.
[60] B. S. Goldstein, Y. A. Kryukov, and V. I. Polyantsev, "Проблемы и Решения СОРМ-2" [Problems and Solutions of SORM-2], *Vestnik Svyazi* no. 12 (2006), http://www.protei.ru/company/pdf/publications/2007/2007-003.pdf.
[61] Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal*, Fall 2013, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.
[62] "Grani.ru journalist summoned to Investigative Committee" [in Russian], Grani.ru, September 6, 2012, http://grani.ru/Society/Law/m.206066.html.
[63] Ibid.

website Ingushetia.ru, was the result of a police officer's careless handling of a gun.[64] There has been no prosecution dealing with the attempted murder of journalist and blogger Oleg Kashin, and there were dozens of other assaults and beatings for which no individual has been brought to justice. Critics blame the Russian Federal Security Service for failing to provide the necessary operational support to solve such cases.[65]

From 2012–2013, the threat of cyberattacks continued, including DDoS attacks on websites and hacking into the private accounts of users. The police and Investigative Committee have consistently failed to investigate these attacks, including dozens of cyberattacks on online media and opposition websites. During 2012, at least 47 episodes of DDoS attacks were registered,[66] but only 2 of them (against the official websites of the government and the prime minister) were investigated.[67] Most of the attacks occurred during important events such as the presidential election or mass protests. There were also significant attacks launched against independent media outlets. In May 2012, a botnet of 182,000 computers was used to attack the website of the television channel Dozhd. On June 12, 2012, a single botnet made up of 133,000 computers attacked four online media outlets, including the websites of *Novaya Gazeta*, the radio station Echo of Moscow, Slon.ru, and the website for Dozhd.[68] In the past, similar cyberattacks on media outlets have been linked to leaders of the progovernment youth group Nashi.[69]

In January 2013, President Vladimir Putin signed Decree #31c "On the formation of a state system for detecting, preventing and mitigating the effects of computer attacks on the information resources of the Russian Federation." Under this decree, the FSB has been vested with the task of developing a method for preventing and investigating attacks by hackers on Russia's internet resources, and with promoting international cooperation in the fight against cybercrime; however, no further steps have been taken toward the prevention of cybercrime.

---

[64] Svetlana Bocharova, "The end at the "Oriental Fairytale" [in Russian], October 4, 2010, http://www.gazeta.ru/politics/2010/08/04_a_3404590.shtml.

[65] "Advocate blames FSB of inactivity while investigation of attempted murder of Oleg Kashin" [in Russian], Openinform.ru, November 6, 2012, http://openinform.ru/news/pursuit/06.11.2012/27620/.

[66] AGORA Association, Доклад: Россия как глобальная угроза свободному Интернету, [Report: Russia - a global threat to Internet freedom], http://eliberator.ru/news/detail.php?ID=21.

[67] Второй красноярский хакер получил срок за атаки на сайт Путина в мае 2012 года [Second hacker from Krasnoyarsk sentenced to jail for cyber-attacks against Putin's website on May 2012], Gazeta.ru, March 29, 2013, http://www.gazeta.ru/social/news/2013/03/29/n_2823469.shtml.

[68] Alexander Panasenko, Впервые сайты четырех российских СМИ атакованы одним ботнетом [For the first time fout websites of Russian media are under attack of one botnet], Anti-Malware.ru, June 14, 2012. http://www.anti-malware.ru/news/2012-06-14/9345.

[69] "Mail Leaks Link Youth Tsars to Cyberattack," RIA Novosti, February 9, 2012, http://en.rian.ru/russia/20120209/171235899.html.

RWANDA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	13	12
Limits on Content (0-35)	19	18
Violations of User Rights (0-40)	19	18
Total (0-100)	**51**	**48**

* 0=most free, 100=least free

POPULATION: 10.8 million
INTERNET PENETRATION 2012: 17 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- ICT development continued to spread, expanding access. Rwandan internet users became more active on social media and vocal in criticizing the government (see **OBSTACLES TO ACCESS** and **LIMITS ON CONTENT**).
- A number of independent online news outlets and opposition blogs were intermittently inaccessible in Rwanda, though it is uncertain whether the disruptions were due to deliberate government interference, as was the case in past years, or to technical issues (see **LIMITS ON CONTENT**).
- An amended media law expanded the rights of journalists and recognized freedom for online communications; however, it retained provisions that may increase government control over internet content (see **VIOLATIONS OF USER RIGHTS**).
- A new law on interception authorized high-ranking security officials to monitor e-mail and telephone conversations of individuals considered potential threats to "public security" (see **VIOLATIONS OF USER RIGHTS**).
- SIM card registration requirements were launched in 2013 (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

In recent years, the government of Rwanda under President Paul Kagame has embarked on an ambitious economic development strategy that aims, among other things, to create a vibrant industry for information and communication technologies (ICTs) and position Rwanda as a regional ICT hub. Although internet penetration remains low—hampered primarily by poverty and lack of appropriate infrastructure, especially in rural areas—access is continually expanding with public and private investments in broadband technology across the country, and mobile internet access is increasing at an impressive rate. Meanwhile, the proliferation of ICTs has contributed to progress in the country's governance, health, education, agriculture, and finance sectors.[1]

While ICT development has been among the top priorities for the Rwandan government, the country's tenuous political environment and sensitive ethnic relations since the 1994 genocide has led the government to exert some controls over online content and expression. A few critical news websites that were previously blocked in 2010-2011 were intermittently inaccessible in Rwanda throughout 2012 and early 2013, though a number of critical blogs were unavailable altogether. In addition, worries remain that the government's firm restrictions on print and broadcast media—particularly on contentious content concerning the ruling party and the 1994 genocide—will cross over into the internet sphere, as occurred when the authorities blocked the online version of an independent newspaper in the lead-up to the 2010 presidential election. Nevertheless, there were no reported cases of imprisonment or violence against online journalists or internet users in 2012-2013.

Progressive amendments to the 2009 Media Law were adopted in March 2013, providing journalists with the "right to seek, receive, give and broadcast information and ideas through media;" the amendments also explicitly recognize freedom for online communications. Nevertheless, the passage of the new law has led to some fears of increasing government control over the establishment of online outlets. The government-run Media High Council systematically monitors all print and broadcast media coverage during the country's annual genocide mourning period every April, and the monitoring of online media was incorporated for the first time during Rwanda's 18th commemoration period in April 2012. Legislative initiatives in 2012 also expanded the surveillance and interception capabilities of security authorities, and there are increasing indications that the government may be systematically monitoring and intercepting e-mail and other private communications.

OBSTACLES TO ACCESS

Poverty continues to be the primary impediment barring Rwandans from accessing new ICT tools, especially the internet. Over 90 percent of the population lives in rural areas, with the majority

[1] Ministry of Youth and ICT, "Measuring ICT sector performance and Tracking ICT for Development (ICT4D) towards Rwanda Socio-Economic Transformation," Rwanda ICT Sector Profile 2012, http://bit.ly/18lFhdJ.

practicing subsistence agriculture and approximately 45 percent living below the poverty line.[2] Consequently, internet penetration in Rwanda is still low at 8 percent in 2012, up from 7 percent in 2011, according to estimates from the International Telecommunication Union (ITU).[3] Meanwhile, official government statistics cite a penetration rate of 26 percent in 2012.[4] In addition, access is still limited mostly to Kigali, the capital city, and remains beyond the economic capacity of most citizens, particularly those in rural areas who are limited by low disposable incomes and who do not have high levels of ICT awareness or digital literacy.[5] Between 70 and 90 percent of the population speaks only Kinyarwanda, making internet content in English unavailable to the majority of Rwandans.[6]

In the face of such challenges, the Rwandan government has made ICT development a high priority. Recent government initiatives include the "National ICT Literacy and Awareness Campaign" launched in early 2013 that aims to familiarize at least 200,000 Rwandans with ICT tools within six months.[7] The government has also invested in a project to enhance digital literacy among women as part of an effort to bridge Rwanda's gender gap and encourage women entrepreneurs.[8] In addition, MTN Rwanda has launched a portable solar energy system known as the "Comeka ReadySet," which is a multifunctional energy system that can charge mobile phones as well as power lights, radios, tablets and other devices, enabling ICT use among citizens living in rural areas with little to no electricity.[9] Accordingly, Rwanda was ranked by the ITU as the most dynamic African country in the field of ICTs in its "Measuring the Information Society 2012" ICT Development Index.[10]

The expansion of broadband internet services across the country is further facilitating access to new media tools and technologies. A 2013 analysis of worldwide broadband download performance ranked Rwanda in first place in Africa for download speeds and 62nd place globally with an internet speed of 7.88 Mbps as of February 2013.[11] In partnership with the private sector, the country is

---

[2] Central Intelligence Agency, "Rwanda," *The World Factbook*, accessed April 12, 2013, https://www.cia.gov/library/publications/the-world-factbook/geos/rw.html.

[3] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[4] Calculated as total estimated internet users divided by total population, from a 2010 RURA survey. See, Ministry of Youth and ICT, "Measuring ICT sector performance and Tracking ICT for Development (ICT4D)"; Daniel Nkubito, "ISSUE PAPER: Internet Connectivity and Affordability in Rwanda," REF. NO: 002/12/2012, http://ppd.rw/wp-content/uploads/2012/12/internet-connectivity-and-affordability-in-Rwanda-issue-paper-Final.pdf.

[5] Ministry of Youth and ICT, "Measuring ICT sector performance and Tracking ICT for Development (ICT4D)."

[6] Ann Garrison, "Rwanda Shuts Down Independent Press," *Digital Journal*, April 14, 2010, http://www.digitaljournal.com/article/290545; Beth Lewis Samuelson and Sarah Warshauer Freedman, "Language Policy, Multilingual Education, and Power in Rwanda," *Language Policy* 9, no. 3 (June 2010), http://bit.ly/1bmZW5X.

[7] "ICT Literacy Campaign Gets Under Way," *Rwanda Focus*, January 21, 2013, http://bit.ly/1fDDDuz.

[8] "Promoting Digital Opportunities for Women in Rwanda," Rwanda Telecentre Network, December 22, 2012, http://www.rtnrwanda.org/index.php/en/news/100-promoting-digital-opportunities-for-women-in-rwanda. Other major ICT projects that aim to expand access to ICTs include: the Kigali Metropolitan Network, the National Backbone , the IT innovation center, Wibro wireless broadband, the ICT Bus, One Laptop per Child, TracNet, and the Regional Communications Infrastructure Program. See, Rwanda Development Board, http://www.rdb.rw/.

[9] Eric Bright, "MTN Launches Portable Renewable Energy System in Rwanda," *Rwanda Focus*, January 29, 2013, http://focus.rw/wp/2013/01/mtn-launches-portable-renewable-energy-system-in-rwanda/.

[10] International Telecommunication Union, "Measuring the Information Society 2012," http://www.itu.int/ITU-D/ict/publications/idi/index.html; Tom Jackson, "ITU Report Ranks Rwanda's ICT Sector Most Dynamic," *Humanipo*, October 16, 2012, http://www.humanipo.com/news/1884/ITU-report-ranks-Rwandas-ICT-sector-most-dynamic.

[11] Net Index, "Rwanda," Download Index, accessed February 24, 2013, http://www.netindex.com/download/allcountries/.

aiming to deploy a much wider National Last Mile broadband network in 2013 to expand internet penetration countrywide, complementing the 1,380 mile fiber-optic telecommunications network built in 2011 that links Rwanda to the undersea cables running along the East African coast.[12]

As a result of these infrastructural developments, internet prices are decreasing. In 2012, the Broadband Systems Corporation, a local service provider, charged monthly fees of about US$30 for single users and $46 for multiple users, while the cost of using the internet in a cybercafe is approximately $1.28 for 30 minutes.[13]

Mobile phone penetration in Rwanda is significantly higher than that for internet access, growing from 40 percent in 2011 to over 50 percent in 2012, according to the ITU, while government figures noted a penetration rate of 57 percent in May 2013.[14] This growth has been largely a result of increasing competition between the three main mobile phone operators—MTN, TIGO and AIRTEL[15]—whose respective market share is 64 percent, 34 percent, and 2 percent.[16] Rural populations have a comparatively high mobile phone usage rate compared to rural internet access rates,[17] as access has been made easier by a well-developed mobile phone network that covers nearly 98 percent of the population.[18] Innovative initiatives targeting rural populations have further encouraged increased mobile phone and internet usage, such as the e-Soko ("e-market") program created by the Rwanda Development Board that provides farmers with real-time information about market prices for their agricultural produce on their mobile devices.[19]

Internet access via mobile phones has been available since 2007, but the high cost of data-enabled handsets and limited bandwidth restrained its popularity in the first few years. With the government-sponsored fiber-optic cable expansion project completed in early 2011, internet services throughout the country have improved, facilitating increased mobile phone internet access.[20] As of September 2012, mobile internet tariffs range from 20 Rwfr/Mb to 50 Rwfr/Mb (US$0.03/Mb to $0.08/Mb), and the three mobile internet companies—MTN, TIGO and AIRTEL—offer their customers daily bundles at 1,000 Rwfr, 800 Rwfr and 650 Rwfr (US$1.52,

[12] The fiber-optic project is meant to boost access to various broadband services, increase electronic commerce, and attract foreign direct investment through business process outsourcing. "Rwanda Completes $95 Mln Fibre Optic Network," Reuters Africa, March 16, 2011, http://af.reuters.com/article/investingNews/idAFJOE72F07D20110316.
[13] Laurent Kamana, "National Backbone Reduces Internet Prices, Increases Speed," *New Times*, February 28, 2012, http://www.newtimes.co.rw/news/index.php?i=15282&a=64384.
[14] "Rwanda Mobile Penetration Tops 57%," *Biztech Africa*, May 1, 2013, http://bit.ly/13L8xYk.
[15] Airtel and Tigo have the same tariffs for on-net (RWF20 or US$0.03) and East Africa mobile (RWF120 orUS$0.18) telephone tariffs. TIGO remains with the highest off-net (RWF90 or US$0.13) and international (RWF240 or US$0.36) tariffs. MTN charges RWF60 per minute both for off-net and EAC tariffs. MTN dominates the outgoing voice traffic with 53 percent of on-net traffic; 49 percent of off-net traffic and 89 percent of international voice traffic. See, RURA, "Statistics and Tariff Information in Telecom Sector as of September 2012," Republic of Rwanda, http://bit.ly/GzwThp.
[16] RURA, "Statistics and Tariff Information in Telecom Sector as of September 2012."
[17] As illustrated by an August 2011 report from MTN Rwanda, one of the largest telecom operators in the country, which stated that the majority (60 percent) of its mobile voice users resides outside of Kigali. See, Saul Butera, "Rwanda: High Costs Affecting Rural Internet Penetration," *New Times*, August 15, 2011, http://bit.ly/1aFj4aU.
[18] RURA, "Statistics and Tariff Information in Telecom Sector as of September 2012."
[19] Ruth Kang'ong'oi, "Rwanda Telecenter Network Introduces Web 2.0 to Farmers," CIO East Africa, November 15, 2011, http://www.cio.co.ke/view-all-top-stories/4482-rwanda-telecenter-network-introduces-web-20-to-farmers.html.
[20] MasimbaTafirenyika, "Information Technology Super-charging Rwanda's Economy," *Africa Renewal,* April 2011, http://www.un.org/ecosocdev/geninfo/afrec/vol25no1/rwanda-information-technology.html.

$1.21, and $1.00), respectively.[21] In addition, MTN Rwanda offers low-cost data-enabled mobile phones ranging from 18,500 to 20,000 RWF (US$28 to $32) to further expand internet access, especially in rural areas,[22] though in late 2012, RURA announced plans to switch off unregistered counterfeit phones.[23]

Following the country's market liberalization policies implemented in 2001,[24] the number of companies providing telephone and internet services increased from one—the state-run Rwandatel—to 10 in 2012.[25] These providers are all privately owned, with the exception of the state-owned Rwandatel,[26] which has the largest market share of fixed broadband subscriptions as of September 2012.[27]

Two government-appointed regulatory bodies—the Rwanda Information Technology Authority under the Rwanda Development Board, and the Rwanda Utilities Regulatory Agency (RURA)—supervise the regulatory frameworks and implementation of the county's policies and strategies in the telecommunications sector. Although these bodies were created by the government, they seem to be working freely, and no known complaint has been leveled against them by investors in the ICT sector. Officially, RURA is a national body with autonomy in its administrative and financial management. However, its seven board members, supervisory board, and the managing director are nominated by and work under full control of the government.[28] Despite this, RURA has taken some independent decisions, such as measures to penalize MTN Rwanda for lack of compliance with license obligations in 2012.[29]

In 2009, RURA set up the Rwanda Internet Exchange (RINEX) to connect ISPs and enable the routing of local internet communications through a central exchange point without having to pass through international networks.[30] ISPs can also opt to connect via RINEX to the international

[21] RURA, "Statistics and Tariff Information in Telecom Sector as of September 2012."
[22] Saul Butera, "Rwanda: High Costs Affecting Rural Internet Penetration."
[23] Frank Kanyesigye, "Move to Ban Fake Phones Draws Mixed Reactions," *New Times*, October 5, 2012, http://www.newtimes.co.rw/news/index.php?i=15136&a=59161.
[24] Albert Nsengiyumva and Emmanuel Habumuremyi, *A Review of Telecommunications Policy Development and Challenges in Rwanda*, Association for Progressive Communications (APC), September 2009, http://www.apc.org/en/system/files/CICEWARwanda_20090908.pdf.
[25] These include fixed-line providers (Rwandatel, MTN Rwandacell, and Airtel International), mobile phone providers (Rwandatel, MTN Rwandacell, TIGO and AIRTEL), and internet service providers (ISPA, Rwandatel, MTN Rwandacell, New Airtel, Altech Stream Rwanda, 4G Rwanda, BSC, and 4G Networks). See, RURA, "Statistics and Tariff Information in Telecom Sector as of September 2012."
[26] Rwandatel was partially privatized in 2010 when it sold 80 percent of the company to the Libyan firm, LAP Green. Due to the political turmoil in Libya in 2011 and the subsequent freeze on Libya's investments and assets, however, LAP Green was forced to terminate its business in Rwanda.[26] In 2012, Rwandatel was liquidated; its assets were purchased by Tigo and Airtel, and the company was taken over by the Government of Rwanda. See, Shyaka Kanuma, "Bye Bye Rwandatel," *Rwanda Focus*, February 20, 2012, http://focus.rw/wp/2012/02/bye-bye-rwandatel/.
[27] RURA, "Statistics and Tariff Information in Telecom Sector as of September 2012."
[28] Article 9, "Law No. 39/2011 of 13/09/2001, Establishing an Agency for the Regulation of Certain Public Utilities," http://www.mhc.gov.rw/fileadmin/templates/PdfDocuments/Laws/RURA_Law.pdf.
[29] In line with its mission to protect consumers, RURA has imposed in November 2012 a daily fine equivalent to RWF 5,000,000 (US$7,692 for one month for non-compliance with its license obligations. See: RURA, "Decision No. 13/ICT-RURA/2012 of 4th December 2012 on MTN Rwanda Ltd. Non-Compliance with its License Obligations Related to Service Continuity," Republic of Rwanda, December 4, 2012, http://bit.ly/19iUmdf.
[30] RURA, *Guidelines for Rwanda Internet Exchange Point (RINEX) Management* (Kigali: RURA, 2009), http://bit.ly/16QXMD0.

internet. The aim, ostensibly, is to make intra-Rwandan internet communications cheaper and faster, though such control over internet traffic has the potential to facilitate efforts to systematically censor or monitor domestic online communications. As of the end of 2013, only five ISPs exchange internet traffic via RINEX,[31] and the price for national access remained the same as for international access.[32]

LIMITS ON CONTENT

In 2012 and early 2013, a number of independent online news outlets and opposition blogs were intermittently inaccessible in Rwanda, though it is uncertain whether the disruptions were due to deliberate government interference, as was the case in past years, or to technical issues. Nevertheless, users increased their engagement with social media tools in the past year and have become more vocal in criticizing the government.

While the government of Rwanda has been committed to expanding access to ICTs across the country, it has also simultaneously endeavored to restrict the types of content that users can access, particularly news content of oppositional nature. For example, in June 2010 the Media High Council ordered the website of the online version of the independent paper *Umuvugizi* to be blocked after its print version was suspended in April 2010, arguing that the ban on the newspaper applied to the online version as well.[33] *Umuvugizi* was unblocked after its six-month suspension period had expired, though it has reportedly experienced periodic blocking in the years since, including in 2012 and early 2013.[34] Some opposition sites continue to be blocked on some ISPs as of early 2013,[35] including *Umusingi* and *Inyenyeri News,*[36] which were both first blocked in 2011. *Umusingi's* content can still be accessed on its Facebook page,[37] and other news sites that have been sporadically blocked can still be accessed through their associated blogs.

Meanwhile, social-networking sites such as YouTube, Facebook, Twitter, and international blog-hosting services are freely available. The websites of international human rights organizations such as Freedom House, Amnesty International, and Human Rights Watch, as well as the online versions of media outlets like the BBC, *Le Monde*, Radio France Internationale, the *New York Times*, and many others are freely accessible. Websites of national news outlets are also easily accessible. These include the web versions of state-run media and pro-government outlets as well as independent

[31] RINEX, accessed April 13, 2013, http://www.rinex.org.rw/.
[32] Antoine Bigirimana, "Rwanda: The Story of the Internet—One Step Forward, Two Steps Backward," *New Times*, December 12, 2009, http://allafrica.com/stories/200912150559.html.
[33] Reporters Without Borders, "Persecution of Independent Newspapers Extended to Online Versions," news release, June 11, 2010, http://en.rsf.org/rwanda-persecution-of-independent-11-06-2010,37718.html. The newspaper *Umuseso,* which was also given a six-month suspension, does not have an online version.
[34] *Umuvugizi* websites include: http://www.umuvugizi.com/, http://umuvugizi.wordpress.com, and http://umuhanuzi.blogspot.com. Accessed April 11, 2013.
[35] Examples of these opposition sites include: http://inyenyerinews.org/, www.umuvugizi.com, www.umusingi.com, www.banyarwandapoliticalparty.org, http://leprophete.fr, www.therwandan.com.
[36] *Inyenyeri News,* accessed April 5, 2013, www.inyenyerinews.org.
[37] Umusingi Newspaper's Facebook page, accessed February 24, 2013, http://www.facebook.com/pages/Umusingi-Newspaper/122730681083696.

outlets such as *The Rwanda Focus*, *Rushyashya*, *The Chronicles*, *Umusanzu* and *Rwanda Dispatch*. Most radio stations are accessible online, either through their own websites and blogs, or through social media.

As a result of the more limited space for press freedom in the traditional media sphere, Rwandan media outlets are increasingly going online to avoid government control or suspension as well as heavy production costs.[38] Nonetheless, the economic environment for online news websites remains a challenge for independent outlets, particularly in comparison to their state-run counterparts that receive income from government advertisements and direct subsidies.

According to a 2010 law relating to electronic messages, signatures and transactions, intermediaries and service providers are not held liable for the content transmitted through their networks.[39] Nevertheless, Media High Council reportedly operates an online monitoring department to screen web content,[40] and has been known to contact websites to request the removal of certain information. Two online news websites, *Umusingi* and *Umurabyo*, have experienced such requests to delete content related to local political affairs and ethnic relations in recent years. In mid-2013, an independent test conducted by Freedom House found a number of opposition blogs inaccessible altogether;[41] however, it is uncertain whether those sites were taken down out of the owners' own accord or due to external pressure to do so. Appeals can be made through the Media High Council, though they are not often successful, according to journalists.

Online journalists based in Rwanda are joining their print and broadcast colleagues in exercising self-censorship, particularly on topics that can be construed as disruptive to national unity and reconciliation. According to some journalists, self-censorship is viewed as a legitimate practice given the country's sensitive social and political environment. Nevertheless, the spread of social media tools has empowered Rwandans to discuss issues that were formerly taboo and not open to public discussion due to fears of persecution. For example, President Kagame's succession following the end of his current term in 2017 has been debated in various media with diverging views. A number of citizens support Kagame's reelection, which would require a constitutional amendment to increase presidential term limits, while others oppose Kagame's efforts to prolong his tenure and suggest a peaceful transition to a new leadership.[42]

The expansion of internet access has enabled the Rwandan blogosphere to evolve into a vibrant platform for expression, even though the websites and blogs of opposition activists both within and outside Rwanda are inconsistently available.[43] While opposition supporters living outside Rwanda,

---

[38] "Rwanda: Why We Went Online: Media Icons Speak Out," *Itangazamakuru*, March 2012, http://bit.ly/18GUIy1.
[39] "Law No. 18/2010 of 12/05/2010, Relating to Electronic Messages, Electronic Signatures and Electronic Transactions," http://www.wipo.int/wipolex/en/text.jsp?file_id=243157.
[40] "Rwandan Gov't Officials to Counter 'Harmful' Propaganda Through Social Media," *Great Lakes Voice*, March 13, 2011, http://greatlakesvoice.com/?p=681.
[41] Opposition blog websites that were unavailable as of May 2013 were: http://ww.iwacu1.com, http://ww.musabyimana.be, http://rwandarwabanyarwanda.over-blog.com, http://ww.banyarwandapoliticalparty.org.
[42] Shyaka Kanuma, "Big Debate Starts on Whether Kagame Contests Another Term," *Rwanda Focus*, February 10, 2013, http://focus.rw/wp/2013/02/big-debate-starts-on-whether-kagame-contests-another-term/#comment-11752.
[43] This includes the website of opposition leader Victoire Ingabire at http://www.victoire2010.com, as well as other sites at http://rwandaspeaks.com/tag/freedom-of-the-press/, and www.newsrwanda-nkunda.blogspot.com.

mainly in Europe and the United States, are responsible for most of the criticism against the government on forums, websites, and blogs, local dissenting voices are increasingly heard in online news portals such as *Igihe*.

Facebook and Twitter are also emerging as popular platforms for online interaction, in part as a result of the increasing use of internet-enabled phones.[44] MTN Rwanda introduced a "SMS to Twitter" tool to facilitate the social media platform's use for people who do not have easy access to the internet on computers.[45] The president is an active supporter of these social networks, occasionally using the platforms to engage in discussions with users and openly respond to issues concerning the current state of governance in the country. By the end of 2012, Kagame emerged as one of the most popular African presidents on Twitter with nearly 95,000 followers.[46]

Twitter has also offered Rwandans a new platform for protest. For example, netizens flocked to Twitter in 2012 to reject a decision by the Kigali City Council to close a local entertainment venue.[47] In another instance, Rwandans came together on Twitter to denounce a controversial United Nations report on Rwanda's involvement in the conflict taking place in the Democratic Republic of Congo. Citizens also used the social media platform to circulate a petition against the United Kingdom's cuts in development aid that came in response to the UN report's findings.[48]

With mobile phones more widely accessible than the internet, text messages have become another important channel for citizens to voice discontent with the authorities and expose abuses of power. For example, the live radio programs, "Good Morning Rwanda" and "Good Evening Rwanda," have become a significant venue for citizens to criticize government malpractices via SMS messages, which are broadcast on the radio. Most recently, citizens challenged the education ministry over the country's quality of education. Nevertheless, the ability of citizens to use digital media for organizing large-scale street protests remains limited due to broader restrictions on freedom of assembly, particularly regarding politically sensitive topics.

VIOLATIONS OF USER RIGHTS

Legislative initiatives in 2012 and early 2013 had both positive and negative effects on freedom of expression and internet freedom in Rwanda, including amendments to the 2009 Media Law, an Access to Information Law, and a revised law on the interception of communications. SIM card registration requirements were also launched in 2013.

Article 34 of the Rwandan constitution, adopted in May 2003, provides for freedom of the press and freedom of information, but in practice, the government maintains tight control over the

[44] "Facebook Statistics: Rwanda," Socialbakers, accessed February 24, 2012, www.socialbakers.com/facebook-statistics/rwanda.
[45] MTN, "MTN Twitter SMS," accessed February 25, 2013, http://www.mtn.co.rw/Content/Pages/54/MTN_Twitter_SMS.
[46] Allan Brian Ssenyonga, "Twitter: 2012 was a Very Interesting Year for 'RwOT,'" *New Times*, December 31, 2012, http://newtimes.co.rw/news/views/article_print.php?&a=13541&week=52&icon=Print.
[47] Allan Brian Ssenyonga, "Twitter: 2012 was a Very Interesting Year for 'RwOT.'"
[48] Steve Doughty, "British Aid to Rwanda 'Is Funding a Dictator': UK Millions Fuel Armed Conflict, says President's Former Aide," *Mail Online*, November 25, 2012, http://dailym.ai/Tf37yA.

media. In March 2013, the state adopted progressive amendments to the 2009 Media Law, granting journalists the "right to seek, receive, give and broadcast information and ideas through media" and explicitly providing for freedom of online communications in Section 3, Article 19.[49] Nevertheless, the passage of the new law has led to some fears of increasing government control over the internet,[50] with the freedom of expression organization Article 19 criticizing the law for containing "too many provisions which pose a threat to journalists and the independence of the media, including online media."[51] In particular, the new law gives the minister of ICTs unlimited powers to establish the conditions for both local and foreign media companies to operate in Rwanda.

A revised Access to Information Law was passed in December 2012 and is expected to allow journalists to conduct investigative journalism with more official and credible sources of information.[52] Nevertheless, the extent to which the media should have the unchecked right to free expression is often a matter of public debate in Rwanda, with some commentators suggesting that Rwanda's media practitioners should be cautious in their speech as long as the history of genocide continues to haunts the country.[53]

While there are no laws that specifically restrict internet content or criminalize online expression, Rwanda's generally restrictive legal provisions governing the traditional media could be applied to the internet, particularly given the lack of a fully independent judiciary. For example, the decision to ban the online version of *Umuvugizi* in 2011 was based on charges of publishing "divisive language,"[54] a category of expression that is criminalized by the 2001 Law on Discrimination and Sectarianism.[55]

A vague 2008 law against "genocide ideology" similarly threatens freedom of expression both online and off, prescribing heavy prison sentences and fines for any offender "…who disseminates genocide ideology in public through documents, speeches, pictures, media or any other means."[56] In response to criticisms of the law's overly broad nature, the minister of justice proposed

[49] "Law Regulating Media, No. 02/2013 of 08/02/2013," Official Gazette 10, March 11, 2013, http://blog-tdas.s3.amazonaws.com/blog-tdas/2013/03/Official_Gazette_no_10_of_11.03.2013.pdf.
[50] "Proposed Media Law Fails to Safeguard Free Press," IFEX, January 5, 2012, http://www.ifex.org/rwanda/2012/01/05/media_law/.
[51] Article 19, "Rwanda: Media Law Does Not go Far Enough," press release, March 18, 2013, http://www.article19.org/resources.php/resource/3665/en/rwanda:-media-law-does-not-go-far-enough.
[52] Frank Kanyesigye, "Will Information Bill Change the Rwanda's Media Environment?" *Sunday Times*, February 17, 2013, http://allafrica.com/stories/201302180094.html.
[53] David Kabuye, "Rwanda's Media – Cautious of Content," *New Times*, November 19, 2012, http://www.newtimes.co.rw/news/index.php?i=15181&a=60840; Daniella Waddoup, "Press Freedom in Rwanda," *Think Africa Press*, February 18, 2011, http://thinkafricapress.com/rwanda/press-freedom-rwanda.
[54] Media Institute, "Tabloid Website Blocked," IFEX, June 8, 2010, http://ifex.org/rwanda/2010/06/08/umuvugizi_website_blocked/.
[55] "Law No. 47/2001 on Prevention, Suppression and Punishment of the Crime of Discrimination and Sectarianism," http://www.adh-geneva.ch/RULAC/pdf_state/Law-47-2001-crime-discrimination-sectraianism.pdf; Jennie E. Burnet, "Rwanda," in *Countries at the Crossroads 2007* (New York: Freedom House; Lanham, MD: Rowman and Littlefield, 2007), http://freedomhouse.org/template.cfm?page=140&edition=8&ccrpage=37&ccrcountry=167.
[56] Article 8, "Law No. 18/2008 of 23/07/2008 Relating to the Punishment of the Crime of Genocide Ideology," http://www.refworld.org/docid/4acc9a4e2.html.

amendments in November 2012 that aim to make the law more definitive and easier to interpret.[57] Awaiting consideration by the senate after its passage in the lower house in July 2013, the amended law reduces prison sentences from 25 years to a maximum of nine and requires proof of criminal intent behind an offending act that must be "characterized by thoughts based on ethnicity, religion, nationality or race to foment genocide [or] support genocide."[58] Nevertheless, the law still restricts freedom of expression by retaining the notion of "genocide ideology" as a criminal offense and by excluding a clear distinction between a private conversation and public speech.[59]

Penalties for criminal defamation may also be applicable to the internet, with defamation of the president or other public officials carrying a penalty of up to five years in prison.[60] Only one prosecution for online activity was reported in December 2012 concerning the entertainment journalist John Kalisa of the website *kigalihits*, who was arrested on allegations of defamation after he had posted a picture of a young girl on a drinking spree on his Facebook wall. The same journalist had been arrested and warned by authorities in 2011 for similar professional offenses.[61]

Although many traditional journalists view the threat of imprisonment as a key constraint on their work, detentions have been less common for online expression with the last case of imprisonment for online activities occurring in 2007.[62] There were also no reported cases of extralegal intimidation or violence against online journalists or users in 2012 and early 2013, but intimidation tactics against journalists still generally limit freedom of expression in Rwanda, which ranks among the top 10 countries from which journalists seek exile, according to the Committee to Protect Journalists.[63]

There are no restrictions on anonymous communication online in Rwanda, though RURA initiated SIM card registration requirements in early 2013 to "decrease mobile phone related crimes across the country."[64] SIM card owners were given the deadline of July 31, 2013 to register their cards with service providers, after which point unregistered cards would be disconnected.

Up until 2012, government monitoring of online communications did not appear to be widespread, though there had been instances in past years of e-mails, phone calls, and text messages belonging

---

[57] Jane Nishimwe, "Rwanda: Controversial 'Genocide Ideology' Law to Send More Rwandans Behind Bars," *Jambo News*, April 25, 2013, http://bit.ly/16DxMli.
[58] "Rwanda Parliament Votes to Amend Genocide Law," *Times Live*, July 17, 2013, http://www.timeslive.co.za/africa/2013/07/17/rwanda-parliament-votes-to-amend-genocide-law.
[59] *Emmanuel R. Karake, "Gov't Seeks to Amend Genocide Ideology Law," New Times, November 3, 2012, http://www.newtimes.co.rw/news/index.php?i=15165&a=60288.*
[60] Freedom House, "Rwanda," *Freedom of the Press 2013*, http://www.freedomhouse.org/report/freedom-press/2013/rwanda.
[61] "Rwanda: K Kohn Arrested Over Defamation," *Rwanda Show*, December 20, 2013, http://www.rwandashow.com/index.php/2012/12/rwanda-k-john-arrested-over-defamation/.
[62] Freedom House, "Rwanda," *Freedom on the Net 2012*, http://www.freedomhouse.org/report/freedom-net/2012/rwanda.
[63] Committee to Protect Journalists, "Journalists in exile 2012," June 19, 2012, http://www.cpj.org/reports/2012/06/journalists-in-exile-2012-crisis-in-east-africa.php.
[64] Nizon Segawa, "Rwanda Flags Off SIM Card Registration Exercise," *Chimp Reports*, February 4, 2013, http://www.chimpreports.com/index.php/news/news-as-it-happens-around-the-east-african-region/8072-rwanda-flags-off-sim-card-registration-exercise.html.

to opposition activists being produced as evidence in trials.[65] Worryingly in December 2012, the Rwandan parliament's lower house adopted amendments to the 2008 Law Relating to the Interception of Communications that authorize high-ranking security officials to monitor e-mail and telephone conversations of individuals considered potential threats to "public security."[66] Under the amended law, communications service providers are required to ensure that their systems have the technical capability to intercept communications upon demand and, according to a report from Privacy International, such interception technology may include the use of keyword scanning to identify certain topics of discussion.[67] While the law requires government officials to apply for an interception warrant, it also includes a provision that allows for a warrant to be issued verbally in urgent security matters, to be followed by a written warrant within 24 hours.[68] The amended law is awaiting senate approval as of April 2013.

Meanwhile, the Media High Council systematically monitors all print and broadcast media coverage during the country's annual genocide mourning period every April with the aim of "highlighting the civic contribution of the media during the commemoration period and discerning the extent to which media abide by legal and professional standards while covering genocide related issues."[69] The monitoring of online media was incorporated for the first time during Rwanda's 18th commemoration period in April 2012, which has led to a growing sense that the authorities may be monitoring other online communications as well.

There have been no reported cases of serious cyberattacks in the country, though the Rwandan police recently noted an increasing threat of cybercrime associated with expanding internet penetration across the country.[70] In 2010, RURA initiated a strategy to increase awareness of such threats among business owners and ordinary users.

---

[65] This was the case in the trial of opposition leader, Victoire Ingabire, during which e-mails and proof of money transfer to FDLR (French acronym for the Democratic Forces for the Liberation of Rwanda) rebels were used as evidence. These were mostly obtained via low-tech methods of confiscating suspects' mobile phones and computers rather than via service providers. See: Didas Gasana and Ann Garrison, "Ingabire trial: Rwanda prosecution fails 'evidence test,'" *Rwandinfo_ENG* (blog), accessed February 10, 2012, http://rwandinfo.com/eng/ingabire-trial-rwanda-prosecution-fails-evidence-test/.

[66] Sunny Ntayombya, "Proposed Communications Intercept Law: is our Privacy Adequately Protected," *New Times*, August 29, 2012, http://newtimes.co.rw/news/index.php?i=15099&a=57661.

[67] Carly Nyst, "Rwandan Government Expands Stranglehold on Privacy and Free Expression," Privacy International, August 25, 2012, https://www.privacyinternational.org/blog/rwandan-government-expands-stranglehold-on-privacy-and-free-expression#footnote2_4eosbda.

[68] "Online Freedoms in Rwanda," OpenNet Africa, accessed June 15, 2013, http://opennetafrica.org/dev/policy-and-legislation/rwanda/#fn-210-6.

[69] Media High Council, "Analysis of Media Coverage of the Eighteenth Commemoration of the Genocide Against the Tutsi in Rwanda," December 2012, http://bit.ly/16DxN8T.

[70] "Rwanda National Police Warns Internet Users Against Cybercrime," Rwanda National Police, October 17, 2012, http://www.scoop.it/t/african-internet/p/3006349174/rwanda-national-police-warns-internet-users-against-cyber-crime-rwanda-national-police.

SAUDI ARABIA

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	14	14
Limits on Content (0-35)	26	24
Violations of User Rights (0-40)	31	32
Total (0-100)	**71**	**70**

* 0=most free, 100=least free

POPULATION: 28.7 million
INTERNET PENETRATION 2012: 54 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The past year saw an increase in the use of Twitter and other social media to debate national issues and criticize government officials, contributing to the overall increase in activism and diversity of online content. Nonetheless, expressing negative views toward the royal family and Islam remained off limits (see **LIMITS ON CONTENT**).
- Harsh laws on libel and defamation have been consolidated through a series of government warnings directed at online speech (see **VIOLATIONS OF USER RIGHTS**).
- While the number of people arrested for their online activities has continued to grow, instances of physical attacks against users have decreased overall (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

In the wake of popular uprisings throughout the Arab world, the government of Saudi Arabia held tightly to power through the enforcement of strict limits on free speech and organized protest. The vulnerability of the country's existing social order has been most visible in the Eastern Province (*Ash-Sharqiyah*), where a continued crackdown on protesters belonging to the underrepresented Shi'a minority has led to over a dozen deaths.[1] Facebook groups calling for the release of prisoners of conscience list the names of hundreds of detained activists, though detailed figures for those arrested are not available. While the Ministry of Interior (MOI) has ostensibly claimed that only 2,221 Saudis were being held in prison as of March 2013,[2] others estimate the number at around 30,000, including hundreds of prisoners of conscience listed on Facebook groups.[3] While the recent wave of demonstrations has not changed the political landscape of Saudi Arabia as it has in other countries of the region, a notable rise in online activism throughout 2012 and early 2013 suggests that an increasing—though still limited—number of Saudis are no longer afraid to challenge the status quo.

Having first gained access to the internet in 1998, Saudis now go online from their home, place of employment, data-enabled mobile phones, and internet cafes. All forms of internet and mobile phone access are available in the country, including fiber-optic networks (FTTx), third-generation (3G) and fourth-generation (4G) mobile networks, internet via satellite, and High-Speed Packet Access (HSPA) technologies. Similarly, while Saudi Arabia is a regional leader in providing e-government services, authorities have looked to exploit technology to more disturbing ends as well.[4] For instance, in line with restrictions to Saudi women's freedom of movement imposed in November 2012, a woman's male "guardian" is alerted by text message when she presents herself at the airport to ensure that she has gained permission to leave the country.[5] While the government is keen to use ICTs to enforce strict social norms and monitor its users, public figures and religious authorities continue to warn citizens against the "evils" of social media and other online tools. In March 2013, uproar over numerous defamation cases led the Grand Mufti to criticize Twitter as a "council of clowns" made up of users who "unleash unjust, incorrect and wrong tweets."[6]

Social media has come to play an increasingly crucial role in the country. Saudis have employed online tools to highlight corruption, discuss sensitive issues of national relevance, and demand the release of prisoners of conscience. However, as the use of Twitter has skyrocketed, so have

[1] "Questions over Death of Protester in Saudi Arabia's Eastern Province," Al-Monitor, January 23 2013, http://www.al-monitor.com/pulse/politics/2013/01/peaceful-protestor-killed-in-saudi-arabia.html.
[2] "Ministry's appeal: Ignore rumors, maintain peace", Arab News Newspaper, March 8, 2013, http://www.arabnews.com/saudi-arabia/ministry%E2%80%99s-appeal-ignore-rumors-maintain-peace
[3] "Saudi Arabia show of force stifles 'day of rage' protests", BBC, December 27, 2012, http://news.bbc.co.uk/2/hi/programmes/newsnight/9422550.stm.
[4] , United Nations, "United Nations E-Government Survey 2012," December 26, 2012, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf.
[5] "'Where's my wife?' Electronic SMS tracker notifies Saudi husbands", AlArabiya, December 27, 2012, http://english.alarabiya.net/articles/2012/11/22/251255.html.
[6] "Twitter is for clowns: Saudi Arabia's Grand Mufti", AlArabiya, March 23, 2013, http://english.alarabiya.net/en/2013/03/23/Twitter-is-a-council-of-clowns-Saudi-Arabia-s-Grand-Mufti-.html

government efforts to monitor and in some cases detain users for tweeting about sensitive aspects of Islam or the Saudi monarchy. Although the government has spoken of the difficulties of monitoring Twitter,[7] in early 2013 it conducted an experiment in which it temporarily blocked millions of Twitter pages.[8] There is no doubt that these measures have been very effective in quelling any movements that could potentially challenge the monarchy's absolute grip on political power and the overriding social order.

OBSTACLES TO ACCESS

Saudis have enjoyed a rapid growth of internet and communications technologies in recent years. Access had increased to 54.1 percent of the population, or 15.8 million users, by the end of 2012, up from 20 percent in 2006.[9] Fixed broadband use stands at 40.8 percent of all connections, while less than 20 percent of subscribers still use a slower dial-up service.[10] WiMAX, a prepaid technology that allows users to access broadband internet wirelessly from any location through a USB modem, is widely used in Saudi Arabia due to its affordability.

Similarly, standard mobile phone subscriptions have almost tripled since 2006, rising to 53.1 million subscriptions in use as of February 2013.[11] This represents a penetration rate of 181.6 percent[12] or an estimated average of 4.6 mobile lines per household.[13] Finally, 86 percent of mobile subscriptions are prepaid, while 42.1 percent are mobile broadband connections.[14]

Connection speeds for broadband users generally vary between 724 Kbps and 1.22 Mbps, depending on the service package. According to a recent survey, a majority of those questioned were not satisfied with their connection speeds or with prices.[15] Monthly expenditure on broadband service ranges from between SAR 42 ($11) and SAR 334 ($89),[16] representing a sharp drop from the 2003 price of SAR 700 ($187) per month.[17] One Gigabyte (GB) of prepaid broadband starts at SAR 100 ($26) per month, while an unlimited internet connection for three months costs SAR 333 ($89).[18]

[7] "Govt monitoring of Twitter 'too difficult'", Arab News Newspaper, February 13, 2013, http://bit.ly/VY61Je.
[8] "Saudi Authorities performs an experiment to block millions of Twitter links" [in Arabic], Anhri.net, March 6, 2013, http://www.anhri.net/?p=72079.
[9] CITC, "ICT Indicators Report – 2012," http://bit.ly/18zqBbV.
[10] CITC, "ICT Indicators Report – 2012."
[11] CITC, "ICT Indicators Report – 2012."
[12] CITC, "ICT Indicators Report – 2012."
[13] "The State of ICT Market Development in Saudi Arabia," Kingdom of Saudi Arabia, 2010, CITC, December 23, 2012 , http://bit.ly/HPUZyN.
[14] CITC, "ICT Indicators Report – 2012."
[15] CITC, "The State of ICT Market Development in Saudi Arabia." Those surveyed were predominantly male (95 percent) and between the ages of 20 and 39 (83 percent).
[16] CITC, "The State of ICT Market Development in Saudi Arabia."
[17] "User's Survey", Internet Services Unit (ISU), King Abdulaziz City for Science & Technology, 2006, http://www.isu.net.sa/surveys-&-statistics/new-user-survey-results.htm.
[18] Mobily, "Connect", http://bit.ly/JkA07w.

Overall, infrastructure is not considered a major barrier to access except in remote and sparsely populated areas. Internet penetration is highest in major cities such as Riyadh and Jeddah, as well as in the oil-rich Eastern Province. Residents of provinces such as Jizan in the south and Ha'il in the north are the least likely to use the internet, while young Saudis make up the majority of the user population throughout the country.[19] Arabic content is widely available, as are Arabic versions of applications such as chat rooms, discussion forums, and social media sites.

Saudi Arabia is connected to the internet through two country-level data services providers, the Integrated Telecom Company and Bayanat al-Oula for Network Services, up from a single gateway in years past. These servers, which contain long lists of blocked sites, are placed between the state-owned internet backbone and global servers. All user requests that arrive via Saudi internet service providers (ISPs) travel through these servers, where they can be filtered and possibly blocked. The authorities blocked the Voice over Internet Protocol (VoIP) application Viber three months after warning that VoIP and internet messaging services may be blocked if they do not meet regulatory standards (for more on internet censorship, see "Limits on Content").[20]

The two country-level service providers offer services to licensed ISPs, which in turn sell connections to dial-up and leased-line clients. The number of ISPs in the country has risen from 23 in 2005 to 36 in 2011.[21] Broadband and mobile phone services are provided by the three largest telecommunications companies in the Middle East: Saudi Telecom Company (Saudi Arabia), Etisalat (United Arab Emirates), and Zain (Kuwait).

Internet cafes, once prevalent in the country, have become less popular in recent years due to the broad availability and affordability of home broadband access. With the departure of many power users, internet cafes are now mainly used by youth from lower socio-economic backgrounds to congregate and socialize. Due to a mandate[22] issued by the Ministry of Interior (MOI) on April 16, 2009,[23] all internet cafes must close by midnight, compliance of which is ensured by the police. These measures were ostensibly designed to crack down on internet use by extremists, but in practice they allow the police to deter any activity that the government may find objectionable. Conversely, coffee shops have grown in popularity among business people, young adults, and single males, who enjoy free Wi-Fi access with their paid beverages.

Previously, all internet governance fell under the purview of the Internet Services Unit (ISU), a department of the King Abdulaziz City for Science & Technology (KACST). Established in 1998 and reporting directly to the Vice President for Scientific Research Support of KACST, the ISU now only provides internet access to government departments, as well as Saudi research and

[19] CITC, "The State of ICT Market Development in Saudi Arabia."
[20] "CITC blocks Viber", Saudi Gazette, June 5, 2013, http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentid=20130605168659
[21] CITC, "Annual Report, 2011" [in Arabic], Kingdom of Saudi Arabia, 2012, http://www.citc.gov.sa/arabic/MediaCenter/Annualreport/Documents/PR_REP_007.pdf.
[22] For more information on this mandate, please refer to [Arabic] http://www.okaz.com.sa/okaz/osf/20090416/Con20090416271112.htm.
[23] "New hidden camera rule for Internet cafés", Saudi Gazette, April 16, 2009, http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentID=2009041635209

academic institutions.[24] In 2003, the Communication and Information Technology Commission (CITC) became responsible for providing internet access to the private sector.

The CITC establishes policies and enforces the regulations on the country's information and communication technology (ICT) services, including duties such as managing tariffs, performing content filtering, and licensing providers.[25] Under the 2007 Anti-Cyber Crime Law, the CITC also assists the Ministry of Interior (MOI) in monitoring extremists and political activists.[26] While both the CITC and KACST claim to enjoy administrative and financial independence, there is no evidence to support this. On the contrary, the CITC chairman is also the Minister of Communications and Information Technology, while the KACST President reports directly to the Prime Minister and is appointed by the King. Board members consist of government officials, appointed to these roles on the basis of their position within the government.

LIMITS ON CONTENT

The Saudi government continued to employ strict filtering over internet content throughout 2012 and early 2013. Sites that are judged to contain "harmful," "illegal," "anti-Islamic," or "offensive" material are routinely blocked, including pages related to pornography, gambling, and drugs. While part of the government's blocking policy is designed to disrupt terrorist networks and the dissemination of extremist ideology, the government also blocks any content that it deems harmful to society or challenging to the royal family. Criticism of Saudi Arabia, the royal family, or other Gulf Arab States is not tolerated, in addition to sites that organize political opposition or question the ruling family's strict conception of Islam.[27] The extensive list of sites blocked under these policies is supplemented by an additional list formulated from recommendations of the public.[28] In early 2013, the government also temporarily blocked millions of Twitter pages in an experiment to test its capabilities.[29]

Websites and social media pages belonging to human rights or political organizations, such as the Saudi Civil and Political Rights Organization (ACPRA) and the Arab Network for Human Rights Information (ANHRI), are blocked.[30] Sites belonging to several Saudi religious scholars and dissidents are blocked,[31] as well as those related to the Shi'a religious minority, such as

[24] "ISU History", KACST, March 2, 2013, http://www.kacst.edu.sa/en/depts/isu/Pages/about.aspx
[25] "CITC Roles and Responsibilities", CITC, March 2, 2013, http://www.citc.gov.sa/English/AboutUs/AreasOfwork/Pages/default.aspx
[26] Anti-Cyber Crime Law, MOI [in Arabic], March 2, 2013, http://bit.ly/19JUq7S.
[27] "The censorship policy of websites that spread extremist ideologies has proven its success"[in Arabic], AlArabiya.Net, December 22, 2012, http://www.alarabiya.net/articles/2012/05/29/217356.html.
28 "General Information on Filtering Service", Internet.gov.sa, June 22, 2013 http://www.internet.gov.sa/learn-the-web/guides/content-filtering-in-saudi-arabia
[29] "Saudi Authorities performs an experiment to block millions of Twitter links" [in Arabic], Anhri.net, March 6, 2013, http://www.anhri.net/?p=72079.
[30] According to the Alkasir.com, which provides information on blocked websites, the URLs acpra6.org and anhri.net are blocked in Saudi Arabia. See https://alkasir.com/map, accessed March 2, 2013.
[31] Blocked websites of Saudi religious scholars include: www.almoslim.net, www.albrrak.net, and islamqa.info/ar. "Blocking some sites because they violate rules and spread bold ideas and theses" [in Arabic], AlArabiya.net, April 6, 2012, http://www.alarabiya.net/articles/2012/04/06/205754.html.

Rasid.com,[32] Yahosein.org, and Awamia.net.[33] Authorities also block the website of the Islamic Umma Party, the country's only underground (and illegal) political party, which has called for the royal family to step down in return for a safe exit.

The CITC also censors individual social media pages that demand political reforms or basic civil rights. These include the Facebook pages of Abdullah al-Hamid and Mohamed Saleh al-Bejadi, well-known Saudi human rights activists and co-founders of the ACPRA,[34] as well as the Twitter accounts of the Saudi journalist and blogger Hassan Almustafa,[35] Saudi human rights activist and blogger Nouf Abdulaziz,[36] Saudi journalist and political activist Muhana al-Hubail, and the head of the organization "Monitor of Human Rights in Saudi Arabia" Waleed Abo al-Khair.[37]

Authorities have also occasionally moved to block entire online products and services for breaching the country's strict laws. In September 2012, the government threatened to block all of YouTube if Google did not restrict access to the controversial "Innocence of Muslims" video containing an offensive depiction of the Prophet Mohamed. Google later blocked the video in Saudi Arabia.[38] The CITC also has an aggressive stance toward VoIP services that circumvent the country's regulatory environment and, by some indication, the surveillance apparatus. So far only Viber has been blocked, though authorities have threatened to institute further restrictions.[39] BlackBerry services were temporarily stopped on June 30, 2012 following glitches experienced by the BlackBerry maker Research in Motion, according to Saudi Telecom Company (STC). There was no evidence to suggest that the government was behind the short suspension.[40]

In 2011, legislation was passed requiring that the owners of online news sites obtain a license from the Ministry of Culture and Information.[41] While not all blogs and websites have complied with this legislation, those that did not register with the ministry risk the possibility of closure at any time. Numerous sites have been closed for copyright violations[42] or for featuring advertisements for drugs.[43] In addition, several political opposition websites such as Humanf.org, Saudihr.org, Hummum.net, and Alwaqa.com have ceased operations over the past year, presumably because of pressure from the MOI. Reacting to a court verdict, in December 2012 the Ministry of Culture and

[32] "A list of blocked sites from within Saudi Arabia" [in Arabic/English], Adala Center], December 22, 2012, http://www.adalacenter.net/?act=sec&pg=39.
[33] https://alkasir.com/map viewed March 2, 2013
[34] "A list of blocked sites from within Saudi Arabia" [in Arabic/English], Adala Center,],December 22, 2012, http://www.adalacenter.net/?act=sec&pg=39.
[35] See http://hasantalk.com.
[36] See http://nofah.com/wordpress/.
[37] See https://twitter.com/abualkhair.
[38] "YouTube blocks 'Innocence of Muslims' in Saudi Arabia", AlArabiya.net, September 19, 2012, http://english.alarabiya.net/articles/2012/09/19/238987.html.
[39] "CITC blocks Viber", Saudi Gazette, June 5, 2013, http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentid=20130605168659
[40] "STC: BlackBerry service stoppage problem solved and service to return progressively" [in Arabic], Al-Madina Newspaper, June 30, 2012, http://www.al-madina.com/node/387238?liv.
[41] "Internet Enemies, Saudi Arabia," Reporters Without Borders, 2012, http://bit.ly/JrLevJ.
[42] "CITC closed down Haraj site after advertising half kilo Hashish", [in Arabic], AlSharq Newspaper, March 30, 2013, http://www.alsharq.net.sa/2013/03/30/783097
[43] "Saudi Arabia closes 52 sites violated intellectual property copyrights" [in Arabic], Ameinfo.com, October 16, 2012, http://www.ameinfo.com/ar-248952.html

Information also closed down an online discussion forum, "the Global Club," after a sports journalist who rooted for al-Nassr soccer team complained that forum members had been verbally abusing him and his family.[44]

There were several incidents in which pressure from social media users and online newspapers led to users deleting "controversial" tweets, disassociating themselves from their accounts, or even deleting their accounts. For instance, Twitter user Hesaah al-Sheikh disassociated herself from her account after public anger erupted over her tweet in which she equated listening to the singer Mohamed Abdo as listening to Allah.[45] Disassociating oneself from a Twitter account is common in Saudi Arabia, particularly when simply deleting a controversial tweet is not enough to calm public anger. Users who are deemed to have acted inappropriately often publicly declare that the account does not belong to them and that another user is using their name to impersonate them, a common occurrence in Saudi Arabia.[46]

Similarly, the government also responds to take-down notices from members of the public, who can use a web-based form to submit a complaint regarding undesirable material.[47] Sites can also be unblocked through a similar process.[48] Once an individual completes such a request, a team of CITC employees determines whether the request is justified. The manager of public relations at the CITC said the commission receives about 200 requests each day, though he would not comment on how often the CITC unblocks a site based on such an appeal.[49] In one example, the CITC unblocked the website "Mustamel" after the owners obeyed a request from the CITC to remove illegal advertisements.[50]

The government is somewhat transparent about what content it blocks. Users who attempt to access a banned site are redirected to a page displaying the message, "Access to the requested URL is not allowed!" Still, a full list of banned sites is not publicly available. The country's two data service providers must block all sites banned by the CITC,[51] and failure to abide by these bans may result in a fine of up to SAR 5 million ($1.33 million), according to Article 38 of the Telecommunication Act.[52] It should be noted, however, that many Saudi internet users have become savvy at using circumvention tools such as Hotspot Shield, which allows users to access a virtual private network (VPN) to bypass censorship.[53]

---

[44] "A Nasrawi journalist won his case against an online discussion forum" [in Arabic], Sabq.org, December 27, 2012, http://sabq.org/a7ifde.
[45] "Writer Hessa Al-Sheikh explains to 'Sabq': Twitter account impersonated my personality" [in Arabic], Sabq.org, December 26, 2012, http://sabq.org/Uuhfde.
[46] "Saudi Minister of Culture and Information criticizes impersonation of intellectuals" [in Arabic], AlArabiya.net, March 2, 2013, http://www.alarabiya.net/articles/2012/11/20/250707.html
[47] The CITC block-request form is available at http://bit.ly/aRBpYa.
[48] The CITC unblock request form is available at http://www.internet.gov.sa/resources/block-unblock-request/unblock/.
[49] "About 300,000 requests to block sites in Saudi Arabia annually" [in Arabic], Ajl.com.sa, January 13, 2010, http://www.burnews.com/news-action-show-id-12100.htm.
[50] "For the second time Haraj site blocked in Saudi Arabia" [in Arabic], Qbas, March 26, 2013, http://qbas.org/home/news.php?action=show&id=3585
[51] CITC, "General Information on Filtering Service," September 30, 2010, http://bit.ly/yhOPwD.
[52] Telecommunication Act found here [in Arabic]: http://bit.ly/16Jzjj5.
[53] Saudis refer to this circumvention tool as a "proxy breaker."

In addition to government censorship, self-censorship by online journalists, commentators, and social media users is widespread. For example, the owner of the popular "3al6ayer" YouTube channel admitted that he avoids crossing certain "red-lines" over fears of "getting into trouble with the authorities."[54] Online commentators who express support for extremism, liberal ideals, minority rights, or political reforms, in addition to those who expose human rights violations, are closely monitored and often targeted by the government. Questioning religious doctrine is strictly taboo, particularly content related to the Prophet Mohamed.

These limitations are compounded by the self-censorship that online news moderators and site owners must exercise. Gatekeepers frequently delete user-generated content that could be deemed inappropriate or inconsistent with the norms of society, as they can be held legally liable for content posted on their platforms.[55] In one case that highlights the degree to which moderators pre-censor, user comments on the news site Sabq.org were full of praise for the poem "al-Haboob," written by Prince Khalid al-Faisal, even though it was clear from Twitter that the majority of Saudis were making fun of him.[56]

The recent amount of controversial tweets that have been reported may reflect a decrease in Saudis' willingness to censor themselves over Twitter. Indeed, many readily take to social networks to criticize problems in the country or government ministers so long as no references are made to the king or to religion. Users often employ hashtags to inspire a national debate on a certain political issue, including the tags "Breaking the fences"[57] and "elected Consultative Council" to expose corruption by public officials or call for reforms.[58] Prominent religious scholars, such as al-Awdah, have even contributed to these debates on Twitter.[59]

With so much activity occurring on social networks, the Saudi government maintains an active presence online as a means of manufacturing consent for its policies. It is believed the government employs an "electronic army" to constantly post progovernment views, particularly on social media. Progovernment trolls have taken to "hashtag poisoning," a method of spamming a popular hashtag in order to disrupt criticism or other unwanted conversations through a flood of unrelated or opposing tweets. Through the use of a "bot," such as those provided by Yoono.com, one individual can send thousands of tweets to a hashtag at the same time.[60] While the tweet may contain the same message, the bot sends the tweet on behalf of numerous fabricated accounts, created by combining random photos of faces with names searched from the internet. The

[54] "Idaat with Turki Al Dakheel" [in Arabic], AlArabiya.net, May 18, 2012, http://bit.ly/LdV6EO.
[55] "Raif Badawi's wife provides "Anhaa" with the list of charges against her husband and calls for his release [in Arabic], Anhaa, April 25, 2013, http://www.an7a.com/102662.
[56] "'Al-Haboob'by Khalid Al-Faisal received high praise and harsh criticism on Twitter" [in Arabic], Sabq.org, January 1, 2013, http://sabq.org/IWtfde.
[57] #الشبوك_تحطيم
[58] #مجلس_شورى_منتخب
[59] "Salman Al-Awdah calls for an elected Consultative Council in Saudi Arabia [in Arabic], Watan.com, December 29, 2012, http://www.watan.com/news/world-news/2012-12-29/18048.
[60] "Fake accounts and drowning the hashtag in Twitter [in Arabic], Osama Al Muhaya, March 16, 2013, http://osamh.me/blog/wp-content/uploads/2013/03/twitterstudy.pdf

government also influences online news reporting by offering financial support to news sites such as Sabq.org and Elaph.com in return for coordination between site editors and the authorities.[61]

Whereas the authorities provide monetary support to progovernment websites, the owners of opposition websites can come under strong financial pressures as a result of the country's environment of censorship. Revenue from third-party advertisers can be heavily impacted by a government decision to block a website. The government can also request advertisers to cancel their ads on a particular website in order to pressure the website to close. Restrictions on foreign funding further inhibit the sustainability of websites that are critical to the ruling system.

Whereas opposition blogs and online forums were once the main instrument for discussing political and social matters, most Saudis now use social media to share information and express opinions. According to Abdul Rahman Tarabzouni, the Head of Emerging Arabia at Google, Saudis collectively watch 190 million YouTube videos per day, the highest amount of views per capita of any country in the world.[62] There are now dozens of comedic channels on YouTube, the most popular being "Eysh Elly," "La Yekthar," and "3al6ayer," which respectively have around 126 million, 51 million, and 39 million total views.[63] One reason for the success of these videos is their engagement in cautious rather than harsh criticism and their restraint against pushing the limits too far.

Similarly, Twitter continued to grow as a platform for expressing sensitive issues. Indeed, when interviewed, one Saudi described the country's Twitter environment as a sort of virtual parliament "where people from all political sides meet and speak freely."[64] Saudis are the largest adopters of Twitter in the Arab world, with the number of users reaching 2.9 million, or slightly over 10 percent of the population, as of October 2012.[65] Facebook is the third most visited site in the country[66] with 5.9 million local users, or 23 percent of the population.[67] A myriad of Facebook groups have been recently active in organizing low-level demonstrations in cities throughout the country.[68] The banned Islamic Umma Party also uses its official website to call for sit-ins and protests. While disparate protests do occur, these demonstrations generally have low attendance and do not lead to substantial political or social changes.

---

61 "Othman Al-Omair in Turning Point 8-5" [in Arabic] MBC (YouTube), December 24, 2012, http://www.youtube.com/watch?feature=player_embedded&v=r9oqwtWiSYA.

62 "The emergence of Google", Arab News Newspaper, November 27, 2012, http://www.arabnews.com/emergence-google.

63 Other popular channels include 'Quarter to Nine,' 'Sa7i,' 'Masameer,' 'Eysh Elly,' 'Fe2aFala,' 'Hajma Mortadda' 'Just For Wanasah,' and 'Eysh Sar Fi Twitter.' "Twitter usage in KSA grows '10 times' the world average," *Saudi Gazette*, January 6, 2013, http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentid=20130106148256.

64 "Twitter Gives Saudi Arabia a Revolution of Its Own," Robert F. Worth, The New York Times, October 20, 2012, http://nyti.ms/ORCPoc.

65 "Saudis Cross Social Boundaries on Twitter", New York Times, October 20, 2012, http://nyti.ms/S3hBS7.

66 "Twitter usage in KSA grows '10 times' the world average," *Saudi Gazette*, January 6, 2013, http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentid=20130106148256.

67 "Facebook Statistics by country," Socialbakers, December 23, 2012, http://bit.ly/fyo6Id.

68 These include 'Islamic Umma Party', 'Kulna Hasm' (which is associated with 'Saudi Civil and Political Rights Association'), "Rajab Revolution 1432 in Holly Mosques Land", "Day of Anger in Saudi Arabia", "the coalition of free youth", "The national campaign for supporting detainees in Saudi Arabia", and "The Coordinating Committee for the Youth movement in Saudi Arabia".

However, more recently, the robustness of security forces in dismantling demonstrations has forced many Saudis to devise more creative forms of organized protest. Facebook is commonly used to specify the date, time, and place a protest or sit-in will take place, while YouTube has been instrumental in documenting the demonstrations and attracting media attention.[69] Videos documented a protest on June 6, 2012, in which a group of detainees' families carried out a demonstration inside a shopping mall after initially pretending to be regular customers.[70] Later that summer, demonstrators "marched" together in their cars on a highway.[71] In March 2013, 182 family members, including 15 women and 6 children, participated in a 12-hour sit-in in the central city of Buraidah. Police arrested 161 of the protestors[72] and blamed social media for stirring up the protests (for more on the arrests of users, see "Violations of User Rights").[73]

In addition to documenting protests, users secretly film officials engaging in inappropriate behavior at work. Footage is uploaded to YouTube and then disseminated via Twitter. In a recent case from December 2012, Abdullah al-Sheri (@Abdula73), a Saudi doctoral student in the United States, tweeted out the names of dozens of high-profile Saudi citizens who had obtained fake post-graduate university degrees. By matching information in the public domain against a Ministry of Higher Education list of universities that offer fictitious qualifications, al-Sheri was able to back up his claims with evidence.[74] His tweets caused a huge uproar, attracting media attention and putting pressure on the Consultative Council (*Majlis al-Shura*) to enact laws that would deter businesses from dealing with fictitious universities and punish those who obtained fake degrees.[75] Significantly, no complaint has been lodged against al-Sheri for his actions thus far.

Similarly, the anonymous Twitter user "@Mujtahidd" continues to criticize high profile members of the royal family[76] and to provide detailed descriptions of state corruption.[77] The popularity of the account has more than doubled over a short period, increasing from around 410,000 Twitter followers in June 2012 to over 960,000 as of March 2013.[78] More recently in 2013, he shared the tweets of dozens of users who defended the government using the exact same wording, thus evidencing the presence of an MOI Twitter army.[79] Due to his insider knowledge, the person(s) behind the Mujtahidd account is believed to be a disgruntled member of the Saudi royal family.

---

[69] "Ministry's appeal: Ignore rumors, maintain peace", Arab News Newspaper, March 8, 2013, http://bit.ly/1eQ61Z0.
[70] "Saudi activists stage rare protest march in Riyadh", USA Today, June 7, 2012, http://usat.ly/16TutAS.
[71] e3teqal YouTube Channel (http://www.youtube.com/user/e3teqal/videos), August 1, 2012, http://www.youtube.com/watch?v=VKF0MPbiRxY
[72] "161 arrested in Buraidah", Arab News Newspaper, March 2, 2013, http://bit.ly/1azlEz2.
[73] Angus McDowall, "Saudi accuses activists of lying to stir protests," Reuters, March 7, 2013, http://reut.rs/Z39vMW.
74 "The fictitious qualifications scandal" [in Arabic], Alriyadh Newspaper, November 30, 2012, http://bit.ly/UfQyUS.
[75] "Defaming 'fake degrees' holders puts pressure on Al-Shura to implement more deterrent laws" [in Arabic], AlSharq Newspaper, December 27, 2012, http://www.alsharq.net.sa/2012/12/22/637690.
[76] "Twitter Gives Saudi Arabia a Revolution of Its Own", York Times, December 27, 2012, http://nyti.ms/RmDtYD.
[77] "Mujtahidd," Twitter, accessed on February 12, 2013. http://bit.ly/MtgI50.
[78] " 'Mujtahidd' exposes secrets of Saudi royal family on Twitter," LBC International, June 24, 2012, http://www.lbcgroup.tv/news/37984/mujtahidd-exposes-secrets-of-saudi-royal-family-on
[79] https://twitter.com/assaflovhotmail/status/307325546847694848/photo/1.

VIOLATIONS OF USER RIGHTS

The legal environment surrounding online expression remains a significant impediment to internet freedom in Saudi Arabia. While there have been no reported instances of users being physically attacked for online posts over the past year, authorities have become more proactive in prosecuting citizens using the country's restrictive laws. The MOI has introduced a new method for users to report offensive comments made toward them by other users, opening the door for an upsurge in defamation lawsuits that may ultimately have repercussions for freedom of expression. Overall, the MOI continues to enjoy relative impunity over its abuses of online users. Some have reported that authorities have confiscated their cars, computers, and other personal items indefinitely. Online commentators are often detained without specific charges and denied the right to an attorney. New registration requirements have also harmed the safety of using ICT tools anonymously and free from government interference.

The Basic Law of Saudi Arabia contains language that calls for freedom of speech and freedom of the press, but only within certain boundaries. The 2000 Law of Print and Press also addresses freedom of expression issues, though it largely consists of restrictions rather than protections. Online journalists employed at newspapers and other formal news outlets maintain the same rights and protections as print and broadcast journalists, and like their counterparts, are also subject to close government supervision. Similarly, laws designed to protect users from cybercrimes also contain clauses that limit freedom of expression. The 2007 Anti-Cyber Crime Law assigns jail sentences and fines for defamation; the unauthorized interception of private e-mail messages; the hacking of a website to deface, destroy, modify, or deny access to it; or simply the publishing or accessing of data that is "contrary to the state or its system."[80]

In late 2012, after an upsurge in defamation cases stemming from Twitter and the popular messaging service WhatsApp, the CITC deployed a large-scale media campaign to remind Saudis that "anyone who re-sends messages (via mobile phones and smart phone applications) that violate the sanctity of the private lives of citizens through insult, mockery, and violation of the sanctity of public morals, religious values and public order, will be sentenced to five years in jail, in addition to a fine of SAR 3 million ($800,000)."[81] On August 8, 2012, the MOI also introduced a new web-based form on its official website allowing internet users to complain about offensive comments made online about them.[82]

Many online commentators have been imprisoned for publicly defaming other citizens. For example, a 25-year-old man was sentenced to four months and fined SAR 10,000 ($2,666) by a court in the Eastern city of al-Qatif for publicly vilifying and defaming another man on Twitter after

[80] http://bit.ly/VWXEmI.
[81] "Privacy violators on Web face tough punishments", Arab News Newspaper, December 27, 2012, http://www.arabnews.com/privacy-violators-web-face-tough-punishments.
[82] "'Interior' confronts social networking sites abuse.. electronically", [in Arabic], Aleqtisadiah Newspaper, March 9, 2013, http://www.aleqt.com/2012/08/08/article_681378.html

a dispute erupted between the two.[83] Significantly, laws regarding libel and defamation are not equally applied when it comes to the country's Shi'a minority. For example, after a prominent Saudi lawyer insulted Shi'as on Twitter by claiming that they are the "children of adultery and of unknown descents," authorities did not act to arrest him. Over ten thousand citizens in the Eastern province had signed a petition to call for a lawsuit against him.[84]

Twitter users who expose the misdeeds of government officials or public sector employees are often targeted by authorities. While there were no charges issued against al-Sheri for exposing the fake university qualifications of government officials (see "Limits on Content," above), authorities arrested an undisclosed Twitter user in late 2012 for frequently criticizing known public figures.[85] While the government stated that the user is a former public official, Twitter users believed that the user in question was @Saryat_Aljibal and discussed the user's arrest using a Twitter hashtag. The account—well-known for frequently criticizing the President of the Royal Court—disappeared from followers' lists around the same time as the news of the arrest.[86]

In September 2012, Bader Thawab (@Bader Thawab) was arrested after tweeting "down with the House of Saud." He was put on trial in early 2013 for using social media to disturb "national unity," among other charges.[87] Prominent writer Turki al-Hamad was also arrested in December 2012 after tweeting "…we need someone to rectify [the Prophet] Mohamed bin Abdullah's doctrine."[88] Any discussion that questions an aspect of how Islam is practiced in society commonly leads to arrest. The incident inspired its own hashtag on Twitter and drew large amounts of both support and criticism. After five months in detention, al-Hamad was finally released on June 5, 2013.[89]

Following the latest wave of low-level demonstrations in the country, the number of online political activists that have been arrested has increased significantly. On March 9, 2013, a court in Riyadh disbanded the human rights organization ACPRA and sentenced two of its members, Abdulah al-Hamid and Mohammed al-Qahtani, to 11 years and 10 years of jail time respectively, in addition to a travel ban equal in length to their jail sentences.[90] Five years of their sentences were based on Article 6 of the Anti-Cyber Crime Law, relating to the creation of a website that could disturb social order.[91] Five founding members of ACPRA are also currently in detention.[92] Two founding members of the Islamic Umma Party', al-Wahiby and al-Gamidi,[93] have been in prison

[83] "Jailing a Saudi youth and fining him SAR 10000 because of 'Twitter'" [in Arabic], Alarabiya.net, December 27, 2012, http://www.alarabiya.net/articles/2012/09/16/238303.html.
[84] "Bin Zahim Recedes and Shiites Refuse to Step Down", Saudi Shia, April 24, 2012, http://saudishia.com/index.php?act=artc&id=281&hl=sultan
[85] "Riyadh Security (authorities) toppled a Twitter user from those threaten public order" [in Arabic], Sabq.org, December 27, 2012, http://sabq.org/2iqfde.
[86] http://bit.ly/1azm6NT.
[87] "Saudi Charged for "Down with the House of Saud" Tweet", GlobalVoices, February 16, 2013, http://bit.ly/Xfj7UE.
[88] "As ordered by the Minister of Interior. Turki Al-Hamad arrested because of his "offensive tweets" against doctrine" [in Arabic], Sabq.org, December 24, 2012, http://sabq.org/Ygtfde.
[89] "Turki Al-Hamad released after 5 months from his dentition" [in Arabic], Sabq.org, June 5, 2013, http://sabq.org/O65fde.
[90] "10 years jail for Al-Qahtani and 11 for Al-Hamid in the ACPRA case" [in Arabic], Sabq.org, March 9, 2013, http://sabq.org/onyfde.
[91] Anti-Cyber Crime Law, MOI [in Arabic], March 2, 2013, http://bit.ly/19JUq7S.
[92] Those members are Suliaman Al-Rushoody, Mansour Al-Awth, Mousa Al-Garni, Mohamed Al-Bijadi and Saleh Al-Ashwan.
[93] Islamic Umma Party page on Twitter, [in Arabic], December 22, 2012, http://twitter.com/islamicommapart.

since February 2011.[94] Both the ACPRA and the Islamic Umma Party base many of their operations online.

In the most high-profile cases from the past, Hamza Kashgari and Raif Badawi continue to be held on charges related to their online activities. Kashgari, a young Saudi writer, published three tweets detailing an imaginary conversation with the Prophet Mohammed on February 4, 2012, causing tens of thousands of Twitter and Facebook users to call for his execution. King Abdullah reportedly ordered his arrest on charges of "disrespecting Allah" and "insulting the Prophet."[95] After fleeing the country, he was immediately extradited from Malaysia despite pressure from international human rights groups.[96] The decision was heavily shrouded in controversy, as Malaysian authorities denied him access to his lawyers and refused requests from the United Nations Refugee Agency (UNHCR) to interview him.[97]

In the case of Raif Badawi, authorities have targeted the "Free Saudi Liberals" website co-founder repeatedly since March 2008, when he established the forum for discussing political and religious topics. He was arrested on June 17, 2012 and initially faced up to five years in prison and a hefty fine for "insulting Islam through electronic channels" and "going beyond the realm of obedience." However, in December 2012 a court elevated the charge to apostasy, which is punishable by death.[98] While the apostasy charge has since been dropped, Badawi is still in prison facing other charges. [99]

As previously mentioned, the Ministry of Culture and Information requires that all blogs, forums, chat rooms, and other sites obtain a license from the Ministry to operate online, thus putting more pressure on online writers to self-regulate their content.[100] While the law has not yet been widely enforced, it is a serious threat to anonymity online. Users are also legally required to use their real names and register with the government when purchasing mobile phones. In 2012, the CITC introduced a new law making it mandatory to enter a user's ID number to recharge a prepaid mobile card, rendering it virtually impossible to use prepaid mobile phones anonymously.[101] Nevertheless, a black market has since emerged in which vendors sell new SIM cards and prepaid refill cards with pre-existing ID numbers.[102] To stop this lucrative practice, the government is now considering linking these cards to fingerprints.[103]

---

[94] Islamic Umma Party official webpage, [in Arabic], March 10, 2012, http://www.islamicommaparty.com/Portals/default/
[95] Tehmina Kazi, "Those who threated 'Twitter blasphemy' writer Hamza Kashgari should stop and remember what Islam is for," *The Guardian*, 17 February 2012, http://bit.ly/zsZOyo.
[96] "Malaysia deports Saudi in Twitter posts row," Al-Jazeera English, 13 February 2012, http://aje.me/wCHThO.
[97] "Saudi Arabia: Writer Faces Apostasy Trial," Human Rights Watch, 13 February 2012, http://bit.ly/xZmdHx.
[98] "Saudi Arabia: Website Editor Facing Death Penalty", Human Rights Watch, December 27, 2012, http://www.hrw.org/news/2012/12/22/saudi-arabia-website-editor-facing-death-penalty, and "Saudi Arabia: Free Editor Held Under Cybercrime Law," Human Rights Watch, July 17, 2012, http://bit.ly/Pb4Oxy.
[99] "Apostasy Case against Saudi Activist Dismissed", GlobalVoices, January 23, 2013, http://bit.ly/149EutE.
[100] "Internet Enemies, Saudi Arabia," Reporters Without Borders, 2012, http://bit.ly/JrLevJ.
[101] "User's ID number now required to recharge prepaid mobile phones", Arab News, July 4, 2012, http://bit.ly/1azmvzS.
[102] "Black market for SIM cards with ID thriving", Saudi Gazette Newspaper, December 31, 2012, http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentid=20121231147657
[103] "Study to link SIM cards with fingerprints", Arab News Newspaper, June 20, 2013, http://www.arabnews.com/news/455594.

Even anonymous users and writers who employ pseudonyms when making controversial remarks face special scrutiny from the authorities, who attempt to identify and detain them. Surveillance is rampant in Saudi Arabia; anyone who uses communication technology is subject to government monitoring, which is officially justified under the pretense of protecting national security and maintaining social order. The authorities regularly monitor websites, blogs, chat rooms, social media sites, e-mails, mobile phone text messages, and messages sent through the very popular service WhatsApp. Evidencing the government's determination to monitor its citizens, the American security expert Moxie Marlinspike published e-mail correspondence with an employee at Mobily who sought to recruit him to help the telecommunications firm with intercepting encrypted data from mobile applications such as Twitter, Viber, Vine, and WhatsApp.[104]

In addition to direct government monitoring, access providers are required to monitor their own customers and supply the authorities with information about their online activities, often without legal process. Since 2009, the MOI has made it mandatory for internet cafes to install hidden cameras and provide identity records of their customers. The security regulations also bar entrance to anyone under the age of 18.

As ICT use has grown across the country, the threat of cyberattacks has also escalated. Several websites and portals were subject to attacks in 2012 and early 2013, including Saudi Aramco, the world's largest oil company,[105] and the official website of the Directorate General of the Ministry of Education in Riyadh.[106] Smart phones and tablets are banned at security organizations out of fears of being targeted by hackers.[107] As part of a protest for the release of political detainees, a group of hackers also attacked the websites of the Ministry of Petroleum and Mineral Resources and the Saudi television station "Channel One."[108]

The hijacking of Facebook and Twitter accounts or impersonating public figures on Facebook and Twitter also remained widespread. The Saudi Human Rights Organization site was hacked on December 31, 2012[109] and, four days later, the Twitter account of the Saudi television show Al Raeis came under attack.[110] Al-Raeis, which appears on the channel "Line Sport", was apparently targeted for allowing harsh criticisms of prominent Saudi government officials and departments to be aired.

[104] "A Saudi Arabia Telecom's Surveillance Pitch", Moxie Marlinspike, May 13, 2013, http://bit.ly/101lYnw.
[105] "Saudi Aramco hit by computer virus", The Guardian, August 16, 2012, http://bit.ly/St7x3l.
[106] "A hacker mocks the weak security of the website of Riyadh Education Directorate" [in Arabic], AlArabiya.net, November 4, 2012, http://www.alarabiya.net/articles/2012/11/04/247500.html.
[107] "Saudi Arabia bans iPhones and Galaxy 'tablets' at security organizations," Al-Arabiya, July 15, 2011, http://english.alarabiya.net/articles/2011/07/15/157742.html.
[108] "Websites belonging to Saudi Regime hacked in response to the latest detentions and in preparation for the 'Detainees Friday'" [in Arabic], Watan.com, December 27, 2012, http://www.watan.com/news/world-news/2012-12-19/17708.
[109] "'Hacker' penetrates 17 Saudi sites and register them I 'Zone-h'" [in Arabic], Sabq.org, December 31, 2012, http://sabq.org/qBtfde
[110] "Anonymous hacked into Al-Raeis Twitter account" [in Arabic], Sabq.org, January 4, 2013, http://sabq.org/6Ptfde

SOUTH AFRICA

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	8	7
Limits on Content (0-35)	8	8
Violations of User Rights (0-40)	10	11
Total (0-100)	26	26

* 0=most free, 100=least free

POPULATION: 51.1 million
INTERNET PENETRATION 2012: 41 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- In May 2012, President Jacob Zuma sought to ban the display of a painting of himself known as "The Spear" from appearing online. Though he failed to win an injunction, the *City Press* newspaper removed a reproduction from its website (see **LIMITS ON CONTENT**).
- The Constitutional Court upheld a 2011 high court judgment ruling controversial 2009 amendments to the Films and Publications Act of 1996 unconstitutional, concluding that prescreening publications, including those online, is an unjustifiable limitation on freedom of expression (see **LIMITS ON CONTENT**).
- The Protection of State Information Bill, which parliament passed in 2013, will criminalize reporting on classified state information and intentionally accessing leaked information online if signed into law (see **VIOLATIONS OF USER RIGHTS**).
- The General Intelligence Laws Amendment Bill, enacted in 2013, authorized state security agencies to intercept "foreign signals intelligence" without a warrant (see **VIOLATIONS OF USER RIGHTS**).
- FinFisher command and control servers were discovered on the Telkom network in April 2013, though the extent to which the spyware has been deployed is unknown (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Digital media freedom is generally respected in South Africa. Political content is not censored, and neither bloggers nor content creators are targeted for their online activities. Access to the internet continued to expand in the past year, facilitated in part by falling costs due to the arrival of the Seacom and the East African Submarine System (EASSy) undersea cables and new fiber-optic cables, though most South Africans access the internet from their mobile phones.

In 2012 and early 2013, internet freedom in South Africa was threatened by two pieces of legislation: the General Intelligence Laws Amendment Bill (GILAB), which aimed to legalize the bulk monitoring of communications known as "foreign signals intelligence" without judicial oversight in its original 2011 version; and the Protection of State Information Bill (POSIB), which makes it illegal to publish and access certain state information, affecting whistleblowers in both traditional and digital media, bloggers, and internet users. In a positive development, the Constitutional Court found the 2009 amendments to the Films and Publications Act of 1996 unconstitutional, concluding that the requirement to prescreen and classify publications, including those online, is an unjustifiable limitation on freedom of expression.

Prior to the Constitutional Court ruling, an art gallery successfully appealed the classification of a controversial painting of President Jacob Zuma known as "The Spear." Zuma and the ANC ruling party had also sought a court injunction to ban the painting and its digital representations from public display and dissemination online, though their failed efforts only led to more widespread circulation of and greater attention paid to the artwork.

OBSTACLES TO ACCESS

The internet is steadily spreading across South Africa, with 41 percent of the South African population having access by the end of 2012, up from 34 percent in 2011, according to the International Telecommunications Union (ITU).[1] Nevertheless, access to the internet is unequal across income lines. A 2012 household and individual survey by Research ICT Africa found that internet users comprise a little over 18 percent of the population at the bottom of the economic pyramid and about 40 percent of the rest of the pyramid.[2]

[1] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. The ITU figures may be an overestimate, as they may not take into account multiple internet subscriptions. Another measure of internet usage is the South African Advertising Research Foundation's All Media Product Survey, which estimated that in December 2012, 15.7 percent of adults had used the internet in the last day, 24.6 percent in the past month, and 27.1 percent in the last year. See, South African Advertising Research Foundation, "AMPS Trended Media Data: Internet," accessed July 24, 2013, http://www.saarf.co.za/amps/internet.asp.

[2] The "bottom of the pyramid" definition uses the 2012 South African National Planning Commission Development Plan poverty datum line, defined as households with income of less than ZAR 432 per month per household member, approximately $52.50, or less than $1.80 per person per day. See, Research ICT Africa and Intelecon, *Mobile Usage at the Base of the Pyramid in South Africa*, World Bank, December 2012: 29, http://www.infodev.org/infodev-files/resource/InfodevDocuments_1193.pdf.

The majority of users access the internet from mobile phones due to the high cost of access, infrastructural limitations, and waiting periods for fixed-line ADSL broadband installation in some areas. Accordingly, mobile phone access in South Africa is much higher than internet access, with an estimated 83 percent of the population identified as mobile phone users and about 74 percent of the population using prepaid mobile services as of July 2012, according to the South African Advertising Research Foundation.[3] The latest ITU data notes over 68 million mobile phone subscriptions in 2012, amounting to a penetration rate of nearly 135 percent.[4] Moreover, access to and usage of mobile phones is more equal across economic strata than internet access, as reported by the 2012 Research ICT Africa study, which found that 75 percent of individuals at the bottom of the economic pyramid own a mobile phone, a rate that is only 14 percent lower than mobile phone ownership in the rest of the pyramid.

South Africa has five mobile phone companies—Vodacom, MTN, Cell-C, Virgin Mobile and 8ta—all of which are privately owned except for 8ta, which is owned by Telkom, a partly state-owned company of which the government has a 39.8 percent share and an additional 10.5 percent share through the state-owned Public Investment corporation. The state previously owned a stake in Vodacom through Telkom, but its shares were relinquished in 2008.[5] The costs of mobile telecommunication services are expensive, with South Africa's mobile affordability ranked 33rd out of 44 African countries surveyed by Research ICT Africa in 2012 for the cheapest price available from dominant operators.[6]

Fixed-line broadband is also expensive, as documented in a report by the telecom research firm Ovum in 2012 that sampled 20 emerging market countries and found South Africa to have the most expensive broadband tariffs.[7] One gigabyte (GB) of data per month at a speed of 512-1024 Kbps is available for 313 rand ($36),[8] while the cheapest unlimited 1 Mbps connection costs 492 rand ($56) per month.[9] Some mobile broadband packages offering small amounts of data are cheaper than the fixed-line alternatives. The cheapest prepaid mobile data packages are 40 rand ($5) for 100 MB, 120 rand ($13.50) for 500 MB, and 266 rand ($30) for 2 GB.[10] Consequently, there were only 2.2 fixed-line broadband connections per 100 inhabitants in 2012, up from 1.8 connections in 2011,[11] and those with access are generally concentrated in urban areas. South Africa also lags behind other countries in terms of broadband speed, ranking 122 out of 180 countries for download speeds in a test conducted by Ookla.[12]

---

[3] "AMPS Trended Media Data: Cellphone Trends," South African Advertising Research Foundation, accessed February 28, 2012, http://www.saarf.co.za/amps/cellphone.asp.
[4] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions, 2000-2012."
[5] Richard Wray, "Vodafone Offers £1.2bn for Control of Vodacom," *Guardian*, June 2, 2008, http://bit.ly/1dSIGD7.
[6] Research ICT Africa, "South Africa's Mobile Termination Rate Debate: What the Evidence Tells Us," Policy Brief SA 2, November 2012, http://bit.ly/1aFoaE7.
[7] Ovum, "Broadband Pricing in Emerging Markets in 2012," cited in Nicola Mawson, "Broadband Still Too Expensive," *ITWeb*, January 8, 2013, http://www.itweb.co.za/index.php?option=com_content&view=article&id=60921.
[8] This package includes ADSL line rental as well as mandatory fixed-line voice rental. For prices see, "1GB ADSL Accounts," *Hellkom*, accessed February 27, 2013, http://hellkom.co.za/1gb-telkom-adsl/.
[9] "1Mbps Uncapped ADSL," *Hellkom*, accessed February 27, 2013, http://hellkom.co.za/uncapped-adsl/1mbps-uncapped-adsl/.
[10] These prepaid data bundles are from the mobile operator 8ta, which is owned by the fixed-line incumbent Telkom. Prices are from http://www.8ta.com/plans/prepaid-data/, accessed February 27, 2013.
[11] International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2012."
[12] "Download Speeds: Mongolia Beats SA," *IOL Scitech*, January 10, 2013, http://bit.ly/11ja0Xh.

There are hundreds of internet access providers (IAPs) in South Africa, with Telkom retaining a monopoly on fixed-line broadband access via ADSL. Although there is competition in the ADSL market and users can choose from hundreds of providers, ADSL lines are only available through Telkom due to its control over the "local loop" or "last mile" of connectivity, which is the copper (or fiber) line that connects to internet users' homes. While other operators and IAPs have been allowed to build their own last mile connectivity since 2008, they have yet to do so, leaving Telkom as the *de facto* consumer choice. It was hoped that the second national operator, Neotel, would enter the broadband market to increase competition, but the telecom has instead chosen to focus on providing wireless internet and telecom services, which has had minimal impact on last mile connectivity and the associated price of broadband.

Currently, subscribers cannot enjoy ADSL without also paying for additional voice service, while IAPs selling ADSL access need to pay Telkom for its IPConnect (IPC) service for access to Telkom's local loop. As such, Telkom has been accused of charging twice for the same product by making both Telkom consumers and providers pay for access to the same ADSL network.[13] In February 2013, the Internet Service Providers Association stated that the IPC service fee still comprised up to 70 percent of the total costs for IAPs to provide ADSL internet access. In response, the Independent Communications Authority of South Africa (ICASA) regulatory body acknowledged that the high cost of IPC could be a barrier to competition in the fixed-line sector and announced plans to conduct a study of electronic communications costs in South Africa.[14]

In 2007 the Department of Communications mandated ICASA to implement local loop unbundling by 2011 to open up the local loop between IAPs and their customers to competition. The only measure towards implementing local loop unbundling that has taken place thus far is the reduction in the IPC service price, which is regarded as more of a palliative measure rather than a solution. In April 2012, ICASA promised to implement Bitstream access—a key tool in local loop unbundling—by November 2012, but as of mid-2013, Telkom has not offered any Bitstream products to the local loop, which it still completely controls.[15]

In addition to the market challenges faced by telecom service providers, cybercafes face regulatory controls that impact their economic viability. Pursuant to Section 27(A)1 of the Electronic Communications Act, internet service providers (ISPs) and internet cafes are required to register with the Film and Publications Board (FPB), which falls under the Department of Home Affairs and is a relic, albeit a reformed one, of the Apartheid publication censorship regime. The registration requirements are not unreasonably onerous,[16] though failing to register is an offence that may be subject to a fine, six months of prison, or both. Although many internet cafes do register with the board, there is little public evidence of enforcement.

[13] Gareth Vorster, "Telkom Charging Twice for the Same Product," *BusinessTech*, March 6 2012, http://bit.ly/wQMZZV.
[14] Bonnie Tubs, "ICASA Mulls Further IPC Cut," *ITWeb*, February 21, 2013, http://bit.ly/1eUVvQk.
[15] Jan Vermeulen, "LLU: A Lost Opportunity," My Broadband, February 11, 2013, http://bit.ly/X2fP57.
[16] The applicant needs to provide his or her name, business name, national identification number, address and contact details, and nature of his or her business. The cost of registration is ZAR 462 (US$47). See, Internet Service Providers Association, "ISPA ISPs/Internet Cafés Training Course," January 2011, http://bit.ly/1bmQTP5.

Access providers and other internet-related groups are self-organized and quite active in lobbying the government for better legislation and regulations. The autonomy of the regulatory body, ICASA, is protected by the South African constitution, although several incidents involving ministerial policy directives sent to the regulator have called into question the extent of its independence.[17] In addition, the Ministry of Communications has on two different attempts in recent years proposed amendments—one to the Independent Communications Authority Act and another to the Electronic Communications Amendment Act—that would have limited ICASA's independence in various ways. A cabinet reshuffle in June 2012, which saw the replacement of the minister of communications, resulted in the removal of the problematic clauses in both bills.[18]

LIMITS ON CONTENT

Internet content and social media platforms remain free from government censorship and interference in South Africa. In September 2012, the Constitutional Court upheld a 2011 Gauteng High Court judgment ruling the controversial 2009 amendments to the Films and Publications Act of 1996 unconstitutional, based on the conclusion that the prescreening of publications (including internet content) would affect the value of news and be an unjustifiable limitation on freedom of expression.[19] Before the Constitutional Court ruling, an art gallery successfully appealed the classification of a controversial painting of President Jacob Zuma known as "The Spear," which the ruling party tried to ban from public display and dissemination online.

When the 2009 amendments to the Films and Publications Act were passed—ostensibly to regulate child pornography and hate speech—they raised concerns that certain types of controversial content could be subject to prepublication censorship. The amendments required every print and online publication not recognized by the press ombudsman to submit potentially "pornographic" or "violence-inciting" materials to the government's Film and Publications Board (FPB) for approval and imposed criminal penalties for noncompliance.[20] Exemptions were provided for artistic and scientific speech, but the FPB had the discretion to grant or deny these exemptions.[21] Movies and games were classified before their release, though the FPB could not classify publications or websites until it first received a complaint from the public. Before the amendments were overturned in September 2012, appeals could be made to the FPB's Appeals Tribunal, which had been known to rule in favor of freedom of expression online in a few cases.

The most notable case presented to the FBP in 2012 involved a controversial painting by artist Brett Murray known as "The Spear," which depicted President Jacob Zuma in Soviet attire with his

[17] See: Freedom House, "South Africa," Freedom on the Net 2012, http://www.freedomhouse.org/report/freedom-net/2012/south-africa; Open Society Initiative for Southern Africa, *South Africa*, Public Broadcasting in Africa Series (Johannesburg: Open Society Initiative for Southern Africa, 2010), http://bit.ly/GzyPq8.
[18] Nicola Mawson, "ICASA's Power Affirmed by New Bills," *ITWeb,* July 16, 2013, http://bit.ly/12TdmwN.
[19] "Film and Publications Act Amendments Declared Unconstitutional," *BizCommunity*, November 3, 2011, http://www.bizcommunity.com/Article/414/466/66617.html. http://allafrica.com/stories/201209281478.html.
[20] The Film and Publications Board is part of the Ministry of Home Affairs. According to the Film and Publications Amendment Act of 2003, all ISPs are required to register with the board.
[21] Films and Publications Amendment Act, No. 3 of 2009, accessed June 4, 2010, http://bit.ly/18H9bIu.

genitals exposed. Upset by the painting's display in Johannesburg's Goodman Gallery, the African National Congress (ANC) ruling party, Jacob Zuma and his family tried to obtain a high court injunction to ban the display of the painting, arguing that the artwork infringed upon Zuma's dignity both as an individual and as president. The aggrieved parties also sought to have an image of the painting taken down from the website of *City Press* newspaper,[22] in addition to calling for a boycott of the newspaper and pressuring advertisers to withdraw business from the publication.[23] While the May 2012 court case was postponed indefinitely,[24] the Goodman Gallery came to a private agreement with the ANC to remove the painting from display in exchange for dropping charges; the *City Press* newspaper also voluntarily removed the painting's image from its website.[25]

In response to complaints over the artwork's supposedly pornographic nature, the FPB classified the uncensored version of the painting as "16N" in June 2012, effectively proscribing the artwork and its digital reproductions from being exhibited publically or online where it could be viewed by youth under the age of 16.[26] The Goodman Gallery appealed the classification to the FPB's Appeals Tribunal in July 2012, which ultimately overruled it, concluding that the painting was neither pornographic nor harmful to children.[27] The tribunal's decision stripped the artwork's classification, thereby removing all restrictions on access to the painting and its publication online or elsewhere.[28]

Under the Electronic Communications and Transactions Act of 2002 (ECTA), ISPs are required to respond to and implement take-down notices regarding illegal content such as child pornography, defamatory material, or copyright violations. Members of the Internet Service Providers Association are not held liable for third-party content that they do not create or select,[29] though they can lose their protection from liability if they do not respond to take-down requests. As a result, ISPs often err on the side of caution by taking down content upon receipt of a notice to avoid litigation, and there is no incentive for providers to defend the rights of the original content creator if they believe the take-down notice was requested in bad faith.[30]

Meanwhile, any member of the public can submit a take-down notice, and there are no existing or proposed appeals mechanisms for content creators or providers. The Department of

[22] Karen MacGregor, "A Spear to the Heart of South Africa," *New York Times*, Op-Ed, June 5, 2012, http://nyti.ms/K9Ob5Q.
[23] David Smith, "Zuma Genitals Row Escalates as ANC Calls for Boycott of Newspaper," *Guardian*, May 25, 2012, http://www.guardian.co.uk/world/2012/may/25/zuma-genitals-row-anc-newspaper-boycott.
[24] Erin Conway-Smith, "Jacob Zuma 'The Spear' Painting Case Postponed Indefinitely," *Global Post*, May 24, 2012, http://bit.ly/LId7Bt.
[25] Phillip De Wet, "Boycott Fails, but City Press Agrees to Drop 'The Spear,'" *Mail and Guardian*, May 28, 2012, http://mg.co.za/article/2012-05-28-boycott-fails-but-city-press-agrees-to-drop-the-spear.
[26] Film and Publications Board, "FPB Classification of 'The Spear' Artwork," June 1, 2012, http://bit.ly/LRNwQu.
[27] "'The Spear' Classification Overturned," *Webber Wentzel*, October 15, 2012, http://www.webberwentzel.com/wwb/content/en/ww/ww-most-popular?oid=37612&sn=Detail-2011&pid=32704.
[28] Phillip De Wet, "Appeal Tribunal Shreds Classification of 'The Spear,'" *Mail and Guardian*, October 12, 2012, http://mg.co.za/article/2012-10-12-00-appeal-tribunal-shreds-classification-of-the-spear.
[29] The Ministry of Communications has recognized the association as an industry representative body under the act. The association acts as an agent on behalf of its 160 members and provides the ministry with annual information about the total number of take-down notices issued, the actions taken in response, and the final results. Most of the complaints lodged are resolved amicably, with ISPA's clients agreeing to take down the offending content.
[30] Alex Comninos, "Intermediary Liability in South Africa," Intermediary Liability in Africa Research Papers, 4, October 2012, http://www.apc.org/en/pubs/intermediary-liability-south-africa.

Communications has suggested improving this with a new ECTA provision that would allow a service provider to respond to the grounds of the complaint before acting upon the notice. The complainant could then reconsider and decide to withdraw the notice or send a final take-down request that would obligate the service provider to act or lose its protection from liability.[31] This proposed mechanism, however, still falls short of an actual appeals process.

The government does not restrict material on contentious topics such as corruption and human rights. Citizens are able to access a wide range of viewpoints, and there are no disproportionate government efforts to limit or manipulate online discussions. Online content, however, does not match the diverse interests of South Africa's society, especially with respect to the country's 10 other official languages besides English. Radio and television continue to be the main sources of news and information for most South Africans, but there are increasing efforts to extend mainstream news outlets to online platforms. All major media groups now have an online presence.

There are a number of political and consumer-activist websites, though the internet is not yet a key space or tool for social or political mobilization. Nevertheless, individuals and groups openly express their views via e-mail, instant messaging, chat rooms, and social media, while the South African blogosphere has become highly active in discussing issues such as HIV and AIDS, and the environment. The internet and mobile phones are increasingly used for political organization, as seen during the protests and activism against the controversial Protection of State Information Bill throughout 2011 and 2012, though they were unsuccessful in preventing the passage of the controversial bill. Meanwhile, the main political parties have developed online campaigns to attract young voters and are very active in social media.

VIOLATIONS OF USER RIGHTS

The Protection of State Information Bill (POSIB) was passed by parliament in 2013 and, if signed into law, will impose criminal penalties on journalists who report on classified state information and on individuals who intentionally access leaked information, including internet users. Meanwhile, a revised version of the 2011 General Intelligence Laws Amendment Bill (GILAB) was enacted in 2013 that tacitly authorizes the interception of electronic communications known as "foreign signals intelligence" without a warrant. FinFisher command and control servers were discovered on the Telkom network in April 2013, though the extent to which the spyware has been deployed is unknown.

The South African constitution guarantees freedom of the press and other media, freedom of information, and freedom of expression, among other guarantees. However, it also includes constraints, and freedom does not extend to "propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender, or religion and that

[31] Andrew Rens, "Notice and Take Down or Notice and Notice and Take Down?" *ex Africa semper aliquid novi* (blog), November 30, 2012, http://aliquidnovi.org/notice-and-take-down-or-notice-and-notice-and-take-down/.

constitutes incitement to cause harm."[32] The judiciary in South Africa is independent and has issued a few rulings protecting freedom of expression online in recent years. Libel is not a criminal offense, though civil laws can be applied to online content, and criminal law has been invoked on at least one occasion to prosecute against injurious material.[33]

Current threats to the traditional media in South Africa may have an impact on the internet sphere. Most notably, the Protection of State Information Bill (POSIB)—passed by the lower house of parliament in late 2011 and the upper house in November 2012—imposes sentences on journalists of up to 25 years for reporting on classified information. An amended version that marginally narrowed the definition of "national security" was approved by the National Assembly in April 2013 and was awaiting the president's signature in May 2013. Once signed into law, the bill is expected to have a chilling effect on the media as well as on internet users who could face sentences of up to ten years in prison for intentionally accessing classified South African state information on whistleblower websites. Opponents vowed to challenge the bill at the Constitutional Court before it is signed into law.

Concerning restrictions on anonymous communication, another piece of legislation—the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA), in force since 2005—requires mobile subscribers to provide national identification numbers, copies of national identification documents, and proof of a physical address to service providers.[34] An identification number is legally required for any SIM card purchase, and those in possession of an unregistered SIM card are required to register with proof of residence and an identity document.[35] As many people in South Africa do not live in formal housing, this can be an obstacle to mobile phone usage. RICA also requires ISPs to retain customer data for an undetermined period of time and bans any internet system that cannot be monitored, though under the Electronic Communications and Transactions Act of 2002 (ECTA), ISPs do not have an obligation to monitor communications on their network.[36] Internet cafes are also not required to register users or monitor customer communications.

While RICA obligates ISPs to send questionable communications to a designated interception center, it also explicitly prohibits the interception of communications, except with permission from a judge designated to rule on the practice.[37] This is based on the Criminal Procedures Act, which allows law enforcement agencies to apply to a high court judge or regional court magistrate for mobile phone records or the location of a cell phone. RICA also requires judicial oversight and

[32] Constitution of the Republic of South Africa, May 8, 1996, Bill of Rights, Chapter 2, Section 16, http://www.info.gov.za/documents/constitution/.
[33] See: Freedom House, "South Africa," Freedom of the Net 2011, http://www.freedomhouse.org/report/freedom-net/2011/south-africa.
[34] Chapter 7, "Duties of Telecommunication Service Provider and Customer," RICA, http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf.
[35] Nicola Mawson, "'Major' RICA Threat Identified," *ITWeb*, May 27, 2010, http://bit.ly/16aWGqe.
[36] Electronic Communications and Transactions Act, 2002, No. 25 of 2002, Article 78, "No general obligation to monitor," http://www.internet.org.za/ect_act.html#No_general_obligation_to_monitor.
[37] Act No. 70, 2002, Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002, Government Gazette, 22 January 2003, http://bit.ly/19iWT7k.

includes guidelines for judges to establish whether the interception is justified in terms of proportionality and narrowly defined standards.

Despite explicit legislative provisions, an investigative report by the *Mail and Guardian* in 2011 found that "[s]tate intelligence agencies can—and do—access citizens' private communications illegally," and that "it is a common occurrence, especially in police crime intelligence."[38] According to the news report, the government conducts bulk surveillance of mobile phone conversations, SMS messages, and e-mails through the National Communications Center (NCC)—a government agency that houses interception facilities and operates outside the boundaries of the law because it targets "foreign signals intelligence,"[39] which is not considered under the purview of RICA.[40] According to other reports, the NCC has the technical capability and staffing to monitor both SMS and voice traffic originating outside South Africa.[41] Calls from foreign countries to recipients in South Africa can ostensibly be monitored for certain keywords; the NCC then intercepts and records flagged conversations. While most interceptions involve reasonable national security concerns, such as terrorism or assassination plots, the system also allows the NCC to record South African citizens' conversations without a warrant and is subject to abuse without sufficient oversight mechanisms.[42]

To address the concern that the NCC operates without a legislative mandate, the South African government proposed the General Intelligence Laws Amendment Bill (GILAB) in 2011 with the aim of regulating the NCC's activities and legalizing the monitoring and interception of foreign signals intelligence.[43] Known as the so-called "Spy Bill," the 2011 version of GILAB allowed for any electronic communications originating from or passing through a foreign server—such as e-mails on international platforms, Facebook, Twitter, and Voice over IP applications—to be tapped without a warrant.[44] Civil society groups voiced deep concern over the bill's "vast unchecked powers" and its infringement on constitutional rights.[45] Signed into law in July 2013,[46] a revised version of GILAB avoided concerns over the interception of foreign signals intelligence by excluding mention of it altogether, thus leaving its legalization open to vague interpretation.

---

[38] Heidi Swart, "Secret State: How the Government Spies on You," *Mail and Guardian*, October 14, 2010, http://mg.co.za/article/2011-10-14-secret-state/.

[39] "Foreign signals intelligence" is defined as: "intelligence derived from the interception of electromagnetic, acoustic and other signals, including the equipment that produces such signals, and includes any communication that emanates from outside the borders of the Republic, or passes through or ends in the Republic." General Intelligence Laws Amendment Bill, Government Gazette No. 34747 of 11 November 2011, http://www.info.gov.za/view/DownloadFileAction?id=156569.

[40] Cliffe Dekker Hofmeyr et al., "The General Intelligence Laws Amendment Bill: big "GILA" is watching," Association of Corporate Counsel, March 7, 2012, http://www.lexology.com/library/detail.aspx?g=37a86080-473f-43cc-9037-9398704398ba.

[41] Moshoeshoe Monare, "Every Call You Take, They'll Be Watching You," *Independent*, August 24, 2008, http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20080824105146872C312228.

[42] Moshoeshoe Monare, "Every Call You Take.".

[43] General Intelligence Laws Amendment Bill, Government Gazette No. 34747 of 11 November 2011, http://bit.ly/1eUVUCj.

[44] Drew Forrest and Stefaans Brümmer, "Spooks Bid for New Powers," *Mail and Guardian,* February 3, 2012, http://mg.co.za/article/2012-02-03-spies-bid-for-new-powers/. "R2K Statement of the Final Draft of the 'Spy Bill,'" *Right2Know*, March 27, 2013, http://www.r2k.org.za/2013/03/27/r2k-statement-on-the-final-draft-of-the-spy-bill/.

[45] Cliffe Dekker Hofmeyr et al., "The General Intelligence Laws Amendment Bill: Big "GILA" is Watching," Association of Corporate Counsel, March 7, 2012; "The GILAB (aka the Spy Bill) is Back in Parliament – W You Need to Know," *Right2Know*, February 11, 2013, http://www.r2k.org.za/2013/02/11/gilab-spy-bill-back-in-parliament/.

[46] "Zuma Enacts Five New Bills into Law," *Mail and Guardian*, July 25, 2013, http://bit.ly/172tM7y.

Nevertheless, concerns over the authorities' ability to illegally intercept private communications were further heightened in April 2013 when research conducted by Citizen Lab revealed that two FinFisher command and control servers were discovered on the partially state-owned Telkom network in South Africa.[47] Such servers are used to harvest data and user information such as "screenshots, keylogger data, audio from Skype calls, passwords and more" collected by the spyware suite.[48] While Citizen Lab also found evidence of FinFisher being deployed by the authorities in Ethiopia and used against political dissidents in Bahrain,[49] the extent to which FinFisher has been implemented in South Africa and by what entities was unknown as of mid-2013. Neither Telkom nor government agencies responded to inquiries regarding the Citizen Lab findings when approached by reporters in May 2013.[50]

Meanwhile, ECTA provides for the creation of "cyber inspectors" who are given the responsibility of monitoring and inspecting websites and information systems in the public domain for unlawful activities.[51] No inspectors have been appointed since ECTA's enactment over a decade ago, though in November 2012, the Department of Communications announced that it would soon begin implementing the ECTA provision and appointing cyber inspectors to crackdown against cybercrime.[52] The inspectors are to be trained to "inspect and confiscate computers, determine whether individuals have met the relevant registration provisions, as well as search the internet for evidence of 'criminal actions.'"[53] In addition, the inspectors are not required to have any particular qualifications, and some analysts worry about the potential infringement on individuals' or companies' rights to privacy, though any search and seizure activities do require a warrant.[54]

There have been no reports of extralegal intimidation targeting online journalists, bloggers, or other digital technology users by state authorities or any other actor. In addition, politically-motivated hacking attacks are not significant; however, South African government websites, including the police website, have been hacked from actors outside South Africa a number of times this past year, and some remain unfixed. Meanwhile, spam and malware remain a significant problem in South Africa.

---

[47] Morgan Marquis-Boire et al., "For Their Eyes Only: The Commercialization of Digital Spying," Citizen Lab, https://citizenlab.org/2013/04/for-their-eyes-only-2/.
[48] Jan Vermeulen, "FinFisher Spyware Servers in South Africa," *BusinessTech*, May 6, 2013, http://bit.ly/17HPbFN.
[49] Morgan Marquis-Boire et al., "For Their Eyes Only."
[50] Jan Vermeulen, "FinFisher Spyware Servers in South Africa," *BusinessTech*, May 6, 2013.
[51] Electronic Communications and Transactions Act, 2002, No. 25 of 2002, Article 80, "Appointment of cyber inspectors," http://www.internet.org.za/ect_act.html#CYBER_INSPECTORS
[52] Thabiso Mochiko, "SA to Get Cyber Inspectors as Cyber Crime Proliferates," *Business Day*, November 14, 2012, http://www.bdlive.co.za/business/technology/2012/11/14/sa-to-get-cyber-inspectors-as-cyber-crime-proliferates.
[53] Privacy International, "South Africa," in *Silenced: An International Report on Censorship and Control of the Internet* (London: Privacy International, 2003).
[54] Shumani L Gereda, "The Electronic Communications and Transactions Act," in Lisa Thornton, Yasmin Carrim, Patric Mtshaulana and Pippa Reburn (eds.) *Telecommunications Law in South Africa*, Johannesburg, STE Publishers: 2006.

SOUTH KOREA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	3	3
Limits on Content (0-35)	12	13
Violations of User Rights (0-40)	19	16
Total (0-100)	**34**	**32**

* 0=most free, 100=least free

POPULATION: 49 million
INTERNET PENETRATION 2012: 84 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The Constitutional Court dismantled the infamous "Internet real-name system," preventing most websites from collecting ID numbers, though mobile providers still require them (see **VIOLATIONS OF USER RIGHTS**).
- Political campaigns effectively used ICTs in 2012 after restrictions on online electioneering were lifted in 2011(see **LIMITS ON CONTENT**).
- Positive developments were offset when prosecutors said intelligence agents manipulated online content under false IDs to influence the presidential election, a first for South Korea (see **LIMITS ON CONTENT**).
- In January 2013, outgoing President Lee Myung-bak pardoned a former head media regulator convicted of accepting KRW 800 million in bribes (see **OBSTACLES TO ACCESS**).
- Lawmaker Roh Hoe-chan lost his National Assembly seat after the Supreme Court convicted him of posting official secrets online, though the "secrets," which exposed political corruption, were already in the public domain (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

South Korea is one of the most wired countries in the world, as well as a vibrant fledgling democracy. However, recent years have been marked by sophisticated policing of the online environment. The UN Special Rapporteur on Freedom of Expression, international journalists, and human rights groups voiced concerns that the space for free expression in the country has diminished since 2008, after the government sought to contain public demonstrations.[1]

Developments in 2012 and 2013, nevertheless, showcased a range of democratic checks and balances partially offsetting the negative trend. In August 2012, the Constitutional Court declared 44(5) of the Information and Communications Network Act—requiring users to verify their real names before posting comments on major domestic websites—unconstitutional, although other laws mandating real-name registration in specific circumstances remain in place.[2] Both parliamentary and presidential elections took place in 2012, in April and December, respectively. In past years, online campaigning was restricted in advance of polls, but another landmark Constitutional Court ruling in December 2011 re-interpreted election laws to allow online and social media campaigns throughout the year.[3] Nevertheless, these positive developments have a possible flip-side. A scandal broke out a week before the presidential race involving intelligence agents and their alleged manipulation of online content during the campaign period.[4]

At the end of his term in office, outgoing President Lee Myung-bak issued dozens of pardons to political allies charged with corruption, including the former chairman of the regulatory Korea Communications Commission (KCC). Park Geun-hye replaced Lee as head of state in February 2013, having led Lee's conservative Grand National (*Hannara*) Party to win a majority of seats in the April 2012 National Assembly election under a new name, the New Frontier (*Saenuri*) Party. Park appointed a close aide as the new KCC chairman, perpetuating the impression that the supposedly independent regulator is under the president's direct control.[5]

---

[1] Frank La Rue, "Full Text of Press Statement Delivered by UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Frank La Rue, After the Conclusion of His Visit to the Republic of Korea," United Nations Office of the High Commissioner for Human Rights, May 17, 2010, http://bit.ly/9JplWa; Chico Harlan, "In S. Korea, a shrinking space for speech," *Washington Post*, December 22, 2011, http://www.washingtonpost.com/world/asia_pacific/in-s-korea-a-shrinking-space-for-speech/2011/12/21/gIQAmAHgBP_story.html; Reporters Without Borders, *Internet Enemies Report 2012* (Paris: Reporters Without Borders, March 12, 2012), http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf; Irene Khan, "Statement by Irene Khan, Amnesty International Secretary General, on the Completion of Her Visit to South Korea," Amnesty International, November 24, 2009, http://www.amnesty.org/en/library/asset/ASA25/013/2009/en/81c8df37-c1d9-4d49-aa8c-825cd7ce9203/asa250132009en.pdf.

[2] Sang-hun Choe, "South Korean Court Rejects Online Name Verification Law," *New York Times*, August 23, 2012, http://www.nytimes.com/2012/08/24/world/asia/south-korean-court-overturns-online-name-verification-law.html.

[3] The National Election Commission formerly applied legal provisions banning the display and distribution of election-related paraphernalia for 180 days before elections to online content, with penalties of up to 2 years' imprisonment or a fine of up to KRW 4 million (US$3,500). See, Yeon-Ok Lee & Han Woo Park, "E-Campaigning Versus the Public Official Election Act in South Korea: Causes, Consequences and Implications of Cyber-Exile," *Aslib Proceedings* 65(4), 2013, 388–405.

[4] Hyung-Jin Kim, "South Korea Spy Scandal: Spies Caught in Website Posts Embarrass National Intelligence Service," *Huffington Post*, May 13, 2013, http://huff.to/17lSaGj.

[5] Yonhap News Agency, "(2nd LD) Park Appoints Former Veteran Lawmaker as Communications Commission Chief," *Yonhap News*, March 24, 2013, http://bit.ly/16DpUAk.

In another negative development, opposition lawmaker Roh Hoe-chan lost his seat in the National Assembly after the Supreme Court convicted him of publishing online the full names of seven prosecutors implicated in wiretapped conversations exposing political corruption in August 2005, although the content was already in the public domain. Roh discussed the names in public before posting them on his blog, but the sanction was only for their online publication.[6]

Political tensions with North Korea are a significant motivation for online restrictions, and the government said it had traced a series of high-profile March 2013 cyber-attacks on major institutions to Pyongyang, the capital of the communist North. A handful of prosecutions against users who post pro-North Korean content online are ongoing.[7] One Twitter user, for example, is appealing a November 2012 suspended 10 month prison term for reposting tweets from North Korea in 2011.

OBSTACLES TO ACCESS

South Korea is one of the most wired countries in the world, for both usage and connection speed. Approximately 84 percent of South Koreans used the internet in 2012.[8] Counting access via mobile phones, televisions, and game consoles, an estimated 97 percent of households had access as of June 2012.[9]

Several factors have contributed to the country's high degree of connectivity. First, high-speed access is relatively affordable. Most residences have connections capable of reaching 100 Mbps for under KRW 30,000 ($26) per month.[10] Second, the population is densely concentrated in urban areas. Roughly 70 percent of South Koreans live in cities dominated by high-rise apartment buildings that can easily be connected to fiber-optic cables.[11] Finally, the government has implemented programs to expand internet access, including subsidies for low-income groups.[12] A series of state-led initiatives have been implemented since the 1990s, including Cyber Korea 21

[6] David McNeill and Donald Kirk, "Tax Evasion, Bribery and Price-fixing: How Samsung Became the Giant that Ate Korea," *The Independent*, February 25, 2013, http://www.independent.co.uk/news/world/asia/tax-evasion-bribery-and-pricefixing-how-samsung-became-the-giant-that-ate-korea-8510588.html.

[7] Seok Ahn, "11 Online North Korean Sympathizers Arrested. 5 Times More Social Networking Accounts Blocked [for Violating the National Security Act] Over the Past Year" (in Korean), *Seoul Shinmun*, May 18, 2012, http://www.seoul.co.kr/news/newsView.php?id=20120518011015; Junhee Park, "Violation of the National Security Act in increase. Already 70 Cases in the First Half of the Year" [in Korean], *Munhwa Ilbo*, July 9, 2012, http://www.munhwa.com/news/view.html?no=2012070901071027216002.

[8] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[9] South Korea has consistently led the 34 members of the international trade group the Organization for Economic Co-operation and Development for internet access since 2000. Organization for Economic Co-operation and Development, "Households with Access to the Internet in Selected OECD Countries," http://www.oecd.org/sti/ieconomy/Final_6.b_Internet%20Households_2012.xls.

[10] John D. Sutter, "Why Internet Connections Are Fastest in South Korea," *CNN Tech*, March 31, 2010, http://articles.cnn.com/2010-03-31/tech/broadband.south.korea_1_broadband-plan-south-korea-broadband-internet?_s=PM:TECH. The figures were still current as of April 2013.

[11] J. C. Herz, "The Bandwidth Capital of the World," *Wired*, August 2002, http://www.wired.com/wired/archive/10.08/korea.html?pg=1&topic=&topic_set.

[12] Sutter, "Why Internet Connections Are Fastest in South Korea."

(1999–2002), the e-Korea Vision 2006 (2002–2006), and the U-Korea Master Plan (2006–2010). Cyber Korea 21 was well received by the Korean public, partly because a foundation of computer-mediated communications had already been laid with a pre-internet, text-based online communication known as PC *tongshin* ("communication").

Mobile phone penetration was at 110 percent in 2012—a sign that many users have more than one device.[13] Smartphone users represented 62 percent of all mobile subscribers as of 2012.[14] Wi-Fi coverage has also increased rapidly to accommodate smartphones and tablet computers. Free Wi-Fi services are offered in over 1,000 public spaces across the country, including train stations, airports, libraries, national public hospitals, community centers, and selected tourist spots.[15]

Omnipresent and affordable cybercafés have helped prevent a digital divide in South Korea. Known as PC *bang* ("rooms"), many offer broadband access for approximately $1 per hour, and also serve as venues for social interaction and online gaming. There is no significant gap in access to ICTs with respect to gender or income level, although differences in computer literacy across generational and professional lines persist.[16]

The telecommunications sector in South Korea is relatively diverse and open to competition, with 118 internet service providers (ISPs) operating as of February 2013.[17] Nevertheless, the market remains dominated by three companies: Korea Telecom (44 percent), SK Telecom (24 percent), and LG Telecom (15 percent). The same firms control equivalent shares of the country's mobile phone service market, at 31 percent, 50 percent, and 19 percent respectively.[18] All three companies are publicly traded (Korea Telecom was state-owned until privatization in 2002), but they are part of the country's *chaebol*—large, family-controlled conglomerates connected to the political elite, often by marriage ties.[19] This has given rise to speculation that favoritism was at play in the privatization process and in the selection of bidders for mobile phone licenses.[20]

The conservative Lee Myung-bak government, which was in power from February 2008 to February 2013, restructured regulatory institutions dealing with ICTs. The ministry of information and communication and the Korean Broadcasting Commission merged to create the KCC in February 2008, tasked with overseeing both telecommunications and broadcasting to improve

[13] International Telecommunication Union, "Mobile-cellular Telephone Subscriptions, 2000-2012."
[14] Korea Communications Commission, "Wire and Wireless Communication Service Subscribers in 2012" [in Korean], *IT Statistics of Korea*, March 5, 2013, http://www.itstat.go.kr/board/boardDetailView.htm?identifier=02-008-130306-000001&pub_code=5&page=1.
[15] Jungyun Kwon, "Free Wi-Fi Now Offered at Public Areas Nationwide," *Korea.net*, July 25, 2012, http://www.korea.net/NewsFocus/Sci-Tech/view?articleId=101482.
[16] National Information Society Agency, *The 2011 Digital Divide Index* [in Korean], http://www.itstat.go.kr/board/boardDetailView.htm?identifier=02-008-120309-000001&pub_code=7&page=1.
[17] Korea Internet & Security Agency, "ISP Statistics" [in Korean], accessed April 7, 2013, http://isis.kisa.or.kr/sub01/?pageId=010302.
[18] Korea Communications Commission, "Wire and Wireless Communication Service Subscribers in 2012."
[19] Hyeok-cheol Kwon, "Is *Chojoongdong* One Big Family?" [in Korean], *Hankyoreh*, July 29, 2005, http://www.hani.co.kr/kisa/section-002009000/2005/07/002009000200507291742668.html.
[20] Hyun-ah Kim, "KMI Criticizes Selection Criteria for the 4th Mobile Operator and Sends Out Open Inquiry [to KCC]" [in Korean], *e-Daily*, February 18, 2013, http://bit.ly/1fXe7y8.

policy coherence.[21] The KCC consists of five commissioners, with the president appointing two (including the chairman) and the National Assembly choosing the remainder. The KCC struggled to earn credibility, as its first chairman Choi See-joong was a close associate of then-president Lee, causing some observers to view the restructuring as a government effort to tighten control over the media and ICT sectors.[22] Lee reappointed Choi as chairman in March 2011 over the objections of opposition lawmakers, who said that Choi's personnel choices politicized the agency and that his licensing decisions favored conservative-leaning media outlets. In January 2012, Choi resigned after prosecutors began investigating him in connection with several bribery scandals, including allegations that his former aide received nearly KRW 200 million ($175,400) in bribes from the Korea Broadcasting and Art School in return for business favors.[23] Choi was arrested in April 2012 on charges of accepting KRW 800 million ($701,700) from a real estate developer in return for influence peddling. He was sentenced to two and a half years in prison and a fine of KRW 600 million ($526,300) in September 2012.[24] However, Lee issued 55 pardons marking the end of his term in January 2013, including Choi and other political allies.[25]

In March 2013, the new president Park Geun-hye missed an opportunity to distance herself from this history of cronyism, naming her close aide and former four-term lawmaker Lee Kyeong-jae to head the KCC.[26] Park also transferred the KCC's policy and strategy-related responsibilities to the new Ministry of Science, ICT & Future Planning. The KCC retains its regulatory remit.

LIMITS ON CONTENT

South Korean censors blocked or deleted more than 57,000 sites or web pages in 2012, according to official figures. Law professor Park Kyung Sin, himself a member of the commission responsible for censorship, saw his own conviction and fine for re-posting censored content on his personal blog overturned in July 2012, while a Twitter user who criticized the ruling party in 2011 also saw his fine overturned under a revised interpretation of election laws. During the coverage period, these looser rules allowed online campaigning, diversifying discourse and encouraging the growth of online platforms ranging from independent, not-for-profit news outlets to far-right political forums.[27] In a first for South Korea, however, intelligence agents are currently under investigation

[21] Jong Sung Hwang & Sang-hyun Park, "Republic of Korea," in *Digital Review of Asia Pacific 2009–2010* (London: Sage Publications, 2009), 234–240.
[22] Ji-nam Kang, "Who's Who Behind Lee Myung-bak: Choi See-joong the Chairman of the KCC (Appointed)" [in Korean], *Shindonga* (583, 2008), 48–49, http://shindonga.donga.com/docs/magazine/shin/2008/04/12/200804120500019/200804120500019_1.html.
[23] Yonhap News Agency, "Ex-aide of KCC Chief Under Bribery Probe," *The Korea Herald*, January 4, 2012, http://www.koreaherald.com/national/Detail.jsp?newsMLId=20120103000879; Tae-gyu Kim and Jun-beom Hwang, "Choi See-joong's Protégé Jeong Yong-uk Bags a Huge Bribe and Flees to Canada?" [in Korean], *Hankyoreh*, January 3, 2012, http://www.hani.co.kr/arti/society/society_general/513250.html.
[24] Rahn Kim, "President's Mentor gets Prison Term," *The Korea Times*, September 14, 2012, http://www.koreatimes.co.kr/www/news/nation/2012/09/117_119968.html.
[25] BBC, "South Korean President Issues Controversial Pardons," *BBC News*, January 29, 2013, http://www.bbc.co.uk/news/world-asia-21241376.
[26] Yonhap News Agency, "(2nd LD) Park Appoints Former Veteran Lawmaker."
[27] James Pearson, Conservatives Go on the Online Offensive," *Yonhap News*, April 30, 2013, http://english.yonhapnews.co.kr/n_feature/2013/04/29/45/4901000000AEN20130429006500315F.HTML; Seung-hye Yim,

for manipulating political discussion online under false IDs in advance of the December 2012 presidential election.

Although South Korean cyberspace is vibrant and creative, there are a number of restrictions on the free circulation of information and opinions. Technical filtering of websites and social media accounts and the administrative deletion of content are particularly evident. Technical filtering of blacklisted URLs focuses on content produced by, or otherwise sympathetic to, the North Korean regime. A series of tests conducted in 2008 and 2010 by the OpenNet Initiative found that a significant number of websites containing North Korean propaganda or writings promoting reunification of the two Koreas were explicitly and consistently blocked in South Korea.[28] The justification provided is that these violate the 1948 National Security Act, which classifies content that "praises, promotes, and glorifies North Korea" as "illegal information."

Censorship is carried out on the orders of the Korea Communications Standards Commission (KCSC), which was established in 2008 to maintain ethical standards in broadcasting and internet communications. Technically an independent statutory organization, its nine members are appointed by the president.[29] Observers criticize its vaguely defined standards and wide discretionary power to determine what information should be censored.[30]

A KCSC member outlined the censorship process for Freedom House.[31] A team of 20 to 30 monitoring officers flag possible offenses, including obscenity, defamation, and threats to national security. Citizens can also submit individual petitions against content they believe has violated their privacy or harmed their reputation, or directly request service providers to temporarily remove the content in question for 30 days, effective immediately, under Article 44(2) of the Information and Communications Network Act. Commissioners meet every two weeks to deliberate over flagged cases—the minutes of which are available on the KCSC website[32]—and then make recommendations to bulletin board operators or ISPs to implement corrective measures such as deletion or blocking designated URLs. Such recommendations are not legally binding, but noncompliant service providers face potential sanctions under Comprehensive Measures on Internet Information Protection issued by the KCC in 2008, so practically all providers conform. Some service providers and websites institute their own registration or content monitoring policies so as to preempt KCSC intervention, though no comprehensive data about the extent of these voluntary practices is available.

"Online Communities Keep Politicians Squirming," *Joongang Ilbo*, March 16, 2013, http://www.joongang.ca/bbs/board.php?bo_table=g900t400&wr_id=29.

[28] OpenNet Initiative, "Country Profile: South Korea," August 6, 2012, http://opennet.net/research/profiles/south-korea.

[29] Six members are nominated by the president and the party with a parliamentary majority, while three are nominated by the opposition. Jeong-hwan Lee, "A Private Organization Under the President? The KCSC's Structural Irony" [in Korean], *Media Today*, September 14, 2011, http://www.mediatoday.co.kr/news/articleView.html?idxno=97350.

[30] Jillian York and Rainey Reitman, "In South Korea, the Only Thing Worse Than Online Censorship is Secret Online Censorship," *Electronic Frontier Foundation*, September 6, 2011, https://www.eff.org/deeplinks/2011/08/south-korea-only-thing-worse-online-censorship.

[31] Author's interview with Park Kyung Sin, one of the nine members of the KCSC, April 4, 2013.

[32] Available at http://www.kocsc.or.kr/02_infoCenter/Records_List.php [in Korean].

The KCSC publishes quarterly statistics of content filtered or deleted.[33] These figures have shot up since 2008, its first year of operation, when it reported blocking 4,731 websites or pages,[34] and deleting another 6,442.[35] In 2012, it blocked 39,296 websites or pages and deleted 17,827.[36] The trend continued in the first quarter of 2013, when 11,396 items were blocked and 5,717 items were deleted.[37] Offenses cited for the censorship included "encouraging gambling," "illegitimate food and medicine," "prostitution and obscenity," "violating others' rights," and "violating other laws and regulations," the category that encompasses North Korean sympathies.

In 2011, law professor Park Kyung Sin, one of the KCSC's nine members, challenged the institution's criteria by posting some censored content—such as non-sexual images of human genitalia—on his personal blog for public discussion.[38] Fellow KCSC members began evaluating his blog for deletion and Park subsequently took the pictures down, but prosecutors indicted him for possible violation of obscenity laws in February 2012.[39] The court fined Park KRW 3 million ($2,630) in July, but a higher court cleared him on appeal in October.[40] The prosecution has appealed to the Supreme Court and the case is currently being heard. Park's blog is still available, and he continues to advocate publicly for freedom of expression.[41]

Park told Freedom House a major cause for concern is that authors of blocked or deleted content are never notified of the commission's decision, nor given an opportunity to defend their right to publish. While they can challenge the commission directly if they learn about a ruling, there is no independent avenue for appeal. This allows the KCSC to make politically, socially, and culturally motivated judgments, often lacking legal grounds. In many cases, the KCSC blocks entire blogs, though only a small portion of posts are considered to be problematic. All this has contributed to an atmosphere of self-censorship, particularly on topics related to North Korea.

---

[33] Available at http://www.kocsc.or.kr/02_infoCenter/info_Communition_List.php [in Korean].
[34] 3,816 for "encouraging gambling," 549 for "disturbing social order," and 366 for "obscenity."
[35] 3,238 for "disturbing social order,"1,460 for "obscenity," 1,201 for "violating others' rights," 424 for "violence, cruelty and hatred," and 119 for "encouraging gambling."
[36] Among those blocked, 18,971 were for "encouraging gambling," 13,065 for "illegitimate food and medicine," 5,600 for "prostitution and obscenity," 962 for "violating others' rights," and 698 for "violating other laws and regulations." Among those deleted, 6,908 were for "illegitimate food and medicine," 5,481 for "prostitution and obscenity," 3,910 for "violating other laws and regulations," 920 for "encouraging gambling," and 608 for "violating others' rights."
[37] Among those blocked, 6,621 were for "encouraging gambling," 2,875 for "illegitimate food and medicine," 1,179 for "prostitution and obscenity," 412 for "violating other laws and regulations," and 309 for "violating others' rights." Among those deleted, 2,464 were for "violating other laws and regulations," 1,665 for "illegitimate food and medicine," 902 for "prostitution and obscenity," 377 for "violating others' rights," and 309 for "encouraging gambling."
[38] R. Jai Krishna and Evan Ramstad, "'Offensive' Web Content Targeted in Asia," *The Wall Street Journal*, December 6, 2011, http://online.wsj.com/article/SB10001424052970204770404577082080244171866.html; York and Reitman, "In South Korea, the Only Thing Worse Than Online Censorship."
[39] Evan Ramstad, "Prosecutors Target Censorship Critic," *The Wall Street Journal*, March 8, 2012, http://blogs.wsj.com/korearealtime/2012/03/08/prosecutors-target-censorship-critic/.
[40] Jeongin You, "Professor Park Kyung Sin 'Not Guilty' in an Appellate Court. A Promising Ruling for Freedom of Expression" [in Korean], *Kyunghyang Shinmun*, October 18, 2012. http://bit.ly/RFfmnp.
[41] *K.S. Park's Writings* (blog), http://blog.naver.com/kyungsinpark.

In 2011, the KCSC sought to expand the scope of censorship to social networking sites, mobile phone applications, and podcasts.[42] The commission created a team to systematically monitor social media and communication apps, such as Twitter and Facebook, for violations. Since selectively deleting posts is more challenging on social media than from static websites and blogs, the KCSC warns users to voluntarily delete posts containing false or harmful information. If they refuse, the commission can ask ISPs to block other users from accessing the disputed account altogether.[43] Social media cases amount roughly to 5 percent of the total considered by the KCSC, according to Park.

They sometimes lack tolerance for government criticism. In May 2011, the KCSC ordered the blocking of Twitter account "@2MB18nomA," consisting of former President Lee's nickname "2MB" and a phonetic reference to a common Korean curse word.[44] After the KCSC rejected an appeal challenging the block, the user turned to the Seoul Administrative Court, but lost his case in May 2012.[45] He was also fined KRW one million ($877) for violating the election law through tweets posted in May 2011 criticizing the ruling party. That decision was overturned, however, when he successfully appealed in March 2012.[46]

That success was the result of a change in restrictions on online expression surrounding elections in South Korea, which observers have criticized as more stringent than in other democracies.[47] Article 93(1) of the Public Official Election Act, adopted to ensure fair electoral competition, prohibits individual voters from distributing or displaying "an advertisement, letter of greeting, poster, photograph, document, drawing, printed matter, audio tape, video tape, or the like" during the 180 days prior to election day if it contains an endorsement of or opposition to a candidate or a political party. The National Election Commission (NEC) has historically applied this to blog posts, user comments on news websites, and user-generated content in social media, and could demand that websites or blog-hosting services remove such postings. However, the Constitutional Court ruled that interpretation was unconstitutional in December 2011.[48] The NEC allowed online campaigning as of January 13, 2012.[49]

---

[42] Matt Brian, "South Korea May Begin Censoring Social Networking, Mobile Apps from Next Week," *The Next Web*, December 1, 2011, http://thenextweb.com/asia/2011/12/01/south-korea-may-begin-censoring-social-networking-mobile-apps-from-next-week/.

[43] Interview with Kyung Sin Park. See also, Ji-hyun Cho, "Criticism Escalates Over SNS Censorship," *The Korea Herald*, January 29, 2012, http://www.koreaherald.com/business/Detail.jsp?newsMLId=20120129000285.

[44] Harlan, "In S. Korea, A Shrinking Space." See also, Louisa Lim, "In South Korea, Old Law Leads To Crackdown," *National Public Radio (NPR)*, December 1, 2011, http://www.npr.org/2011/12/01/142998183/in-south-korea-old-law-leads-to-new-crackdown.

[45] Jeong-min Yang, "Owner of the Twitter ID 'Cursing MB' Lost his Case, But Why?" [in Korean], *Money Today*, May 4, 2012, http://www.mt.co.kr/view/mtview.php?type=1&no=2012050407583397741&outlink=1.

[46] Seung-mo Kim, "Posting on Twitter a List of Candidates to be Rejected is Not Illegal, Says Court" [in Korean], *The Law Times*, March 20, 2012, http://www.lawtimes.co.kr/LawNews/News/NewsContents.aspx?serial=63156.

[47] Lee and Park, "E-Campaigning Versus the Public Official Election Act."

[48] Yonhap News Agency, "Constitutional Court OKs Twitter for Election Campaigns," *The Korea Times*, December 29, 2011, http://www.koreatimes.co.kr/www/news/nation/2011/12/113_101835.html; Akira Nakano, "S. Korea Allows Campaigning on Social Networking Sites," *The Asahi Shimbun*, December 30, 2011, http://ajw.asahi.com/article/asia/AJ201112300023.

[49] Agence France-Presse, "S. Korea Lifts Ban on Internet for Electioneering," *AsiaOne*, January 13, 2012, http://www.asiaone.com/News/Latest%2BNews/Science%2Band%2BTech/Story/A1Story20120113-321714.html; Yonhap News Agency, "Election Regulator Allows Internet Election Campaigns," *The Korea Times*, January 13, 2012, http://www.koreatimes.co.kr/www/news/nation/2012/01/311_102798.html.

Perhaps the most troubling development stemming from this change came the following year when lawmakers revealed a National Intelligence Service (NIS) agent had published online comments under some 40 different IDs in an effort to influence the December 2012 presidential election. In March 2013, the main opposition party claimed that this manipulation extended to many more NIS agents and implicated NIS Director Won Sei-hoon.[50] In June 2013, Won was indicted on charges of interfering in the election.[51] The prosecution said he also attempted to influence earlier elections in favor of the ruling conservative party.[52]

While the overall media environment is partly restricted,[53] South Koreans continue to enthusiastically embrace online technology for civic engagement and political mobilization. In early 2012, journalists launched a series of strikes against government interference and censorship for the first time since the country's transition to democratic rule in 1987.[54] Born out of this was a variety of alternative and activist media outlets on the internet. The most thriving example is *Newstapa*, a user-funded investigative journalism platform, which reported over 28,000 regular donors and almost six million views of its YouTube content in April 2013. Filmmakers have also successfully solicited funding via social media for socially conscious films, such as "26 Years," about the military crackdown on a democratic uprising in the southwestern city of Gwangju in 1980—which topped the box office in November 2012[55]—and "Another Family," which documents poor working conditions in Samsung semiconductor factories, and is due for release in late 2013.

VIOLATIONS OF USER RIGHTS

The year's most positive development for ICT users came in August 2012, when the Constitutional Court ruled South Korea's historically stringent internet real-name registration requirements violated the constitution. Website administrators are now banned from collecting national identification numbers, except where doing so is mandated by another law such as the Public Official Election Act and the Children and Youth Protection Act. It is not clear whether the court's ruling will also apply to mobile service providers, who still register customers and provided personal information to law enforcement agencies on 395,061 occasions in the first half of 2012, according to official statistics. As in past years, internet users were prosecuted for online activity. Twitter user Park Jung-geun is appealing a November 2012 suspended sentence for re-posting

[50] Yonhap News Agency, "Lawmaker Accuses Spy Agency Chief of Intervening in Politics," *Yonhap News*, March 18, 2013, http://english.yonhapnews.co.kr/northkorea/2013/03/18/0401000000AEN20130318006200315.HTML; Chang-sup Lee, "National Intelligence Service Needs Overhaul," *The Korea Times*, March 28, 2013, http://www.koreatimes.co.kr/www/news/opinon/2013/03/298_132922.html.

[51] Chico Harlan, "In South Korea's Latest Controversies, Spy Agency Takes a Leading Role," *Washington Post*, July 6, 2013, http://www.washingtonpost.com/world/asia_pacific/in-south-koreas-latest-controversies-spy-agency-takes-a-leading-role/2013/07/06/8b610c74-e3ca-11e2-aef3-339619eab080_story.html.

[52] Dong-hyun Lee, "Won Sei-hoon Ordered Operations Against Opposition Candidates in Every Election, Says Prosecution" [in Korean], *Joongang Ilbo*, June 6, 2013, http://media.daum.net/issue/438/newsview?issueId=438&newsid=20130606003705675.

[53] Freedom House, "Freedom of the Press 2012 – South Korea," http://www.freedomhouse.org/report/freedom-press/2012/south-korea.

[54] "No News is Bad News: Reporters Complain of Being Muzzled," *Economist*, March 3, 2012, http://www.economist.com/node/21549008.

[55] Erika Kim, "'26 Years' Tops Box Office in Its First Weekend," *enewsworld*, December 3, 2012, http://enewsworld.interest.me/enews/contents.asp?idx=22873.

content from a North Korean Twitter account, and lawmaker Roh Hoe-chan was ousted in 2013 following a criminal conviction for exposing political corruption online. Another continuing trend was extensive cyber-attacks that crippled broadcast agencies and financial institutions, exposing millions of subscribers to possible fraud.

The South Korean constitution guarantees freedom of speech, the press, assembly, and association to all citizens, but it also enables restrictions by stating that "neither speech nor the press may violate the honor or rights of other persons nor undermine public morale or social ethics." South Korea has an independent judiciary and a national human rights commission that have made decisions upholding freedom of expression. Nonetheless, the continued prosecution of internet users for online activities has generated a chilling effect and international criticism.[56]

Several laws restrict freedom of expression in traditional media, as well as online. The 1948 National Security Act allows prison sentences of up to seven years for praising or expressing sympathy with the North Korean regime. In April 2010, the Ministry of Unification issued a notice reminding citizens that the 1990 Act on Exchanges and Collaboration Between South and North Korea applies to online communications as well as offline,[57] and that any visit to websites or pages maintained by people of North Korea must be reported to the government in advance.[58] Anyone failing to do so faces a fine of up to KRW 1 million ($878).

National security prosecutions against individuals expressing North Korean sympathies increased while the previous conservative government was in power. Those stemming from online communications rose from 5 in 2008 to 82 in 2010, a trend which looks set to continue.[59] In September 2011, police raided the studio of photographer Park Jung-geun after he retweeted posts from a North Korean Twitter account (@uriminzok).[60] Park said his reposts made fun of the regime. Nevertheless, police interrogated him five times and in January 2012, jailed him for one month before releasing him on bail. A court sentenced him to a suspended 10-month prison term in November 2012, and he is currently appealing his conviction in a higher court.[61]

---

[56] La Rue, "Full Text of Press Statement."
[57] Ministry of Unification, "Notice on the Use of North Korean Internet Sites" [in Korean], April 8, 2010, http://www.unikorea.go.kr/CmsWeb/viewPage.req?idx=PG0000000346&boardDataId=BD0000186451&CP0000000002_BO0000000033_Action=boardView&CP0000000002_BO0000000033_ViewName=board/BoardView&curNum=12.
[58] Such reports are to be made through an online system at http://www.tongtong.go.kr/.
[59] Sang-hun Choe, "Sometimes, It's a Crime to Praise Pyongyang," *New York Times*, January 5, 2012, http://www.nytimes.com/2012/01/06/world/asia/06iht-korea06.html?pagewanted=all; Ahn, "11 Online North Korean Sympathizers Arrested" [in Korean]; Park, "Violation of the National Security Act in Increase" [in Korean]; Amnesty International, "Republic of Korea," *Amnesty International Report 2013: The State of the World's Human Rights*, http://files.amnesty.org/air13/AmnestyInternational_AnnualReport2013_complete_en.pdf, 150-152.
[60] Lim, "In South Korea, Old Law Leads To New Crackdown;" Sang-hun Choe, "South Korean Law Casts Wide Net, Snaring Satirists in a Hunt for Spies," *New York Times*, January 7, 2012, http://www.nytimes.com/2012/01/08/world/asia/south-korean-law-casts-wide-net-snaring-satirists-in-a-hunt-for-spies.html?pagewanted=1&_r=1; Agence France-Presse, "Amnesty Urges Release of S. Korean Twitter User," *Google News*, February 1, 2012, http://bit.ly/1dSvfTA.
[61] Paula Hancocks, "South Korean 'Joke' May Lead to Prison," *CNN*, July 4, 2012, http://edition.cnn.com/2012/07/03/world/asia/south-korea-north-joke/index.html; Sang-hun Choe, "South Korean Gets Suspended Sentence in Twitter Case," *New York Times*, November 21, 2012, http://www.nytimes.com/2012/11/22/world/asia/south-korean-man-gets-suspended-sentence-for-tweets.html.

More prosecutions could result from a cyber-attack allegedly orchestrated by the transnational hacking collective Anonymous, who released details of over 15,000 subscribers of North Korean government websites and social media accounts in April 2013. South Korean law enforcement agencies used the data to investigate citizens violating South Korean law, but many of the subscribers used false names, news reports said.[62]

Within South Korea, such pseudonymous registration has been compromised by the infamous "internet real-name system" adopted in 2004 as part of an amendment to the Public Official Election Act.[63] Users were required to verify their identities by submitting their Resident Registration Numbers (RRNs) to join and contribute to web portals and other major sites. An RRN is a 13-digit number uniquely assigned to a Korean citizen at birth. In 2007, the real-name system was expanded to apply to any website with more than 100,000 visitors per day under Article 44(5) of the Information and Communications Network Act.

Beyond its chilling effect for online expression, the risk of such widespread real-name registration became evident in July 2011 when a cyberattack, allegedly originating from China, targeted the popular portal Nate and its social networking service Cyworld. The hackers reportedly stole the personal details of 35 million users, equivalent to 70 percent of the country's total population. The stolen data included users' real names, passwords, RRNs, mobile phone numbers, and e-mail addresses. The portal's parent company, SK Communications, said RRNs and passwords were encrypted,[64] but the incident renewed public concern about internet users' right to privacy.[65]

In August 2012 the Constitutional Court ruled against the internet real-name system, citing vulnerability to cyberattacks, among other factors.[66] As of February 18, 2013, website administrators are prohibited from collecting users' RRNs, and required to destroy those already on record by 2014.[67] Although much welcomed, this ruling does not entirely abolish real-name registration. The recently amended Children and Youth Protection Act, for example, enhanced the requirements for online identity verification from September 2012 to protect young people online (RRNs contain digits from the user's birth date that reveal their age).[68] Some companies use other methods for linking users' identities to their online profiles, and the KCC is also exploring registration options beyond RRNs, such as Internet Personal Identification Numbers (i-PINs),

[62] Chosun Ilbo, "More Details of N.Korean Website Subscribers Released," *Chosun Ilbo*, April 8, 2013, http://english.chosun.com/site/data/html_dir/2013/04/08/2013040801418.html.
[63] The amendment became Article 82, Provision 6.
[64] "Nate, Cyworld Hack Stole Information From 35 Million Users: SKorea Officials," *Huffington Post*, July 28, 2011, http://www.huffingtonpost.com/2011/07/28/south-korea-nate-cyworld-hack-attack_n_911761.html.
[65] Eric Pfanner, "Naming Names on the Internet," *New York Times*, September 4, 2011, http://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html.
[66] Park Kyung Sin, "Korean Internet Identity Verification Rule Struck Down Unconstitutional; 12 Highlights of the Judgment," *K.S. Park's Writings* (blog), August 25, 2012, http://blog.naver.com/kyungsinpark/110145810944.
[67] Yunji Kang, "Hide your RRN Away! Ban on Online Collection of User RRNs" [in Korean], *Sympa Korea*, February 21, 2013, http://reporter.korea.kr/reporterWeb/getNewsReporter.do?newsDataId=148755878.
[68] Ki-bon Lee, "Effective from September 16, 2012, the New Youth Protection Law" [in Korean], *Pol in Love* (Police Agency official blog), September 3, 2012, http://polinlove.tistory.com/4371; Yoo Eun Lee, "South Korea's Child Porn Law Blasted for Restricting Freedom of Expression," *Global Voices Online*, May 24, 2013, http://globalvoicesonline.org/2013/05/24/south-koreas-child-porn-law-blasted-for-restricting-freedom-of-expression/.

authenticated certificates, and SMS verification. In the meantime, mobile service providers still require users to provide their RRNs.

Service providers are expected to make individual users' personal information available on request to investigative agencies, including police, prosecutors, and the National Intelligence Service, under Article 83(3) of the Telecommunications Business Act. According to KCC statistics,[69] mobile phone operators fulfilled 395,061 such requests in the first half of 2012, a 21 percent increase over the number they executed during the same period in 2011.[70] The KCC has not published more recent data.

Defamation, including written libel and spoken slander, is a criminal offense in South Korea punishable by up to five years' imprisonment or a fine of up to KRW 10 million ($8,800), whether the contested statement is true or not; insults are punishable by a maximum KRW 2 million ($1,751) fine or a prison sentence of up to one year. Defamation committed via ICTs draws even heavier penalties—seven years in prison or fines of up to KRW 50 million ($43,900)—under the 2005 Information and Communications Network Act, which cites the faster speed and wider audience of online communication as a basis for the harsher sentencing.[71]

In February 2013, Roh Hoe-chan, a lawmaker from a minor opposition party, lost his seat in the National Assembly after being convicted in the Supreme Court for publishing wiretapped conversations online in 2005 in violation of the 1993 Protection of Communications Secrets Act. The conversations, illegally recorded by intelligence agents in the 1990s, documented representatives of The Samsung Group paying regular bribes to prosecutors, politicians, and presidential candidates. The Supreme Court explained its ruling against Roh by stating, "the internet delivers unfiltered information to the public, while the media select what to publish with responsibility."[72] Observers noted that the conviction appeared to have been pushed through in advance of pending revisions to the 1993 Act, which may have led to a different outcome.[73]

A copyright law that restricts file sharing was passed in May 2009 and came into effect two months later. Often referred to as the "three strikes rule," it allows the Minister of Culture, Sports and Tourism, acting through the Korean Copyright Commission, to shut down an entire online bulletin board after a third warning to take down pirated content. Within a year, the ministry had issued

[69] Published twice a year at http://www.kcc.go.kr/user.do?boardId=1030&page=A02060400&dc=K02060400 [in Korean].
[70] Na-young Shim, "Last Year, 390,000 Users Subjected to 'Telecommunication Surveillance'" [in Korean], *Asia Economy*, January 9, 2013, http://www.asiae.co.kr/news/view.htm?idxno=2013010813361388756. The KCC reported 326,785 requests in the first half of 2011.
[71] See "Article 61: Republic of Korea," *Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.,* Amended December 30, 2005, http://www.worldlii.org/int/other/PrivLRes/2005/2.html.
[72] The Associated Press, "MP Loses Seat Over Samsung Wiretaps," *MSN News*, February 17, 2013, http://news.uk.msn.com/world/mp-loses-seat-over-samsung-wiretaps; Sam Byford, "Korean Lawmaker who Exposed Samsung Corruption Forced from Office," *The Verge*, February 15, 2013, http://www.theverge.com/2013/2/15/3991338/samsung-x-file-tapes-lawmaker-roh-hoe-chan-loses-government-seat.
[73] Yonhap News Agency, "Song Ho-chang: Ruling on Roh Hoe-chan's Case Should Wait Until the Amendment," [in Korean], *OhmyNews*, February 8, 2013, http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0001832963.

over 450 warnings and disabled 11 accounts for sharing copyrighted materials.[74] Internet companies and civil liberties advocates say the law threatens fair use and free expression.[75]

There have been no reports of physical violence against online users. Technical violence is more common. A notable increase in such technical disruptions in the past two years has highlighted vulnerabilities in the country's ICT infrastructure. Reported violations of electronic data tripled between 2010 and 2012 from 54,832 incidents to 166,801, according to official figures.[76] Whether politically or financially motivated, these breaches affect a significant proportion of the population, yet ordinary users are barely protected or compensated.[77] Recent investigations revealed that over 15 million voters had their electronic information illegally obtained and traded for use in mobile SMS campaigns prior to the April 2012 general election.[78]

Major incidents during the coverage period include a massive cyberattack against three major South Korean banks and the country's two largest broadcasters on March 20, 2013.[79] The government announced on April 10 that it had traced the attacks to six computers in North Korea, concluding that the military intelligence agency in Pyongyang was responsible.[80] In May 2012, the state-run educational TV station EBS, reported hackers had accessed personal data belonging to more than four million of its website subscribers, and one of the three telecommunication companies, KT, estimated 8.8 million of its customers' personal information was stolen between February and July.

[74] Maekyeong, "First Three-strikeouts for 'Heavy Uploaders,' 11 Accounts Ordered Suspended" [in Korean], *MK News*, http://news.mk.co.kr/newsRead.php?year=2010&no=596419

[75] Cory Doctorow, "South Korea Lives in the Future (of Brutal Copyright Enforcement)," *Boing Boing*, March 30, 2013, http://boingboing.net/2013/03/30/south-korea-lives-in-the-futur.html; Open Net Korea, "International Human Rights Organisations in Support for the Abolition of the Three-strike Rule," *Open Net Korea*, April 1, 2013, http://opennet.or.kr/1529.

[76] Statistics Korea, "Incidents of Personal Information Violation" [in Korean], *e-National Indicators*, accessed July 2013, http://www.index.go.kr/egams/stts/jsp/potal/stts/PO_STTS_IdxMain.jsp?idx_cd=1366&bbs=INDX_001&clas_div=C&rootKey=1.48.0#.

[77] Soon-taek Kwon, "KT's Penalty as Small as [US$613,000] After Having Lost Personal Information of 8.73 Million Customers" [in Korean], *MediaUs*, December 13, 2012, http://www.mediaus.co.kr/news/articleView.html?idxno=30287.

[78] Joonho Choi et al., "Voters' Personal Information Floating Around During Elections—One Agency Sends Out as Many as 40 Million Texts" [in Korean], *Joongang Ilbo*, July 5, 2012, http://article.joins.com/news/article/article.asp?total_id=8665527&ctg=1200.

[79] Laura Sciuto, "South Korea Hit Hard by Massive Cyber-Attack," *PBS NewsHour Extra*, April 1, 2013, http://www.pbs.org/newshour/extra/2013/04/south-korea-hit-hard-by-massive-cyber-attack/.

[80] Agence France-Presse, "S. Korea probe says North behind cyber attack," *The Straits Times*, April 10, 2013, http://www.straitstimes.com/breaking-news/asia/story/s-korea-probe-says-north-behind-cyber-attack-report-20130410.

SRI LANKA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	16	15
Limits on Content (0-35)	18	20
Violations of User Rights (0-40)	21	23
Total (0-100)	**55**	**58**

* 0=most free, 100=least free

POPULATION: 21 million
INTERNET PENETRATION 2012: 18 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The cabinet expanded the application of the Press Council Act to digital media, introducing operation fees and the threat of prosecution for website owners (see **LIMITS ON CONTENT**).
- Police briefly detained nine staff from two news websites; one of their colleagues survived an apparent abduction attempt (see **VIOLATIONS OF USER RIGHTS**).
- Select ISPs blocked three domestic Tamil-language news sites that documented anti-land grab protests (see **LIMITS ON CONTENT**).
- The exile-run *TamilNet* news website—blocked since 2007—withstood cyberattacks that tried to force it offline (see **VIOLATIONS OF USER RIGHTS**).
- Social media sites spreading anti-Muslim rumors and hate speech attracted thousands of supporters, including top officials (see **LIMITS ON CONTENT**).

INTRODUCTION

Increasing internet penetration in Sri Lanka has encouraged the development of news websites, and more users are leveraging social media for socioeconomic and political activism. Yet the government's efforts to regulate and punish dissenting views have undermined the internet's empowering impact.

Since coming into power in 2005, the ruling United People's Freedom Alliance (UPFA) has pursued an ambitious ICT policy to improve internet access and digital literacy through developments like the e-Sri Lanka project initiated in 2002.[1] However, civil conflict with the Liberation Tigers of Tamil Eelam (LTTE)—which ended in May 2009—hindered investment in the information and communication technology (ICT) sector and expansion of the internet across the country. In January 2007, the government made its first attempt to clamp down on internet freedom in response to reportage on the military campaign against the LTTE and civilian casualties.[2]

Content restrictions continued post-war. In 2012, a handful of Tamil news websites were blocked and the administration extended a draconian act governing traditional news outlets to online media, undercutting the government's own recognition of the role of ICTs in promoting access to information. Website owners can challenge censorship at the Supreme Court, but one such petition was rejected out of hand in May 2012. Meanwhile, officials from the highest ranks of government openly harassed their critics. Nine website staffers were detained on charges that proved to be spurious, while a journalist working for one of the same platforms narrowly avoided an apparent abduction attempt. He had reason for concern. Another web journalist, Prageeth Ekneligoda, has been missing since 2010, when colleagues believe he was abducted by government agents.

Suppressing opposition is a hallmark of the UPFA government's offline policies, too. In 2013, parliament defied the Supreme Court to dismiss Chief Justice Shirani Bandaranayake for alleged financial misconduct after she blocked passage of an economic development bill involving one of President Mahinda Rajapaksa's brothers.[3] Sri Lanka rejected 98 out of 210 recommendations from states participating in the United Nations Human Rights Council's Universal Periodic Review of its human rights practices in November 2012, breaking a record for belligerence—no other participating country has rejected more than 95. Disregarded recommendations included ensuring a climate in which "all citizens are able to freely express their opinions and beliefs, without fear of reprisal or retribution;" undertaking measures to allow "access to public information, in particular on alleged violations of human rights;" and one to "refrain from restricting access to and banning websites."[4]

---

[1] Information Communication Technology Agency, "Programmes," accessed July 2013, http://www.icta.lk/en/programmes.html.
[2] "Tamilnet Blocked in Sri Lanka", BBC Sinhala, June 20, 2007, http://www.bbc.co.uk/sinhala/news/story/2007/06/070620_tamilnet.shtml.
[3] "Sri Lanka Lawyers Boycott Chief Justice Ceremony," BBC, January 23, 2013, http://www.bbc.co.uk/news/world-asia-21155932.
[4] "Lanka Rejects 98 Recommendations at UPR," *The Sunday Leader*, November 5, 2012, http://bit.ly/QijPB1.

OBSTACLES TO ACCESS

Eighteen percent of the population had internet access in 2012,[5] as an expanding economic sector and growing youth population drove demand for online services. Government expenditure and private investment in ICTs have led to the implementation of several projects for the development of an island-wide telecommunications infrastructure.[6] In July 2011, the Telecommunications Regulatory Commission (TRC) announced plans to establish Wi-Fi zones in schools, government buildings and public transport areas to expand access.[7] A few reports in 2012 indicate some Wi-Fi zones are now available at railway stations and other public areas.[8]

Internet connectivity has become more affordable in the past two years with the cheapest broadband connections priced at just under $5 a month. Internet service providers (ISPs) lowered monthly rates in 2011 to combat the high market price and low computer ownership that has limited Sri Lanka's broadband penetration.[9] In January 2013, telecom operators welcomed a move by the TRC to reduce a tax on broadband internet access by 50 percent.[10] This has resulted in lower monthly bills for internet subscribers and an increased customer base.[11]

The two largest ISPs are Dialog Axiata and Sri Lanka Telecom (SLT). SLT commands more than 50 percent of the market, and a majority of its shares is owned by the state; it also has the largest fiber-optic national backbone.[12] While the broadband market is competitive, there is no legal requirement for SLT to sell backbone access to its competitors. In contrast, Dialog Axiata has allowed wholesale access to its backbone network.[13]

Sri Lanka's mobile penetration was nearly 96 percent in 2012.[14] Mobile broadband connections are increasingly popular, with monthly subscriptions as low as $3 a month, and the availability of pre-

---

[5] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[6] Ministry of Finance and Planning, "Annual Report 2010," 89, http://www.treasury.gov.lk/reports/annualreport/AnnualReport2010-eng.pdf; "Sri Lanka Dialog to Invest US$150mn in Expansion," *Lanka Business Online*, February 11, 2011, http://www.lankabusinessonline.com/fullstory.php?nid=754125283.

[7] Damith Wickremasekara, "Lanka to Get Wi-Fi Zones," *The Sunday Times* (Colombo), July 31, 2011, http://sundaytimes.lk/110731/News/nws_14.html.

[8] "Airtel Lanka Paints Trains and Stations Red," *Lanka Business News*, September 27, 2012, http://www.lankabusinessnews.com/12.09.September/194.Airtel.html; "SLR to Install Wi-Fi___33 in Top Ten Railway Stations", *Asian Mirror*, September 14, 2012, http://www.asianmirror.lk/english/index.php/news/10163-slr-to-install-wi-fi-in-top-10-railway-stations-. See also, Dialog, "Wi-Fi Hotspots," accessed July 2013, http://www.dialog.lk/personal/broadband/wi-fi/wi-fi-hotspots/.

[9] Rohan Samarajiva, "Sri Lanka: Leased Line Prices to be Lowered to Encourage BPO Business and Internet Use," *Lirne Asia*, March 9, 2011, http://bit.ly/hlSXBl.

[10] "Sri Lanka Reduces Broadband Tax to Promote Internet Use," *Colombo Page*, January 1, 2013, http://www.colombopage.com/archive_12B/Jan01_1357023715CH.php.

[11] Rukshana Rizwie, "Telcos Upbeat Over Levy Reduction," *The Nation*, January 6, 2013, http://www.nation.lk/edition/biz-news/item/14305-telcos-upbeat-over-levy-reduction.html.

[12] Helani Galpaya, *Broadband in Sri Lanka: Glass Half Full or Half Empty?* (Washington, D.C.: infuse/The World Bank, 2001), http://www.broadband-toolkit.org/.

[13] Galpaya, *Broadband in Sri Lanka.*

[14] International Telecommunication Union, "Mobile-cellular Telephone Subscriptions, 2000-2012."

paid one-time access packages. However, the high cost of internet-capable handsets hinders mobile broadband penetration.[15]

With over 7.5 million subscribers,[16] Dialog Axiata is also the largest mobile service provider. Etisalat is the second largest, with 4.2 million customers,[17] followed by SLT subsidiary Mobitel with 3.8 million and Airtel-Bharti Lanka with 1.8 million.[18] Hutchison Telecommunications' client base is under one million.[19] In January 2013, Dialog Axiata introduced the country's first commercial 4G LTE broadband service.[20] Other than Mobitel, which announced the launch of its 4G LTE network immediately after Dialog,[21] other providers have yet to introduce 4G LTE services.[22]

Low digital literacy represents a major barrier to ICT use. Although Sri Lanka's literacy rate is approximately 91 percent,[23] only 20 percent of the population knows how to use a computer on their own.[24] Digital literacy is lower in rural areas where the high cost of personal computers limits access for lower-income families, schools with digital facilities lack corresponding literacy programs, and software is often incompatible with the Sinhala and Tamil languages. As part of the e-Sri Lanka project, the government's Information Communication Technology Agency has sought to address this imbalance, establishing rural community centers to promote ICT access and services.[25] The government also reported computer acquisition rates increasing faster in rural than in urban areas between 2005 and 2009.[26] Notwithstanding significant progress in building infrastructure and implementing important e-governance projects like the Government Information Centre, local journalists have criticized certain aspects of the development, saying high-value contracts were awarded based on cronyism, while some facilities complained of faulty equipment.[27]

There were no recent reports of large-scale interruptions to connectivity during the coverage period of this report, although they have occurred in the past. SLT temporarily severed internet and 8,000 mobile phone connections in the predominantly Tamil-speaking north and east in 2007,

---

[15] Zulfath Suaheed, "Sri Lanka Mobile Internet Usage Poised for Frowth: Nielsen," *Lanka Business Report*, March 4, 2011, http://www.lbr.lk/fullstory.php?nid=201103041615077468.
[16] "UNICEF Partners Dialog on Child Abuse Concerns", *The Sunday Times*, October 7, 2012, http://bit.ly/19cpm4o.
[17] "Internet Drive," *Lanka Business Online*, August 21, 2012, http://www.lankabusinessonline.com/fullstory.php?nid=1005071680.
[18] Bandula Sirimanna, "Mobitel Reached 3.8 Million Subscribers by Nov. 2010," *The Sunday Times*, January 9, 2011, http://sundaytimes.lk/110109/BusinessTimes/bt46.html.
[19] "Sri Lanka Hutchison Unit Subscribers Down," *Lanka Business Online,* April 26, 2010, http://www.lankabusinessonline.com/fullstory.php?nid=682328361.
[20] "Sri Lanka's Dialog Launches 4G-LTE services," *Lanka Business Online*, December 30, 2012, http://www.lankabusinessonline.com/fullstory.php?nid=1454080943.
[21] "Sri Lanka Mobitel Launches 4G-LTE."
[22] Duruthu Edirimuni Chandrasekera, "Etisalat to Head Start on 4G," *The Sunday Times*, February 10, 2013, http://www.sundaytimes.lk/130210/business-times/etisalat-to-head-start-on-4g-31822.html.
[23] UNICEF, "Sri Lanka Statistics," accessed July 2013, http://www.unicef.org/infobycountry/sri_lanka_statistics.html.
[24] Department of Census and Statistics, "Computer Literacy Survey – 2009," http://www.statistics.gov.lk/CLS/BuletinComputerLiteracy_2009.pdf.
[25] Nenasala, "Establishment of Nenasalas," accessed July 2013, http://www.nanasala.lk/.
[26] Media Center for National Development of Sri Lanka, "Computer Literacy Among Sri Lankans is in the Ascension," June 23, 2010, http://www.development.lk/news.php?news=620.
[27] "ICTA Responds to Business Times Report on E-Government Project," *Business Times*, January 6, 2013, http://bit.ly/1bmHPwO.

then center of the conflict with the LTTE, and still a militarized zone.[28] The war also caused severe lags in infrastructure development for the northern and eastern provinces. Since its conclusion, the government has made up some of this ground, thereby boosting the regions' economic growth. The process of development, however, has been criticized for causing issues with respect to land ownership that threaten to further marginalize the local Tamil community.[29]

As a national regulatory body, the TRC's actions lack transparency and independence.[30] Under the Eighteenth Amendment of the Constitution ratified in 2011—which removed term limits to the executive presidency—the president can appoint the heads and members of all commissions, subverting legislative guarantees for the independence of the TRC and other statutory institutions.[31] Rajapaksa cemented control of the TRC by appointing his permanent secretary as its chairman.[32] The TRC's interventions to restrict online content and pronouncements on strengthening online regulation have been partisan, extralegal, and repressive.[33]

LIMITS ON CONTENT

In 2012, the government restricted content supporting its political opposition, instructing ISPs to block a handful of Tamil news websites. Broader online news reporting also came under heightened limitations. The cabinet amended a punitive Press Council Act to regulate online as well as traditional news media, imposing costly registration and maintenance fees on website owners and leaving them liable to prosecution for content violations. Anti-Muslim hate speech spread on social media, apparently with the backing of top leaders, and has prompted violent attacks.

Local and international freedom of expression groups have documented dozens of websites blocked at different times in Sri Lanka since 2007, though the interventions lack a legal framework or judicial oversight.[34] Implementation is not properly coordinated or comprehensive, with some targeted websites available at times on one or more ISPs and at other times completely inaccessible. Officials cite ill-defined national security measures to legitimize these measures, though websites have been blacklisted for content including human rights issues, government accountability, corruption and political violence. Censors have targeted the political opposition and independent news, including Tamil websites, sites run by Sri Lankans in exile, and citizen journalism platforms, though usually without acknowledging a political motive. The government also restricts access to

[28] "Cutting off Telecoms in Sri Lanka Redux…," *Groundviews*, January 30, 2007, http://groundviews.org/2007/01/30/cutting-off-telecoms-in-sri-lanka-redux/.
[29] M.A. Sumanthiran, "Situation in North-Eastern Sri Lanka: A Series of Serious Concerns," *dbsjeyaraj*, October 23, 2011, http://dbsjeyaraj.com/dbsj/archives/2759.
[30] Under the Telecommunications Act No. 21 of 1994, the Minister of Telecommunications and Information Technology has sole discretion in issuing licenses and imposition of license conditions based on the recommendations of the TRC.
[31] "Eighteenth Amendment to the Constitution," October 2010, http://www.priu.gov.lk/Cons/1978Constitution/18th%20Amendment%20To%20Sri%20Lanka%20Constitution%20(2).pdf.
[32] Democratic Socialist Republic of Sri Lanka, "Statutory Institutions and Ministries under the Executive President," accessed July 2013, http://www.president.gov.lk/about_presidency.php.
[33] Sarath Kumara, "Sri Lankan government prepares new Internet restrictions," *World Socialist Web Site*, February 15, 2010, http://www.wsws.org/articles/2010/feb2010/slmd-f15.shtml.
[34] Centre for Policy Alternatives, "Chapter 4: Restriction of Content on the Internet" in *Freedom of Expression on the Internet*, (November 2011), http://www.scribd.com/doc/73393066/Freedom-of-Expression-on-the-Internet-in-Sri-Lanka.

pornographic websites, and police sought to ban access to pornography on mobile phones in 2009.[35]

In 2011, the government announced plans to introduce more comprehensive legislation to control internet use, including the use of Facebook, ostensibly to crackdown on child abuse online.[36] As of mid-2013, none had been put forward, and officials rely on vague directives to control content. In 2011, for example, the ministry of mass media and information introduced a registration policy for websites carrying ill-defined "content relating to Sri Lanka or the people of Sri Lanka,"[37] a move unsupported by law which could potentially be used to hold owners responsible for information posted by users. Local news outlets reported in early 2012 that the ministry had rejected over 50 registrations due to "false and incomplete" registration details, though how they assessed the veracity and which websites were affected remains unclear.[38] And in March 2012, the defense ministry's Media Centre for National Security directed news organizations to submit SMS news alerts containing content related to "national security and security forces" for prior approval,[39] shortly after coverage of the killing of three soldiers in the northern province.[40] The Centre did not outline a legal basis for the directive; SMS news alerts continue to be disseminated by news operators, but there has been a noticeable lack of coverage of military issues.

Under the current system, state officials monitor websites for sensitive political content and direct the TRC to blacklist them, which in turn requests ISPs to block access. They are compelled to comply: Under the country's telecommunications act, ISPs must apply to the ministry for mass media and information for a license, according to specifications laid out by the TRC, who can make recommendations regarding whether or not a license is granted; the ministry can also impose conditions on a license, requiring the provider to address any matter considered "requisite or expedient to achieving" TRC objectives.[41] It is not clear if the TRC can impose other financial or legal penalties on telecommunications companies. To date, however, no company is known to have challenged its requests or sought judicial oversight.

It is not clear whether the government has resources to implement deep-packet inspection (DPI) that would enable real time filtering and other, more sophisticated censorship methods. In 2010, local news reports said IT military intelligence experts from China—where such methods are well-established—were assisting the government in blocking "offensive" websites.[42] Despite anecdotal

[35] Indika Sri Aravinda, "Police Seek Mobile Porn Ban," *Daily Mirror*, May 12, 2010, http://www.dailymirror.lk/news/3705-police-seeks-mobile-porn-ban.html.
[36] Indika Sri Aravinda, "Government to Monitor Internet," *The Sunday Leader*, December 18, 2011, http://www.thesundayleader.lk/2011/12/18/government-to-monitor-internet/.
[37] "Website Ban Further Broadened on News Director General Notification," *Lanka-E-News*, November 5, 2011, http://www.lankaenews.com/English/news.php?id=12427.
[38] Sulochana Perera, "Fifty Website Registrations Turned Down," *Ceylon Today*, March 25, 2012, http://www.ceylontoday.lk/16-3899-news-detail-fifty-website-registrations-turned-down.html.
[39] "New Censorship of SMS News in Sri Lanka," *Groundviews*, March 12, 2012, http://groundviews.org/2012/03/12/new-censorship-of-sms-news-in-sri-lanka/.
[40] "New Censorship of SMS News in Sri Lanka," *Groundviews*.
[41] Centre for Policy Alternatives, *Freedom of Expression on the Internet* (2011), 30.
[42] Bandula Sirimanna, "Chinese Here for Cyber Censorship," *The Sunday Times*, February 14, 2010, http://sundaytimes.lk/100214/News/nws_02.html.

reports that some Sri Lankan telecoms have DPI capabilities to enhance mobile data services, however, there is no evidence they have been used to censor content.

ISPs periodically blocked sites hosted both in and outside the country in 2012. In June, Dialog and SLT blocked at least three domestic Tamil-language news websites without advance warning or justification. The sites had reported on protests organized by the Tamil National Alliance, a coalition of Tamil political parties, against alleged government-orchestrated land grabs in the north and east.[43] Without official notification of the reason for the blocks, it was not possible to confirm whether they came in reprisal for those reports. The exile-run news website *TamilNet* has been blocked since 2007 for its support of Tamil rebels. Local internet users reported it was patchily accessible through some fixed-line and mobile broadband networks during that time.[44]

In July 2012, the ministry of mass media announced that it would "close down" all websites "engaged in mudslinging campaigns targeting politicians and other individuals."[45] Rather than acting against individual sites, however, the ministry directed the cabinet to amend the notorious Press Council Act No.5 of 1973, making news websites subject to the same draconian content regulation as traditional media. The act prohibits the publication of profanity, obscenity, "false" information about the government or fiscal policy, and official secrets. It also allows the president-appointed Council to impose punitive measures on the violators of its provisions, including possible prosecution. The legislation had lain dormant under previous administrations until President Rajapaksa reactivated it after the end of the war in June 2009. Strenuous objections from the international freedom of expression community failed to prevent the government extending the restrictions to digital media.[46] The amendment instituted a hefty registration fee of LKR 100,000 ($790), plus an annual renewal fee of LKR 50,000 ($395), costs which threaten to inhibit the emergence of new websites and force existing ones out of operation.[47] It failed to define what constitutes "news," providing leeway for authorities to scrutinize a wider range of online platforms like blogs or social media.[48]

There is no independent body in Sri Lanka content providers can turn to if they are censored. Instead, they must file a fundamental rights application with the Supreme Court to challenge blocking or other restrictions. Lack of trust in the country's politicized judiciary and fear of

[43] "A New Spate of Web Censorship in Sri Lanka?" *Groundviews*, June 26, 2012, http://groundviews.org/2012/06/26/a-new-spate-of-web-censorship-in-sri-lanka/.
[44] Sanjana Hattotuwa, "Tamilnet.com Accessible Once More in Sri Lanka via SLT ADSL," *ICT for Peacebuilding* (blog), August 5, 2010, http://ict4peace.wordpress.com/2010/08/05/tamilnet-com-accessible-once-more-in-sri-lanka-via-slt-adsl/.
[45] Normas Palihawadana, "Mudslinging Websites Will be Closed–Govt.," *The Island*, July 3, 2012, http://www.island.lk/index.php?page_cat=article-details&page=article-details&code_title=55928.
[46] Bob Dietz, "Defense Tools for Sri Lanka's Online Onslaught," *CPJ Blog*, July 25, 2012, http://cpj.org/blog/2012/07/defense-tools-for-sri-lankas-online-onslaught.php; "Media Skeptical over Press Council Act Amendments," IFEX, July 30, 2012, http://www.ifex.org/sri_lanka/2012/08/03/press_council_act/.
[47] "Rs.100,000 to be Charged from News Websites," *Daily Mirror*, July 12, 2012, http://www.dailymirror.lk/news/20228-cabinet-approves-to-amend-the-press-council-law.html.
[48] "Defining News Hinders Websites Registration," *The Nation*, July 15, 2012, http://www.nation.lk/edition/news-online/item/8321-defining-'news'-hinders-websites-registration.html.

retaliatory measures represent significant obstacles for the petitioner.[49] In December 2011, one settled out of court, agreeing to several TRC conditions—such as removing links to blocked content—in return for restored access.[50]

The absence of clear laws and conflicting official statements also complicate the process of launching legal challenges. In November 2011, officials acknowledged blocking at least five locally-hosted news websites, including the *Sri Lanka Mirror* and *Lanka-E-News,* citing concerns about defamation in the wake of stories about corruption and human rights violations that implicated high-ranking officials. One official accused the sites of publishing "character assassinations" of the president, while another said they were blocked for failing to register with the media ministry.[51] Members of the local Free Media Movement brought a fundamental rights petition challenging the ministry's grounds for blocking unregistered sites—which has no legal basis—but the Supreme Court rejected it in May 2012.[52]

The government actively encourages self-censorship "on matters that would damage the integrity of the island," and many mainstream news websites comply, increasing the importance of citizen journalism and exile-run sites to the media landscape.[53] Online platforms of the main state-run newspaper and broadcasting network support the UPFA government.[54] These and official government websites have waged smear campaigns against government critics in the past.[55]

In early 2013, hate speech against the Muslim community spread online when a Sinhala Buddhist extremist group gained a considerable following on social media.[56] Although most of the webpages supporting these groups have since been removed, they were critical of many Muslim practices, some based on unfounded rumor.[57] The group's violent rhetoric led to the attack of mosques and Muslim-owned businesses, as well as isolated incidents of assault.[58] No legal action was taken

---

[49] International Crisis Group, "Sri Lanka's Judiciary: Politicised Courts, Compromised Rights," Asia Report No.172, January 30, 2009, http://www.crisisgroup.org/en/regions/asia/south-asia/sri-lanka/172-sri-lankas-judiciary-politicised-courts-compromised-rights.aspx.

[50] S.S. Selvanayagam, "Website Previously Blocked now Permitted to Operate by SC," *DailyFT*, December 16, 2011, http://www.ft.lk/2011/12/16/website-previously-blocked-now-permitted-to-operate-by-sc/.

[51] Charles Haviland, "Sri Lanka blocks websites for 'maligning' president," BBC News, November 7, 2011, http://www.bbc.co.uk/news/world-asia-15621160.

[52] Bob Dietz, "Sri Lanka Supreme Court Slams Door on Websites," *CPJ Blog*, May 17, 2012, http://cpj.org/blog/2012/05/sri-lanka-supreme-court-slams-door-on-websites.php.

[53] Dinidu De Alwis, "Media Should Exercise Self-Censorship," *Ceylon Today*, March 23, 2012, http://www.ceylontoday.lk/16-3780-news-detail-media-should-exercise-self-censorship-lakshman-yapa.html.

[54] "Namal's Disclosure of Family Embarrassment," *The Island*, December 21, 2011, http://www.island.lk/index.php?page_cat=article-details&page=article-details&code_title=41622.

[55] World Organization Against Torture, "Sri Lanka: Smear Campaign Against Ms. Sunila Abeysekara, Ms. Nimalka Fernando, Dr. Paikiasothy Saravanamuttu and Mr. Sunanda Deshapriya," March 27, 2012, http://www.omct.org/human-rights-defenders/urgent-interventions/sri-lanka/2012/03/d21700/; Committee to Protect Journalists, "In Sri Lanka, Censorship and a Smear Campaign," news alert, July 14, 2009, http://cpj.org/2009/07/in-sri-lanka-censorship-and-a-smear-campaign.php.

[56] Sanjana Hattotuwa, "Anti-Muslim Hate Online in Post-War Sri Lanka", February 1, 2013, http://sanjanah.wordpress.com/2013/02/01/anti-muslim-hate-online-in-post-war-sri-lanka/.

[57] Charles Haviland, "The Hardline Buddhists Targeting Sri Lanka's Muslims," BBC News, March 25, 2013, http://www.bbc.co.uk/news/world-asia-21840600.

[58] Haviland, "The Hardline Buddhists Targeting Sri Lanka's Muslims."

against the group's members, and prominent public officials—including the president's brother, Defense Secretary Gotabhaya Rajapaksa—openly supported them.[59]

Despite the restrictions, there are still diverse, accessible sources of information online in English, Sinhala, and Tamil, including on socioeconomic and political issues. Some previously blocked content was available in 2013, including *Colombo Telegraph*, a news and commentary website run by exiled Sri Lankan journalists, which ISPs censored in 2011.[60] Citizen media site *Groundviews* and its sister site *Vikalpa* were also operating freely, despite SLT temporarily blocking them for a day in 2011. [61] The platforms report on topics that would otherwise not be covered by the mainstream media, provide links to circumvention tools that can be used, and lobbied the United Nations Human Rights Council to address abuses during Sri Lanka's 2012 Universal Periodic Review.[62] Although online content by Human Rights Watch and Transparency International has been blocked in Sri Lanka in the past when the groups criticized the Rajapaksa administration,[63] websites belonging to international media and human rights groups were freely accessible in 2013. A handful of popular blogs publish political content and dissenting narratives. Authorities have temporarily blocked website domains on blog platforms in the past,[64] but YouTube, Facebook, Twitter and international blog-hosting services were accessible and widely-used for the anonymous or pseudonymous critique of governance, development, and human rights abuses in 2013.

VIOLATIONS OF USER RIGHTS

Sri Lankan authorities have a poor record of abusing vaguely worded laws to imprison or harass legitimate content producers, and arrested nine website staff in 2012 on charges that did not stand up to investigation. Physical attacks and threats against journalists, including many linked to government actors, have decreased since the war and its immediate aftermath. But the failure to investigate past incidents cast a long shadow, perpetuating fear and self-censorship, and significant rights violations persist. In 2013, one web journalist fought off an abduction attempt; another, Prageeth Ekneligoda, remained missing for a third year since his colleagues accused government security forces of abducting him in reprisal for supporting the political opposition in 2010 elections. High-profile leaders publicly threatened individual internet users and journalists with impunity, and obstructed opposition efforts to improve transparency through right to information legislation recommended by a post-war reconciliation commission.

[59] D.B.S. Jeyaraj, "Defence Secretary Gotabhaya Rajapaksa Openly Supportive of "Ethno Religious Fascist" Organization Bodhu Bala Sena," *dbsjeyaraj*, March 10, 2013, http://dbsjeyaraj.com/dbsj/archives/17939
[60] "We are Blocked But Will Not be Stopped," *Colombo Telegraph*, December 26, 2011, http://www.colombotelegraph.com/index.php/we-are-blocked-but-we-will-not-be-stopped/.
[61] "Groundviews Blocked and Unblocked," *ICT for Peacebuilding* (blog), June 22, 2011, http://ict4peace.wordpress.com/2011/06/22/groundviews-blocked-and-unblocked/.
[62] "#UPRLKA: Complete Tweet Archive and Related Visualisation Around Sri Lanka's UPR Review," *Groundviews*, November 2, 2012, http://groundviews.org/2012/11/02/uprlka-complete-tweet-archive-and-related-visualisation-around-sri-lankas-upr-review/.
[63] Reporters Without Borders, "Internet Enemies," March 12, 2009, http://bit.ly/tus9bB.
[64] "More Websites Including ghs.google.com Blocked in Sri Lanka?," *ICT for Peacebuilding* (blog), July 29, 2009, http://ict4peace.wordpress.com/2009/07/29/more-websites-including-ghs-google-com-blocked-in-sri-lanka/.

While the right to freedom of speech, expression, and publishing is guaranteed under Article 14 (1)(a) of Sri Lanka's constitution, it is subject to numerous restrictions for the protection of national security, public order, racial and religious harmony as well as morality. There is no constitutional provision recognizing internet access as a fundamental right or guaranteeing online freedom of expression. A culture of impunity, circumvention of the judicial process through arbitrary action, and a lack of adequate protection for individuals and their privacy, compound the poor enforcement of freedom of expression guarantees.

The Supreme Court has called freedom of expression from "diverse and antagonistic sources" indispensable to democracy.[65] In 2012, however, it rejected a fundamental rights petition brought by members of the local Free Media Movement questioning the media ministry's right to block websites for failure to register.[66] By doing so, it missed a critical opportunity to check the government's use of vague directives to control online content.

Several laws with overly broad scope lack detailed definitions and can be abused to prosecute or restrict legitimate forms of online expression. Computer crimes and intellectual property rights laws allow information contained within computers to be admissible in civil and criminal proceedings. Publishing official secrets, information about parliament that may undermine its work, or "malicious" content that incites violence or disharmony could result in criminal charges.[67] In 2011, the ministry of justice mooted a new obscene publications act to extend anti-pornography laws to electronic media, but did not correct the existing act's failure to define "obscene."[68] Thus far, the ministry has made no announcements regarding the legislation's implementation.

As in past years, the government obstructed right to information legislation which would promote citizens' access to documents held by government agencies and ministries. The Lessons Learnt and Reconciliation Commission—a post-war commission of inquiry appointed by President Rajapaksa in May 2010—recommended RTI legislation as a necessary step towards addressing past and ongoing rights violations.[69] Yet the government left it to the cabinet to establish a time frame for completing a draft,[70] and UPFA parliamentarians rejected an opposition-backed bill in 2011 on grounds that the government would table its own version.[71] In July 2012, Secretary to the ministry of mass media and information, Charitha Herath, said national security concerns would continue to

[65] Centre for Policy Alternatives, *Freedom of Expression on the Internet in Sri Lanka,* (August, 2010), 54, http://www.eldis.org/vfile/upload/1/document/1008/FOE%20and%20Internet%20in%20Sri%20Lanka.pdf.
[66] Bob Dietz, "Sri Lanka Supreme Court Slams Door on Websites," *CPJ Blog*, May 17, 2012, http://cpj.org/blog/2012/05/sri-lanka-supreme-court-slams-door-on-websites.php.
[67] Respective legislation: Official Secrets Act No. 32 of 1955; Parliament (Powers and Privileges) (Amendment) 1997; Prevention of Terrorism (Temporary Provisions) Act No. 48 of 1979.
[68] "Tough New Laws against Porn," *Daily Mirror*, October 24, 2011, http://www.dailymirror.lk/news/14318-tough-new-laws-against-porn.html.
[69] The report further recommended that steps be taken to "prevent the harassment and attacks on media personnel and institutions." See, The Official Website of the Government of Sri Lanka, *Report of the Commission of Inquiry on Lessons Learnt and Reconciliation* (2011), 197-8, http://www.priu.gov.lk/news_update/Current_Affairs/ca201112/FINAL%20LLRC%20REPORT.pdf.
[70] Section 9.115e, "National Plan of Action to Implement the Recommendations of the LLRC," *Government News Portal*, July 26, 2012, http://www.priu.gov.lk/news_update/Current_Affairs/ca201207/20120726national_plan_action.htm.
[71] "Govt. Rejects our Right to Know," *The Sunday Times*, "The Political Editor," June 26, 2011, http://sundaytimes.lk/110626/Columns/political.html.

delay the bill. Freedom of expression experts noted those concerns were disingenuous, since international RTI legislation routinely prevents documents that would jeopardize national security being released into the public domain.[72]

In mid-2012, police arrested nine staff from two news websites. Criminal Investigations Department (CID) officials raided the offices of the *Sri Lanka Mirror* and *Sri Lanka X News* in June on grounds of "propagating false and unethical news on Sri Lanka."[73] The action had scant foundation in law. The CID obtained a search warrant and arrested the employees citing violation of Articles 115, 118 and 120 of Sri Lanka's penal code. Articles 118 and 120 broadly deal with defamation and the incitement of contempt and hatred, although Article 118 was repealed in 2002, and Article 115 covers conspiracy to overthrow government by coercion.[74] The journalists were released on bail the day after their arrest, though investigators later said their computers contained further grounds for prosecution, including content that violated the Obscene Publications Act—although the alleged obscenity was unpublished[75]—failure to register the website, ridiculing the president, and evidence of an attempted coup.[76] While the case was finally set aside due to the CID failing to conclude investigations,[77] the journalists filed a fundamental rights petition with the Supreme Court citing illegal arrest, violation of their right to free expression and legal occupation. Hearings are ongoing. Media activists, rights organizations, and diplomatic missions viewed the arrests as intimidation stemming from the websites' pro-opposition reporting. [78] External Affairs Minister G.L Peiris' defense of the raid compounded that view when he accused the sites of turning "deaf ears to repeated warnings to tone down their coverage."[79]

Extrajudicial surveillance of personal communications is prohibited under the Telecommunications Act No.27 of 1996. However, a telecommunications officer can intercept communications under the direction of a minister, a court, or in connection with the investigation of a criminal offence. There is no provision under the legislation that requires officials to notify users who are targets of surveillance, and journalists and civil society activists believe their phone and internet communications are monitored.

---

[72] Bob Dietz, "No Right to Information in Sri Lanka", *CPJ Blog*, August 7, 2012, http://www.cpj.org/blog/2012/08/no-right-to-information-in-sri-lanka.php.

[73] "Websites Propagating False News Sealed—MOD," *Daily Mirror*, June 30, 2012, http://www.dailymirror.lk/news/19885-websites-propagating-false-news-sealed-mod.html.

[74] Wasantha Ramanayake, "Petitioners Claim They were Arrested Under Law Repealed Ten Years Ago," *The Sunday Times*, July 29, 2012, http://www.sundaytimes.lk/120729/news/petitioners-claim-they-were-arrested-under-law-repealed-10-years-ago-7461.html.

[75] Farook Thajudeen, "Pornographic Material from Sri Lankamirror Computers—CID," *Daily Mirror*, July 23, 2012, http://www.dailymirror.lk/news/20514-phonographic-material-from-srilankamirror-computers-cid.html.

[76] "SL Mirror Computers Returned," *Ceylon Today*, September 18, 2012, http://www.ceylontoday.lk/13044-print.html.

[77] T. Farook Thajudeen, "Sri Lanka Mirror Case Set Aside," *Daily FT*, September 19, 2012, http://www.ft.lk/2012/09/19/sri-lanka-mirror-case-set-aside/

[78] Human Rights Watch, "Sri Lanka: Halt Harassment of Media", July 3, 2012, http://www.hrw.org/news/2012/07/03/sri-lanka-halt-harassment-media, "US Concern over Media Harassment," *Daily Mirror*, June 30th, 2012, http://www.dailymirror.lk/news/19892-us-concern-over-media-harassment.html.

[79] "Sri Lanka FM Hits Back Over Crackdown Criticism," *NY Daily News*, July 4, 2012, http://india.nydailynews.com/newsarticle/4ff5d22ec3d4ca667400000a/sri-lanka-fm-hits-back-over-crackdown-criticism.

Sri Lanka lacks substantive laws for the protection of individual privacy and data. Official statements lauding state surveillance make this absence a particular concern for internet users,[80] as do policies like website registration, which civil society groups fear could be used to hold registered site owners responsible for content posted by users, or to prevent government critics writing anonymously.[81] Digital activists in Sri Lanka also believe Chinese telecoms ZTE and Huawei, who collaborated in the development and maintenance of Sri Lanka's ICT infrastructure, may have inserted backdoor espionage and surveillance capabilities.[82]

There were no new reports of arrests made for information shared by e-mail or text message. Sri Lankan police have made such arrests in the past, though whether the content was obtained through extrajudicial surveillance is not clear. Following the 2010 presidential election, a Media Centre for National Security spokesman told local journalists that police had detained "a few people" for text messages criticizing the outcome of the polls, without elaborating.[83] News reports said the detainees had disseminated similar content on Facebook and Twitter. The TRC denied tracing critical commentators through social media, and an unnamed source in the telecommunications industry told Sri Lanka's *Sunday Times* the police could have been acting on complaints from message recipients. In 2009, police traced an e-mail containing nude photographs sent to President Rajapaksa and his brother Gotabhaya through an internet protocol address and remanded the sender, who had illegally accessed a personal rival's e-mail account to send the offensive content with motives of revenge.[84] Local media mistakenly reported that a blogger had been arrested for writing about Rajapaksa online.

A ministry of defense program to register mobile phone users for the purpose of "curbing negative incidents" was introduced in 2008 and revisited in 2010 after service providers failed to ensure that subscribers registered.[85] Real-name subscriptions are already normal procedure, but the call for registration in 2010 required further information, including photo identification and up-to-date residential details. Unregistered users risk disconnection if they failed to comply, though no cases have been reported.

---

[80] "It's Ok for Government to Infiltrate Online Privacy of Sri Lankan Citizens?," *ICT for Peacebuilding* (blog), April 17, 2010, http://ict4peace.wordpress.com/2010/04/17/its-ok-for-government-to-infiltrate-online-privacy-of-sri-lankan-citizens/.

[81] Centre for Policy Alternatives, "Arbitrary Blocking and Registration of Websites: The Continuing Violation of Freedom of Expression on the Internet," November 9, 2011, http://cpalanka.org/arbitrary-blocking-and-registration-of-websites-the-continuing-violation-of-freedom-of-expression-on-the-internet/.

[82] ZTE Corporation signed an agreement with Mobitel to develop its 4G LTE network and carried out successful trials in May 2011, while SLT's ADSL infrastructure is supported by Huawei. See, "Sri Lanka's Mobitel and ZTE Corporation Carry Out the First Successful 4G(LTE) Trial in South Asia," ZTE, May 17, 2011, http://wwwen.zte.com.cn/en/press_center/news/201105/t20110517_234745.html; Ranjith Wijewardena, "SLT Tie Up With Huawei to Expand Broadband Internet Coverage," Nanasala, September 29, 2006, http://www.nanasala.lk/article_more.php?id=10; Sanjana Hattotuwa, "Are Chinese Telecoms Acting as the Ears for the Sri Lankan Government?," *Groundviews*, February 16, 2012, http://groundviews.org/2012/02/16/are-chinese-telecoms-acting-as-the-ears-for-the-sri-lankan-government/.

[83] "Monitoring Cyberspace to Regulate Anti-Govt. Content," February 14, 2010, http://sundaytimes.lk/100214/News/nws_50.html.

[84] "The Arrest of the 'Blogger' in Sri Lanka: Crowd-Sourcing Trumps Traditional Media Follow Up," *ICT for Peacebuilding*, November 8, 2009, http://bit.ly/19QWs6j.

[85] Bandula Sirimanna, "Sri Lanka to Tighten Mobile Phone Regulations," *The Sunday Times*, October 31, 2010, http://sundaytimes.lk/101031/BusinessTimes/bt32.html.

Online reporters, like their counterparts in traditional media, were attacked by forces on both sides during Sri Lanka's civil conflict. Unsolved cases include the 2005 murder of *TamilNet* co-founder Dharmeratnam Sivaram, who was found dead in a high-security area outside parliament.[86] The UN Human Rights Council adopted a resolution urging the government to investigate war crimes in March 2012, but the trend of violence against traditional journalists and an overarching culture of impunity continues, exacerbating self-censorship and chilling freedom of expression online.

Disappearances continue to be a problem in post-war Sri Lanka: Local English-language media documented 57 incidents between January 1 and July 9, 2012. [87] International news reports and rights groups say government soldiers are responsible for the notorious "white van" abductions—named after the vehicle often used to carry them out—a claim the administration denies.[88] Shantha Wijesooriya, an investigative journalist for the news website *Sri Lanka X News*, avoided an apparent abduction attempt in the capital, Colombo, on July 5, fighting off unidentified men in plain clothes when they tried to bundle him into a white vehicle.[89] *Lanka-E-News* journalist and cartoonist Prageeth Ekneligoda has been missing since January 24, 2010, after the website backed the political opposition in elections. His wife and colleagues believe government agents abducted him, and police have made no effort to investigate his disappearance, despite widespread international pressure.[90] Officials have denied Ekneligoda is even missing, saying he sought asylum overseas.[91] The inaction on his case, combined with other methods of intimidation including arson attacks and legal harassment, forced *Lanka-E-News* and its editor out of the country.[92]

Officials harassed and threatened freedom of expression advocates and journalists with impunity in 2012. In March, Minister for Public Affairs, Mervyn Silva, threatened to break the limbs of four individuals—some with a prominent online presence—for criticizing the government at the UN,[93] acknowledging he had driven veteran journalist Poddala Jayantha out of the country to support the threat.[94] Frederica Jansz, editor of the *Sunday Leader* newspaper, fled Sri Lanka in November after Gotabhaya Rajapaksa threatened her during a telephone conversation.[95]

---

[86] Committee to Protect Journalists, "Journalists Killed, Sri Lanka: Dharmeratnam Sivaram," accessed January, 2013, http://www.cpj.org/killed/2005/dharmeratnam-sivaram.php.
[87] "A Disappearance Every Five Days in Post-War Sri Lanka," *Groundviews,* August 30, 2012, http://groundviews.org/2012/08/30/a-disappearance-every-five-days-in-post-war-sri-lanka/#.
[88] "Abduction squads in Sri Lanka target foes of powerful," August 22, 2012, http://www.washingtontimes.com/news/2012/aug/22/abduction-squads-in-sri-lanka-target-foes-of-power/?page=all.
[89] Indika Gamage, "Sri Lanka: A Journalist's Abduction Attempt Thwarted," Journalists for Democracy in Sri Lanka, July 9, 2012, http://www.jdslanka.org/index.php/2012-01-30-09-30-42/media/130-sri-lanka-a-journalist-abduction-attempt-thwarted.
[90] T. Farook Thajudeen, "Prageeth Eknaligoda Disappearance Case Still Going On," *Daily FT*, December 24, 2011, http://www.ft.lk/2011/12/24/prageeth-eknaligoda-disappearance-case-still-ongoing/; Bob Dietz, "UN Heard Eknelygoda's Cry For Help; Husband Still Missing," *CPJ Blog*, May 21, 2011, http://bit.ly/Gzv9o2.
[91] Chris Kamalendran, "Eknaligoda Case: Focus on Ex-AG," *The Sunday Times*, December 11, 2011, http://sundaytimes.lk/111211/News/nws_24.html.
[92] Bob Dietz, "Sandhya Eknelygoda Speaks for Sri Lanka's Disappeared," *CPJ Blog*, September 4, 2012, http://cpj.org/blog/2012/09/sandhya-eknelygoda-speaks-for-sri-lankas-disappear.php.
[93] "Mervyn Threatens to Break Limbs of Journos," *Daily Mirror*, March 23, 2012, http://dailymirror.lk/news/17607-mervyn-threatens-to-break-limbs-of-journos.html.
[94] Jayantha has lived in exile since six unidentified men abducted and beat him in June 2009. "Arrest This Thug!," *The Nation*, March 25, 2012, http://www.nation.lk/edition/editorial/item/4312-arrest-this-thug.html.
[95] Frederica Jansz, "Gota Goes Berserk," *The Sunday Leader*, July 8, 2012, http://bit.ly/RBuH9u.

Cybercrime is a growing problem in Sri Lanka, with illegal breaches of social media and e-mail accounts becoming more common.[96] Networks associated with the LTTE have been reported attempting to hack into national security networks and carry out web defacement attacks.[97] The government has recognized the need to strengthen its defensive capability, yet critics fear technology bought for this purpose could be used to restrict legitimate expression.[98]

Cyberattacks have also targeted government critics. Twice in 2012, in February and September, *TamilNet* reported it had been hit with distributed denial of service (DDoS) attacks, which force a website to crash by bombarding its host server with requests for information.[99] These attacks cannot be definitively attributed the government agents. However, Media Minister Keheliya Rambukwella openly publicized his intent to incapacitate the site as early as June 2007. "We are looking for hackers to disable…*TamilNet* but could not find anyone yet," he told journalists.[100]

[96] "681 SL Cyber Security Incidents So Far in 2011," *The Sunday Times*, October 16, 2011, http://www.sundaytimes.lk/111016/BusinessTimes/bt31.html.
[97] "Sri Lanka Army Commander says Cyber War Still Continues," *Colombo Page*, February 22, 2011, http://www.colombopage.com/archive_11/Feb22_1298388902CH.php.
[98] Centre for Policy Alternatives, *Freedom of Expression on the Internet* (2011), 42.
[99] "TamilNet: 27.02.12 DDoS Attack Disrupts TamilNet Web Traffic," *TamilNet*, February 27, 2012, www.tamilnet.com/art.html?catid=13&artid=34927; "TamilNet: 29.09.12 DDoS Attacks on TamilNet Foiled," *TamilNet*, September 29, 2012, www.tamilnet.com/art.html?catid=13&artid=35610.
[100] "TamilNet Blocked in Sri Lanka," BBC Sinhala, June 20, 2007, http://www.bbc.co.uk/sinhala/news/story/2007/06/070620_tamilnet.shtml.

SUDAN

	2012	2013
INTERNET FREEDOM STATUS	N/A	NOT FREE
Obstacles to Access (0-25)	n/a	17
Limits on Content (0-35)	n/a	19
Violations of User Rights (0-40)	n/a	27
Total (0-100)	**n/a**	**63**

* 0=most free, 100=least free

POPULATION: 33.5 million
INTERNET PENETRATION 2012: 21 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Large-scale antigovernment protests known as "Sudan Revolts" erupted in Khartoum in June 2012 and spread throughout the country. The protests led to the government's first crackdown on internet users (see **LIMITS ON CONTENT**).
- The intelligence service's Cyber Jihadist Unit ramped up its efforts to censor antigovernment content, target cyber-dissidents, and manipulate online information during and following the protests (see **LIMITS ON CONTENT**).
- Numerous bloggers and online journalists were arrested or harassed for their involvement with the June 2012 protests (see **VIOLATIONS OF USER RIGHTS**).
- In December 2012, a new draft press law was presented to the national assembly that is likely to include provisions regulating online media (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

On September 25, 2013, Sudan experienced a complete internet blackout following the outbreak of antigovernment protests in Khartoum over the suspension of fuel subsidies.[1] According to research conducted by the internet intelligence company, Renesys, no networks were available in Sudan around 1:00pm local time as a result of either a catastrophic technical problem or a centrally coordinated effort to disable all access to the internet.[2] While the government's hand behind the shutdown could not be confirmed at the time of writing, its timing strongly supports suspicions of government involvement, particularly since Renesys reported a similar—albeit a smaller-scale and shorter—outage on the Sudatel network in June 2013 ahead of another large protest.[3]

INTRODUCTION

Much of Sudan's history since 1955 has been preoccupied by civil war and persistent conflict, resulting in the displacement of millions of Sudanese and a situation of economic disfranchisement for the majority of the country. As a result, 46.5 percent of the population lives below the official United Nations poverty line as of the end of 2012.[4] Nevertheless, the discovery of oil in South Sudan prior to the region's independence from the north in July 2011 has led to an economic boom for the country's elite and ruling party over the last 10 years, which has in turn translated into gains for a number of sectors, particularly the telecommunications sector.[5]

Increasingly affordable and reliable internet service has enabled Sudanese citizens to use digital media tools to share information, communicate with the international community, document news not covered in the heavily censored traditional media, and organize protest movements against government repression. This online engagement and activism, however, has led the Sudanese government under President Omar al-Bashir to increasingly crackdown against internet freedom through various tactics that include: growing censorship of opposition news outlets and forums online; the deployment of a Cyber Jihadist Unit to monitor social media websites and hack into activists' accounts;[6] and the harassment and arrest of digital media activists and online journalists; among other tactics.

---

[1] "At least seven killed in Sudan as anti-government violence flares," *Al Arabiya*, September 26, 2013, http://english.alarabiya.net/en/News/middle-east/2013/09/25/Internet-access-shut-down-in-Sudan-amid-Khartoum-riots.html.
[2] Andrea Peterson, "Sudan loses Internet access – and it looks like the government is behind it," *Washington Post*, September 25, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/25/sudan-loses-internet-access-and-it-looks-like-the-government-is-behind-it/.
[3] Renesys Corporation, Twitter post, June 29, 2013, 4:33pm, https://twitter.com/renesys/status/351060825722736640/photo/1.
[4] United Nations Development Programme, "Status of MDGs in Sudan in 2012," http://www.sd.undp.org/mdg_fact.htm.
[5] "Economic Impact of Mobile Communications in Sudan," Zain Group and Telefonaktiebolaget LM Ericsson, June 5, 2009, http://www.ericsson.com/res/thecompany/docs/sudan_economic_report.pdf.
[6] Interview with a press freedom advocate and journalist in Khartoum, Sudan, January 16, 2012.

Internet restrictions and government repression against online users intensified during and following widespread antigovernment protests known as "Sudan Revolts" that erupted in June 2012 and were fueled in large part by digital media tools. In a country where traditional media journalists have for decades faced routine censorship, detention, and violence, the events in 2012 led the government to target bloggers and cyber-dissidents for the first time, with some facing detentions for up to two months and one case of torture reported. Others fled Sudan for fear of their lives after being subjected to threats, sexual assault, or torture.

OBSTACLES TO ACCESS

The internet in Sudan is affordable and widely accessible in big cities and towns. According to the International Telecommunications Union (ITU), internet penetration grew from 19 percent in 2011 to 21 percent in 2012, representing 7.5 million users in a country of 34.2 million.[7] However, the number of users could be somewhat higher as internet-enabled mobile phones have become widespread and cheaper in recent years. The National Telecommunications Corporation (NTC),[8] the government regulatory body, reported over 27 million cell phone subscriptions in Sudan as of December 2012,[9] in addition to a telecom network coverage of 88 percent of the population that extends to at least 800 cities and towns,[10] including remote parts of the war-torn region of Darfur.[11] The ITU noted a mobile phone penetration of over 60 percent at the end of 2012.[12]

Following the 2005 Comprehensive Peace Agreement (CPA) signed between the government of Sudan and the South Sudanese rebels, the Sudan People's Liberation Movement (SPLM), the telecommunications industry expanded at an unprecedented rate as thousands of Sudanese expatriates returned from the diaspora. During this time, prices for pre- and post-paid services were cut in half, and companies began offering wireless connections to serve the growing number of cafes and hotels.[13]

By regional and international standards, Sudan's telecommunications infrastructure is among the most developed and affordable, with Sudan recording the lowest average post-paid rate per minute in the Middle East and North Africa in 2012.[14] There are four licensed telecommunications operators in Sudan: Zain, MTN, Sudatel—which provide both internet and mobile phone

[7] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[8] Founded in 1996, the NTC regulates the telecommunications industry in Sudan, give licenses to telecommunications operators as well as protects the national security of the state, among other duties.
[9] *"Mobile cellular subscriptions 2012," Statistics data, National Telecommunications Corporation, last modified May 6, 2013, http://www.ntc.gov.sd/images/stories/docs/English/mobile_cellular_subscription.pdf.*
[10] "Economic Impact of Mobile Communications in Sudan."
[11] "Telecom Networks Coverage," Statistics data, National Telecommunications Corporation, last modified May 6, 2013, http://www.ntc.gov.sd/images/stories/docs/English/coverage.pdf.
[12] International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2012."
[13] Interview with individuals in the telecommunications industry in Khartoum, Sudan, January 7-25, 2012.
[14] Mohamed Salam, "Sudan Tops MENA Region on Mobile Services Sales Tax," *IT News Africa*, October 3, 2012, http://www.itnewsafrica.com/2012/10/sudan-tops-mena-region-on-mobile-services-sales-tax.

services—and Canar, which provides fixed phone lines and home internet.[15] MTN and Sudatel both offer broadband internet, with Sudatel being the first to introduce 3.75G technology.[16] Zain also offers fast internet through its USB and mobile phone internet services, though along with MTN, it leases its access to the international internet from Sudatel and Canar. Zain, MTN, and Canar are foreign-owned companies,[17] while Sudatel has 22 percent of its shares owned by the government.[18]

Telecommunication companies began providing affordable mobile phone internet services in 2010, which allowed a growing number of citizens, especially students, to browse the internet from their mobile devices and led to a marked increase in the use of social media websites such as Facebook. As of January 2013, a monthly subscription on the Sudani network costs SDG 9 ($1.50) for 1 GB, while unlimited monthly internet costs SDG 15 ($2.50) and SDG 21 ($3.50) on MTN and Zain, respectively.[19] The three companies also offer daily unlimited internet for rates that do not exceed SDG 1 ($0.16).[20]

Aside from mobile internet, users also access the internet from personal desktops that cost between $71 and $100, or from laptop computers that start at $110 for a brand-new device. Second-hand laptops and computers are widely available, and users can make payments towards a computer in weekly or monthly installments. Internet access is enabled through a high-speed internet USB modem, which costs $11 on the Zain network, while 5 GB of data per month costs $4.50. The Sudani network gives its subscribers free internet USB sticks upon the purchase of internet packages ranging from three months (at $21) to one year (at $78).[21] Nevertheless, there were less than 25,000 fixed broadband subscriptions at the end of 2012, representing 0.05 percent of the population, according to the ITU.[22] Cybercafes, which are concentrated in market areas, charge an average of $0.30 per hour,[23] though the number of cybercafes in Khartoum state has decreased noticeably since the early 2000s as the internet has become cheaper and more accessible to the public.

The availability of fast internet in Sudan is largely a result of competition between the four main telecommunications companies. Under normal circumstances, the internet is relatively fast, operating at advertised speeds of up to 21Mbps on the Zain network in Khartoum and at 7.2Mbps in other areas. However, during the antigovernment protests in June and July 2012, there were reports of extremely slow internet speeds before it became completely inaccessible to users on the Zain and Sudani networks for a number of hours before the June 29th protests, according to some

[15] Interview with an expert from the telecommunications industry in Khartoum, Sudan, January 17, 2013.
[16] "Background," Sudani Company, accessed January 2013, http://sudani.sd/PublicOne/Content/Sudani/Background.
[17] The majority shareholders are Kuwaiti for Zain, South African for MTN, and Emirates for Canar. See: "Economic Impact of Mobile Communications in Sudan."
[18] OpenNet Initiative, "Internet Filtering in Sudan," August 7, 2009, https://opennet.net/sites/opennet.net/files/ONI_Sudan_2009.pdf.
[19] Based on calls made to customer care centers for the three telecommunications networks in Khartoum, Sudan, January 7-10, 2013.
[20] Calls made to customer care centers.
[21] Calls made to customer care centers.
[22] International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2012."
[23] Research conducted in January 2013.

independent reports.[24] It remains unconfirmed whether the service disruptions were due to intentional government interference or technical issues, though the disruptions prompted immediate fears among activists that the authorities would follow Mubarak's lead in Egypt and shut down the internet altogether.[25] Most recently in June 2013, and again in September 2013 (after this report's coverage period), the internet intelligence corporation Renesys confirmed two separate internet blackouts that were reportedly directed by the government in advance of large protests (see "Editor's Note on Recent Developments").[26]

While access to the internet is gradually expanding in Sudan, comprehensive economic sanctions imposed by the U.S. government against the al-Bashir regime since 1997 have been a hindrance to the free access of various ICTs and new media tools.[27] In 2010, the sanctions were amended to authorize the export of certain communications technologies to boost the free-flow of information,[28] though as of 2013, the amended sanctions remain ineffective for most Sudanese in many respects. For example, important software such as anti-virus suites, e-document readers, and rich-content multimedia applications are blocked and inaccessible for users to download. Additionally, software security updates are unavailable, forcing users to rely on outdated versions that make their computers and devices vulnerable to malware and other technical attacks. Smartphones and tablets are also affected, as online stores where users can download and update applications are inaccessible in Sudan. Savvy users use circumvention tools such as proxies and virtual private networks (VPNs) to access these blocked services, but ordinary users likely miss out on these key ICT tools. This problem of accessibility poses a serious security threat to activists and human rights defenders, making them unable to use these technologies in their work and potentially exposing them to state surveillance and censorship (see "Violations of User Rights").

The NTC regulates the ICT sector in Sudan. Founded in 1996 and housed under the Ministry of Telecommunications, the government body produces telecommunications statistics, monitors the use of the internet, introduces new technology into the country, and seeks to develop the country's telecommunications and IT industry. Although it is a state body, the NTC receives grants from international organizations such as the Intergovernmental Authority on Development and the World Bank, and its website describes the body as "self-financing."[29]

---

[24] Personal experience of a Freedom House consultant based in Khartoum. See also: Amira Al Hussaini, "Sudan: Netizens Verify Internet Blackout Rumours," *Global Voices*, June 22, 2012,http://globalvoicesonline.org/2012/06/22/sudan-netizens-verify-internet-blackout-rumours/.

[25] Melody Zhang, "Internet Blackout in Sudan?" OpenNet Initiative (blog), June 27, 2012, https://opennet.net/blog/2012/06/internet-blackout-sudan.

[26] Andrea Peterson, "Sudan loses Internet access – and it look like the government is behind it," *Washington Post*, September 25, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/25/sudan-loses-internet-access-and-it-looks-like-the-government-is-behind-it/.

[27] "What you Need to Know About U.S. Sanctions—Sudan," U.S. Department of the Treasury, June 25, 2008, http://www.treasury.gov/resource-center/sanctions/Programs/Documents/sudan.pdf.

[28] "Treasury Department Issues New General License to Boost Internet-Based Communication, Free Flow of Information in Iran, Sudan and Cuba," U.S. Department of the Treasury, press release, March 8, 2010, http://www.treasury.gov/press-center/press-releases/Pages/tg577.aspx.

[29] "Annual Budgets," The National Telecommunications Council, October 16, 2010, http://www.ntc.gov.sd/index.php?n=b3B0aW9uPWNvbV9jb250ZW50JnZpZXc9YXJ0aWNsZSZpZD04JkI0ZW1pZD0xNjYmbGFuZz11aw.

LIMITS ON CONTENT

In response to the nationwide "Sudan Revolts" protests in June 2012, the government blocked three news websites and amped up its use of the Cyber Jihadist Unit to target key protest participants and manipulate the online information landscape. YouTube was unilaterally blocked for a period following the viral spread of an offensive anti-Islam video in September 2012.

The 2001 National Strategy for Building the Information Industry explicitly acknowledges the blocking and filtering of internet content considered "immoral" and "blasphemous." The NTC is relatively transparent about the content it blocks, reporting that 95 percent of blocked material is related to pornography.[30] Tests last conducted by the OpenNet Initiative in 2009 confirmed that websites with "sexually explicit" content were blocked, in addition to some dating and hacking websites and those that facilitated anonymous browsing or circumvention.[31]

Social media websites such as Facebook and Twitter are not blocked, though Sudan has blocked YouTube and the popular Sudanese forum and news website *Sudanese Online* for various periods since 2008 in response to content deemed too sensitive by the regime, such as articles on the war in Darfur.[32] The blocks typically range from a few days to a few weeks, and when a website becomes accessible again, it can take some time for content to be fully restored. The most sustained and long-term blocking of websites followed the June-July 2012 "Sudan Revolts" protest movement. On June 25, 2012, the NTC blocked the online newspapers *Sudanese Online*, *Al-Rakoba*, and *Hurriyat*,[33] the latter two of which are known to be anti-government. *Hurriyat* is based in Kampala, Uganda and its editorial staff is comprised of prominent journalists who left Sudan after enduring numerous court trials for their writings. *Al-Rakoba*, on the other hand, has a number of anonymous journalists inside Sudan but is managed by a group based in the Gulf region.[34] As of April 2013, only *Al-Rakoba* has been unblocked, while *Hurriyat* and *Sudanese Online* remain blocked and accessible only through anonymous browsing programs such as Tor. From some connections, adding an "s" to the "http" component of a blocked URL to access it via the secure https protocol can open the website.

In mid-September 2012, the NTC blocked the entire YouTube platform following the viral spread of the "Innocence of Muslims" video that instigated protests in Sudan and across the Muslim world,[35] though the website was still accessible using https. Two days before YouTube was banned, protests against the film took place in front of the U.S. and German embassies in Khartoum,

[30] "Blocking Or Unblock Websites," National Telecommunications Corporation, last modified May 6, 2013, http://www.ntc.gov.sd/index.php?n=b3B0aW9uPWNvbV9ja2Zvcm1zJnZpZXc9Y2tmb3JtcyZpZD0xJkl0ZW1pZD0xMjkmbGFuZz11aw%3D%3D.
[31] OpenNet Initiative, "Internet Filtering in Sudan."
[32] OpenNet Initiative, "Internet Filtering in Sudan."
[33] Eva Galperin, "Sudan Revolts, Government Cracks Down on Dissent," Electronic Frontier Foundation, July 10, 2012, https://www.eff.org/deeplinks/2012/07/sudan-revolts-government-cracks-down-dissent.
[34] Interview with journalist affiliated with *Al-Rakoba* in Khartoum, Sudan, January 20, 2013.
[35] "Sudan Blocks YouTube Over Anti-Islam Film – Sources," *Sudan Tribune*, September 17, 2012, http://www.sudantribune.com/spip.php?article43916.

leading to the deaths of two protesters following clashes with the police.[36] The platform was unblocked in November 2012 and remains so as of May 2013.

The Internet Service Control Unit within the NTC manages the filtering of online content, and users can submit requests through the NTC website to either block or unblock websites "that are deemed not containing pornography."[37] Nevertheless, the NTC does not specify whether the requests to block or unblock extend to political websites. Users attempting to access a blocked site are met with a black page that explicitly states, "This site has been blocked," by the NTC and includes a contact e-mail address at filtering@ntc.gov.sd.[38]

As a result of growing online censorship, some opposition news outlets have begun to move their servers outside the country to avoid blocking. For example, *Sudanese Online* currently operates from the United States, while *Sudan Tribune* is based out of France and *Al Taghyeer* ("Change"), a new online newspaper launched on May 3, 2013 on World Press Freedom Day, is based in the United Kingdom.[39] This trend will likely continue if a draft media law with implications for digital news is passed (see "Violations of User Rights").

Despite increasing instances of internet censorship in 2012, online newspapers have had more freedom than traditional media outlets, which are frequently subject to pre-publication censorship, confiscations of entire press runs of newspapers, and warnings from National Intelligence and Security Service (NISS) agents against reporting on certain taboo topics.[40] Restrictions on traditional news outlets increased following the National Security Act of 2010, which gives the NISS permission to arrest journalists and censor newspapers under the pretext of "national security."[41] As such, many print newspapers have begun to circulate censored or banned material on their websites and social media pages. For example, *Al-Midan* newspaper, the mouthpiece of the communist party, has used Facebook and its website to publish articles since May 2012. *Al-Jareeda* also uses its Facebook page to publish censored material. Nevertheless, the authorities have begun to crackdown against such forms of online journalism. At the end of 2012, one *Al-Jareeda* journalist reported that he was threatened by the NISS to prevent him from publishing an interview with a young politician on the newspaper's Facebook page after it was censored from the print version.[42]

In response to the Arab Spring events and the proliferation of anti-government protest movements organized on social media sites in early 2011, the ruling National Congress Party launched a Cyber

[36] "Sudan Protesters Storm German Embassy, Raise Islamic Flag," Reuters, September 14, 2012, https://www.nydailynews.com/news/world/sudan-protesters-storm-german-embassy-raise-islamic-flag-article-1.1159566.
[37] "Blocking Or Unblock Websites."
[38] Image of a blocked site: https://docs.google.com/file/d/0B6mgwvplJ6IadERXT3RTZW1jSkk/edit.
[39] Reem Abbas, "Sudan's Shift from Print to Online Newspapers," Doha Centre for Media Freedom, May 16, 2013, http://www.dc4mf.org/en/node/3740.
[40] Interview with an editor-in-chief in Khartoum, Sudan, August 2012.
[41] The NISS carries out arbitrary arrests, may detain an individual for up to 45 days without charges and can renew the detention period after the end of the 45-day period. NISS officers have total immunity from the law. "Sudanese Security Service Carries out Brutal Campaign Against Opponents," Amnesty International, July 19, 2010, http://www.amnesty.org/en/news-and-updates/report/sudanese-security-service-carries-out-brutal-campaign-against-opponents-2010.
[42] Interview with an activist, October 2012, Khartoum, Sudan.

Jihadist Unit to conduct "online defense operations" and "crush online dissent."[43] While the cyber jihadists existed on a smaller scale before 2011, the government began expanding the unit when it realized the powerful capacity of social media and online journalism to disseminate information, communicate events to the international community, and mobilize protests.

In 2011, a leaked document revealed that the Cyber Jihadist Unit employed over 200 individuals divided across different locations and who worked three shifts to ensure around the clock coverage, particularly during timeframes when internet traffic is highest, such as late at night and during the weekend.[44] More recent research found that the number of recruits increased in 2012, with the NISS recruiting heavily at government universities, especially at the police-owned Al-Ribat University.[45] The Unit seems to have adequate funding for training, and stipends are given to the young recruits who are mostly students or unemployed youth. According to private interviews, the cyber-jihadists have also received training courses in hacking and online monitoring in India and Malaysia, among other countries.

Based at the NISS, the Cyber Jihadist Unit proactively monitors content posted on blogs, social media websites, and online newspaper forums. The Unit also infiltrates online discussions in an effort to ascertain information about cyber-dissidents as well as spread misinformation. This strategy has been employed most prominently on the news forum, *Sudanese Online*, which is known for its popularity among antigovernment intellectuals, journalists, politicians and activists. When the government took notice of the website's influence in the mid-2000s, it planted contributors to spread misinformation, instigate problems between users, and discredit information written by members of the forum.[46]

In August 2012, a few weeks after a massive security crackdown subdued the wave of protests across the country, an exiled activist started a thread on *Sudanese Online* titled, "Accounts Targeted and Monitored by the Cyber-Jihad Unit," that included a list of 274 names, Facebook pages and groups and described the expanded technical capacities of the unit. Leaked to the exiled activist by "a trusted source,"[47] the list made evident that the unit's primary targets were online activists, particularly young people, whose social media accounts publish timely information about the protests and news about human rights violations.[48] Also included on the list were Facebook groups of university protest and social movements, such as the "University is Free and the Soldiers should Leave" group, and of youth movements such as Girifna ("We are fed up"), Sharara, and Sudan Change Now. One of the individuals targeted was Mohamed Hassan Alem (known as Boshi), who became popular after a video of him mocking a ruling party official went viral on YouTube in late

[43] E-mail interview with editors from *Hurriyat* and *Al-Rakoba*, January 2013; "Sudan to Unleash Cyber Jihadists," BBC News, March 23, 2011, http://www.bbc.co.uk/news/technology-12829808.
[44] "With the NCP's Documents: Operation Electronic Defense to Bring Down the Sudanese Revolution" [in Arabic], *Sudan Motion,* April 14, 2012, http://sudanmotion.com/index.php/news/3-sudan-news/4143-2012-04-14-10-30-28.
[45] Interview with telecommunications expert in Khartoum, Sudan, January 15, 2013.
[46] Interview with a press freedom advocate and journalist in Khartoum, Sudan, January 16, 2012.
[47] Bukhari Osman, "Accounts Targeted by Cyber Jihad Unit" [in Arabic], August 23, 2012, *Sudanese Online*, http://www.sudaneseonline.com/cgi-bin/sdb/2bb.cgi?seq=print&board=400&msg=1345716699&rn=1
[48] For example, the first name mentioned in the list was Amani Al-Agab, a well-known online activist who is very active on Sudanese forums as well as Facebook. There is little information available on Amani Al-Agab; however, it is known that she is outside Sudan. http://www.change.org/users/7806131

2011, leading to his arrest.[49] Najla Al-Sheikh, a popular Sudanese video-blogger and human rights documentarian whose YouTube page has nearly one million views,[50] and Wail Taha, a former editor of the online newspaper, *Hurriyat*, were also listed.

In 2012, the authorities began to employ social media tools to discredit and spread misinformation about the opposition, launching smear campaigns against activists such as Rudwan Dawod, a Darfurian humanitarian aid worker who was arrested in July 2012 during a non-violent demonstration. Two days after his arrest, a Facebook page was created accusing Dawod of being a part of a terrorist circle that was preparing to bomb Khartoum.[51]

With the growing popularity of forums such as *Sudanese Online* in the mid-2000s, citizens, especially young people, began creating their own blogs to voice their opinions, leading to considerable growth of the blogosphere over the past couple of years. The more active Sudanese bloggers write in the English language. As of early 2013, there were about 300 Sudanese blogs registered in the newly established Sudanese Bloggers Network,[52] compared to approximately 70 blogs in October 2011.[53]

Blogging has also become an important platform for journalists and writers who use it to publish commentary that is free from the restrictions leveled on newspapers, and to publicize their books. For example, the well-known Sudanese writer Abdul-Aziz Baraka Sakin uses his blog to publish sections of his books for preview by the public and to distribute his books that are currently banned.[54]

Blogs have also given ethnic, gender, and religious minorities a venue to express themselves. In 2007, a blogger known as "Black-Gay-Arab" appeared in the Sudanese blogosphere, taking many by surprise in a country where homosexuality is punished by the death penalty.[55] Documenting his life as a gay man in a conservative society and chronicling his family's attitude toward his sexuality, the blog eventually enabled its author and other Sudanese LGBT people to establish a website that became an association for the Sudanese LGBT community called Freedom Sudan.[56] Another blogger, Osman Naway from the Nuba minority ethnic group, uses his blog to spread awareness

---

[49] "Sudanese Activist Arrested Days After Heckling Ruling Party Official," *Sudan Tribune*, January 1, 2012, http://www.sudantribune.com/Sudanese-activist-arrested-days,41152.
[50] Nagla Elshakh's YouTube page, accessed May 24, 2013, http://www.youtube.com/user/naglaseed.
[51] Timeline photo on Facebook page of "Sudan.E.Army, posted July 4, 2012, https://www.facebook.com/photo.php?fbid=340853672655563&set=a.194049490669316.46463.194019520672313&type=1&relevant_count=1; John Zogby, "Sudanese Activist Charged With Terrorism," *On the Ground* (blog), *New York Times*, July 11, 2012, http://kristof.blogs.nytimes.com/2012/07/11/sudanese-activist-charged-with-terrorism/.
[52] Interview with the Sudanese Bloggers Network, January 23, 2013, http://sdunlimitedbloggers.blogspot.com/.
[53] Amir Ahmad Nasr, "Sudanese Bloggers," *Sudanese Thinker* (blog), March 26, 2009, http://www.sudanesethinker.com/sudanese-bloggers/.
[54] Abdul-Aziz Baraka Sakin is one of Sudan's most prolific writers. He is a novelist and short story writer who has published over six books and is also a campaigner for children's rights. He blogs at http://barakasakin.blogspot.com. See, Reem Abbas, "Comment is Free," *Guardian*, October 26, 2012, http://www.guardian.co.uk/commentisfree/2012/oct/26/secret-reading-sudan-banning-books.
[55] *Blackgayarab - Gay and Proud* (blog): http://black-gay-arab.blogspot.com/
[56] Freedom Sudan: The Sudanese LGBT Association: http://freedomsudan.webs.com/

about the persecution of citizens from the Nuba Mountains and to document the recently reignited war in the region.[57]

During the summer 2012 student protests against the government's harsh economic austerity plan, social media and e-mail became the primary tools used to mobilize, share information, and communicate as mobile phones became increasingly unsafe to use. According to youth activists, most communications between the protesters during that time were conducted through Whats App, a free mobile messaging application that can be accessed via mobile internet. The mobile app was considered a much safer mode of communication than phone calls or text messages, which the authorities could tap or track.[58] Nevertheless, an overwhelming number of activists interviewed for this report revealed a low awareness of digital security and limited knowledge of ways to stay digitally safe, such as how to delete a Skype conversation.

Meanwhile, digital media activism enabled the protests to spread from its starting point in Khartoum to numerous cities around the country,[59] gathering between hundreds and thousands of demonstrators to voice opposition against growing economic hardships in Sudan. Despite the effective use of digital media tools in mobilizing the widespread demonstrations, the government was ultimately successful in suppressing the movement through its violent crackdown against the protesters, journalists, and online activists. Consequently, the protest movement resulted in no concrete changes to the government's austerity plans.

Nevertheless, the internet continues to grow as a powerful tool for activists to fight for social, political, and economic change. In one prominent case, an online campaign helped lead to the eventual release of Jalila Khamis, an activist who spent nine months in detention without charge until December 13, 2012, when an online campaign mobilized a silent protest in front of the Women's Prison in Omdurman where she was being held, and she was produced in court. The campaign also informed many individuals, both inside and outside Sudan, of Khamis' case and made her trials a public event, with dozens of attendees waiting outside the courtroom at each trial and posting real-time updates of the trial proceedings on social media.[60] Khamis was finally released and acquitted of all charges on January 20, 2013 (see "Violations of User Rights").[61]

Another significant case of digital media activism erupted in early 2011 and continued through 2012 following the arrest and sexual assault of Girifna activist, Safia Ishaq, in January 2011. After her release, Girifna circulated a YouTube video in which Ishaq detailed the gang-rape she endured at the hands of three NISS agents while in detention, making her the first Sudanese woman to speak

[57] Osman Naway is a human rights activist and blogger from the Nuba Mountains in Southern Kordofan state. He is affiliated with Arry Organization for Human rights (http://arry.org/),which was closed by the Sudanese government in December 2012.
[58] Interviews with youth activists.
[59] Ismai'il Kushkush, "Protesters and the Police Clash in Sudan," *New York Times*, July 6, 2012, https://www.nytimes.com/2012/07/07/world/africa/in-sudan-protesters-clash-with-the-riot-police.html?_r=0.
[60] Interview with cyber-activist in Khartoum, Sudan, January 20, 2013.
[61] Amnesty International, "Sudan Releases Prisoner of Conscience," press release, January 20, 2013, http://www.amnesty.org/en/for-media/press-releases/sudan-releases-prisoner-conscience-2013-01-20.

publicly about sexual assault perpetrated by the authorities.[62] Her YouTube testimony led to a viral online campaign that helped the coalition, "No to Women's Oppression," mobilize public protests against the frequent cases of sexual assault experienced by Sudanese women, especially those who have voiced public opinion against the government.[63]

Nevertheless, the NISS took numerous journalists to trial for writing about the Ishaq case in local newspapers under charges of "publishing false information" and "jeopardizing the trust between the public and security forces."[64] The trials of those journalists also received significant public attention, and activists used Facebook and Twitter to mobilize a public presence at the court hearings. As of April 2013, Ishaq's case is still being heard at a regional African court,[65] though the government maintains its denial of the incident. Ishaq eventually fled Sudan due to increasing harassment.

VIOLATIONS OF USER RIGHTS

A draft media law was proposed in December 2012 that aims to further restrict media freedom in Sudan; it is also likely to include provisions to regulate online media. Numerous bloggers and online journalists were arrested or harassed for their involvement with the June 2012 protests, while a number of activists were prosecuted for their coverage of the conflict areas in Southern Kordofan and the Nuba Mountains. An online journalist was also tortured in 2012 for her social activism.

Freedom of speech, expression and association are nominally protected under the 2005 Interim National Constitution that was adopted as part of the 2005 Comprehensive Peace Agreement (CPA) between the government of Sudan and the Southern rebel group, though the constitution officially expired following the independence of South Sudan in July 2011. A permanent constitution is currently being drafted as of May 2013.

In 2007, Sudan enacted the Informatic Offences (Combating) Act (known as the IT Crime Act),[66] which does not guarantee free speech and criminalizes the establishment of websites that criticize the government, in addition to websites that publish defamatory material and content that disturbs public morality or public order.[67] Violations of the IT Crime Act involve fines and prison sentences between two to five years. While only one case of defamation has been filed under the IT Crime

[62] Maha El-Sanosi, "The Violation of Women's Rights in Sudan: In the Name of the Law?" *Afrika*, April 6, 2012, http://www.afrika.no/Detailed/21360.html.
[63] Amel Gorani, "Rape as a Tool of War," *Geopolitical Monitor*, December 29, 2011, http://www.geopoliticalmonitor.com/rape-as-a-weapon-of-war-4568/; "Safia Ishaq Talks," Girifna, February, 24, 2011, http://www.girifna.com/2602.
[64] Nahid Mohamed Al-Hassan, trial report by Girifna (not published), October 6, 2011, Khartoum, Sudan.
[65] The People's Court in the Gambia.
[66] "The Informatic Offences (Combating) Act, 2007," National Telecommunications Corporation, http://www.ntc.gov.sd/images/stories/docs/English/Informatics_offences_Act_2007.pdf.
[67] Abdelgadir Mohammed Abdelgadir, "Fences of Silence: Systematic Repression of Freedom of the Press, Opinion and Expression in Sudan," International Press Institute, 2012, http://www.freemedia.at/fileadmin/media/Fences_of_Silence-AbdelgadirMAbdelgadir-3.pdf.

Act since its enactment in 2007,[68] the Act inherently contradicts Sudan's constitutional protection of freedom of expression and fundamentally undermines internet freedom in the country.

For bloggers and online activists, the press and criminal laws have been more dangerous. In 2009, the government revised the highly restrictive 2004 Press and Printed Press Materials Law, which continued to allow for restrictions on the press in the interests of national security and public order and holds editors-in-chief liable for all content published in their newspapers.[69] There is no specific reference to online media, though the press law's broad wording allows for its application to online content. In December 2012, a new draft press law was presented to the national assembly that aims to further restrict media freedom in Sudan. While the draft law has yet to be publicly released, a member of the Sudanese National Council revealed in an interview with the Doha Centre for Media Freedom in April 2013 that the new law would include regulations on online media.[70] Meanwhile, the authorities also restrict media freedom through the 2010 National Security Act, which gives the NISS immunity from persecution and the permission to arrest, detain and censor newspapers under the pretext of national security.[71] Furthermore, Sudan's judiciary is not independent and has taken peremptory actions in cases of freedom of expression.

Since the Arab Spring events in 2011, journalists in Sudan have faced increasing harassment and repression,[72] with at least 20 journalists and editors subjected to fines, interrogations, detentions, jail sentences, or trials for charges ranging from defamation, publishing false information, or undermining the constitution in 2012.[73] According to the Sudanese Bloggers Network, bloggers and citizen journalists have also been increasingly harassed or detained in recent years, particularly during times of protest.

In one notable case, the popular blogger and Twitter-user Usamah Mohamed was arrested on June 22, 2012 while covering protests in the Burri neighborhood of Khartoum.[74] As one of the most prominent bloggers using the Twitter hashtag #SudanRevolts to live-tweet the events of the protest, Usamah was detained along with his brother for documenting the arrest of other protestors on Twitter and for posting a video on Al-Jazeera of himself explaining his reasons for taking part in

[68] Interview with a press freedom advocate in Khartoum, Sudan, January 16, 2012.
[69] Committee to Protect Journalists, "Repressive press law passed in Sudan," press release, June 11, 2009, http://www.cpj.org/2009/06/repressive-press-law-passed-in-sudan.php.
[70] Reem Abbas, "Proposed Sudan Media Law Targets Press Freedom," *Al-Monitor*, January 17, 2013, http://www.al-monitor.com/pulse/originals/2013/01/sudan-press-freedom.html#ixzz2OY2WyeL3; Ahmed Vall, "'New Law Will Grant Greater Media Freedom in Sudan,'" Doha Centre for Media Freedom, April 7, 203, http://www.dc4mf.org/en/content/new-law-will-grant-greater-media-freedom-sudan.
[71] "Sudanese Security Service Carries Out Brutal Campaign Against Opponents," Amnesty International, July 19, 2010, http://www.amnesty.org/en/news-and-updates/report/sudanese-security-service-carries-out-brutal-campaign-against-opponents-2010.
[72] "Journalists Face Increasing Harassment in Sudan," Amnesty International, May 3, 2012, http://www.amnesty.org/en/news/journalists-face-increasing-harassment-sudan-2012-05-02.
[73] Journalists are Amel Habbani, Nahid Al-Hassan, Faisal Mohamed Salih, Omer Al-Garrai, Saad Al-Deen Ibrahim, Fatima Ghazzali, Faiz Al-Seleik, Abdullah Al-Sheikh, Mohamed Lateif, Zeinab Mohamed Salih, Gafaar Al-Subki and Hassan Ishaq, among others.
[74] Interview with Sudanese Bloggers Network, January 23, 2013.

the demonstrations.[75] His brother, Asaad Mohamed, who is also popular on Twitter, was released a few hours after his arrest, while Usamah was transported to NISS offices where he was beaten for five hours after he refused to unlock his iPhone. Described by an NISS officer to other detainees as "the first to speak about the protests to the international community,"[76] Usamah was held for two months, during which he was subjected to long interrogations about his e-mail, Facebook, and other accounts on the opposition forums, *Al-Rakoba* and *Sudanese Online*.[77] NISS officers further accused Usamah of posting his video as part of a coordinated effort to take the Sudanese government to the International Criminal Court. He was released in early August 2012 without charges, along with scores of other detainees arrested during the protests.

The same allegation about the International Criminal Court was leveled against the prominent video-blogger Nagla Sid-Ahmed for her documentary work on Southern Kordofan—where rebels have fought against the government since June 2011 following rigged local elections—and the humanitarian situation in the Nuba Mountains. In the past few years, Sid-Ahmed had recorded over 5,000 videos on human rights abuses, detentions, and political events, leading her to become a target of NISS harassment and attack throughout 2012.[78] In January, NISS agents raided Sid-Ahmed's home and confiscated her laptop and cameras. In the following months, she was summoned for interrogation numerous times, particularly during the protests in June, and was often forced to stay in the NISS office for over 12 hours without food. Her home was also monitored, and she received messages on Facebook that threatened to harm her children. After months of harassment amid the deteriorating state of her health, Sid-Ahmed and her family left Sudan in July 2012. [79] In October, the NISS lodged a formal case against her in absentia, charging her with conspiracy against the state and inciting hatred, among other charges, under the Sudanese criminal law of 1991, which prescribe a minimum of three years in jail and a maximum of the death penalty if she returns to Sudan.[80]

In March 2012, teacher and activist Jalila Khamis was arrested from her home in the middle of the night after appearing in a YouTube video filmed by Nagla Sid-Ahmed in which she discussed the humanitarian situation in Southern Kordofan.[81] In May 2012, Sid-Ahmed was summoned for interrogation about Khamis's video and accused of spreading false information.[82] Meanwhile, Khamis remained in detention without charge until December 2012, when she was formally charged under six different articles of the 1991 criminal law, including Article 21 for "participation in the execution of a criminal conspiracy," Article 51 for "waging war against the state," and Article

[75] Interview with Usama Mohammed in Khartoum, Sudan, January 24, 2013; Reem Abbas, "Media and Bloggers Censored as Protests Spread Across Sudan," *UNCUT* (blog), Index on Censorship, July 2, 2012, http://uncut.indexoncensorship.org/2012/07/protests-sudan-intafada-censorship/.
[76] Reem Abbas, "Media and Bloggers Censored as Protests Spread Across Sudan."
[77] Reem Abbas, "Media and Bloggers Censored as Protests Spread Across Sudan."
[78] Interview with Girifna in Khartoum, Sudan, May, June 2012.
[79] "A Citizen Journalist and Activist in Forced Exile," Girifna, October, 7, 2012, http://www.girifna.com/6901.
[80] Interview with Girifna in Khartoum, Sudan, June 2012; "A Citizen Journalist and Activist in Forced Exile," *Sudanese Online*, October 5, 2012, http://www.sudaneseonline.com/news/6233-a-citizen-journalist-and-activist-in-forced-exile.html.
[81] Nagla AlSheikh's YouTube video, "Jalila Khamis Koko Tells the Suffering of the Nuba People" [in Arabic], June 15, 2011, http://www.youtube.com/watch?v=m9EPmxqMLfo; "Nuba Mountains Female Activist Arrested," Girifna, March 18, 2012, http://www.girifna.com/5080.
[82] Interview in Khartoum, Sudan, June 2012.

64 for "inciting hatred against sects or between them," among others.[83] The YouTube video was used as the main evidence against Khamis.

Following a month-long trial, international pressure, and a local campaign calling for her freedom, Khamis was finally released on January 20, 2013 after the prosecutor dropped five of the six charges due to insufficient evidence. While she was ultimately charged under Article 66 for the "publication of false news," which carries a maximum sentence of six months,[84] the ten months that Khamis had already spent in prison was deemed sufficient for her punishment. Nevertheless, Khamis' case sets a dangerous precedent for digital activism and will likely lead to increasing self-censorship and the disempowerment of bloggers and netizens who use social media to advocate for human rights in Sudan.

During the antigovernment demonstrations of 2012, hundreds of activists, journalists, and bloggers were arrested for their participation and coverage of the protest events, including the prominent blogger, Maha El-Sanosi. Although El-Sanosi was released the same day of her arrest on June 21, she was detained again a few days later during a house raid by 12 NISS officers in the middle of the night. She was later released on bail.[85] In a private interview, El-Sanosi expressed concern over the NISS's ability to find her home given the precautions she had taken to keep her whereabouts hidden.[86]

The government actively monitors internet communications, and the NISS regularly intercepts private e-mail messages.[87] The Sudan Police Department also monitors internet cafes to make sure that users do not access websites deemed immoral by the authorities.[88] Government monitoring and surveillance of online activists and journalists became particularly pronounced in 2012 during the "Sudan Revolts" protests. Mobile phones became an especially dangerous tool for activists, with one youth activist describing how the authorities "have the technology not only to tap your phone calls, but to figure out your location if you use your phone."[89] In one notable instance, the activist Mohamed Ahmed switched off his phone for a few days in early July 2012 to avoid arrest while in hiding from the NISS.[90] When he turned his phone back on as he was walking home to see his family, NISS officials roaming his neighborhood managed to track his location based on the nearest telecommunications tower and arrested him later that night.[91]

Mobile phone tapping and tracking was made more feasible in 2008 when a law was enacted requiring subscribers to register their SIM cards. MTN was ordered to disconnect prepaid subscribers who did not register their personal information by the deadline, resulting in the

[83] "Today Jalila Enters her 9th Month!" Girifna, December 15, 2012, http://www.girifna.com/7327. The other charges were under Article 50, undermining the constitutional system, Article 53, espionage against the country and Article 66, publication of false news.
[84] "Video: Jalila Khamis is Free!" Girifna, January 21, 2013, http://www.girifna.com/7724.
[85] "Sudan Arrests Activists as UN Calls for Calm," *al-Akhbar*, June 28, 2012, http://english.al-akhbar.com/node/9009.
[86] Interview in Khartoum, Sudan, June-July 2012.
[87] U.S. Department of State, "Sudan 2012 Human Rights Report," http://www.state.gov/documents/organization/204383.pdf.
[88] OpenNet Initiative, "Internet Filtering in Sudan."
[89] Interview in Khartoum, Sudan, August 1, 2012.
[90] A pseudonym was used here to protect the privacy and identity of this activist.
[91] Interview in Khartoum, Sudan, August 1, 2012.

telecom losing 1.1 million of its 2.2 million subscribers.[92] Nevertheless, it was still relatively easy to purchase a SIM card without providing personal information for activation until the June 2012 protests when the policy became more strictly enforced, particularly within the partially government-owned telecom, Sudani.[93]

Facebook has become increasingly monitored and used to track and incriminate activists for arrest.[94] During the June 2012 protests, the social media website was the first account detainees were asked to open while in detention, and private messages as well as the pages that activists "like" were checked to see if they were affiliated with a certain political party or social movement. Consequently, many young people stopped posting personal pictures on their profiles and began changing their Facebook names to pseudonyms to avoid being tracked. Detained activists were also pressured to provide the passwords to their e-mail accounts, leading the friends and family members of detainees to change passwords or delete accounts for activists while they were in detention.[95]

Despite the pervasive efforts to monitor and intercept internet and mobile communications, the government's technological capacity and expertise is seemingly low. Testimonies from released detainees reveal that security agents still document information manually and that security offices seem to lack computer technology. Testimonies also noted that NISS agents and the Cyber Jihadist Unit have very low levels of English-language competency.[96] This allows citizen journalists working in English to have slightly more freedom, since the authorities have thus far focused mainly on monitoring Arabic-language online content. As such, incidents of arrest and harassment of online journalists and bloggers writing in English have been uncommon.

Nevertheless, telecommunications providers are required to comply with government demands to proactively monitor communications and hand over user information. In 2009, for example, a leaked letter from the ruling party's secretary of political affairs to National Congress Party leaders was published on *Sudanese Online*, detailing a directive made to the four telecom operators in Sudan to "monitor and follow up on any call that harms the interests of the homeland" and to gather the phone numbers of SPLM leaders so they could be placed under surveillance.[97]

Journalists and activists in Sudan often face harassment, extralegal intimidation, and even torture at the hands of security agents. One egregious case of torture occurred in October 2012, when the online journalist and activist, Somia Hundusa, was kidnapped from the street as she left her house to buy food for her sick son.[98] While in detention, she was interrogated about her Facebook activity

[92] "Connecting Sudan," ITP, January 21, 2009, http://www.itp.net/544237-connecting-sudan#.UZ-nALXvtg0.
[93] Based on author's research.
[94] Bukhari Osman, "Accounts Targeted by Cyber Jihad Unit" [in Arabic], August 23, 2012, *Sudanese Online*, http://www.sudaneseonline.com/cgi-bin/sdb/2bb.cgi?seq=print&board=400&msg=1345716699&rn=1.
[95] Interviews, Khartoum, Sudan, June-September 2012.
[96] Interview with a released detainee, August 2012, Khartoum, Sudan.
[97] Abdelgadir Mohammed Abdelgadir, "Fences of Silence: Systematic Repression of Freedom of the Press, Opinion and Expression in Sudan," International Press Institute, 2012, http://www.freemedia.at/fileadmin/media/Fences_of_Silence-AbdelgadirMAbdelgadir-3.pdf: 53.
[98] Interview in Khartoum, Sudan, November 2, 2012.

and shown printed copies of her articles.[99] Hundusa's family found her on November 2, 2012 in the suburbs of Khartoum North in terrible physical condition with a shaved head and burned and bruised body.[100]

Another strategy employed by the Sudanese government to repress internet freedom is through technical attacks against opposition websites. For example, the websites *Al-Rakoba*, *SudaneseOnline*, *Sudanile*, and *Hurriyat* have all been frequently hacked between 2010 and 2012, likely by the Cyber-Jihad Unit.[101] Websites such as *Sudanese Online* have struggled to retrieve archives after the numerous technical attacks throughout the years. The e-mail and social media accounts of activists have also been subject to widespread hacking.[102]

[99] Interview in Khartoum, Sudan, November 2, 2012.
[100] "NISS Tortures Journalist Somia Hundosa," Girifna, November 3, 2012, http://www.girifna.com/7006.
[101] E-mail interview with editors from *Hurriyat* and *Al-Rakoba*, January 2013.
[102] Interview with a press freedom advocate and journalist, Khartoum, Sudan, January 16, 2012.

SYRIA

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	23	24
Limits on Content (0-35)	25	25
Violations of User Rights (0-40)	35	36
Total (0-100)	**83**	**85**

* 0=most free, 100=least free

POPULATION: 22.5 million
INTERNET PENETRATION 2012: 24 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Telecommunications infrastructure has deteriorated as a result of the armed conflict and authorities periodically shut down internet service to thwart citizen journalism and communications among rebel fighters (see **OBSTACLES TO ACCESS**).
- Several users remained in prison for expressing anti-regime views or documenting human rights violations online (see **VIOLATIONS OF USER RIGHTS**).
- Extralegal attacks have escalated, as several online activists and citizen journalists were attacked or killed by military units (see **VIOLATIONS OF USER RIGHTS**).
- Several users were targeted with surveillance malware, and hacktivism against human rights organizations, particularly by the Syrian Electronic Army, was prominent (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

The regime of President Bashar al-Assad has maintained tight control over information and communication technologies (ICTs) in Syria for many years, dominating key networks via government-linked service providers and engaging in extensive blocking of websites. The internet was first introduced to Syria in 2000, reaching only 30,000 users that year. By the end of 2010, more than one-fifth of the population was online. It is in the context of such growing access that the internet and social media have played an important role in a civic protest movement, which began in February 2011, calling for the end of President Bashar al-Assad's undemocratic rule and which, by early 2012, had turned into a fully-fledged armed conflict.

Amidst deadly repression and barred entry to foreign correspondents, citizen journalists using mobile phone devices and video-sharing websites have been a critical channel for informing Syrians and the international community about events in the country. In response, government censorship and retaliation against internet users dramatically intensified. Among the tactics employed have been periodic shutdowns of the internet and mobile phone networks, intensified filtering of websites, and various sophisticated means of monitoring and tracking internet users' online activities. In addition, Syria has emerged as one of the most dangerous countries in the world for citizen journalists and bloggers, with an untold number arrested and several killed.

The role of citizen journalists has lessened, however, as the popular uprising has deteriorated into an armed conflict. The infrastructure in at least seven major cities and provinces has been badly damaged, with many lacking internet access and power. Traditional journalists and human rights groups have slowly returned to northern areas of the country, which are now controlled by rebel groups, although disparate attacks against by radical fighters have been documented. Still, areas controlled by the opposition do enjoy a greater degree of freedom than those controlled by the Syrian government, even if a lack of working infrastructure has limited many individuals to using more expensive options, such as satellite internet. As the country's internet capacity has dwindled over the past year, the situation has become even more difficult for activists and bloggers.

OBSTACLES TO ACCESS

Syria's telecommunications infrastructure is one of the least developed in the Middle East, with broadband connections among the most difficult and expensive to acquire.[1] This dynamic only worsened after 2011, as inflation and electricity outages increased dramatically following public protests and the government's corresponding crackdown. Damage to the country's communications infrastructure has been particularly bad in the cities of Homs, Daraa, and Aleppo, as they were subject to severe shelling by the Syrian armed forces. By the end of 2012, the International Telecommunications Union (ITU) estimated that 24 percent of the population had

[1] "Syria - Telecoms, Mobile, Broadband and Forecasts," BuddeComm, accessed March 8, 2012, http://www.budde.com.au/Research/Syria-Telecoms-Mobile-Broadband.html.

access to the internet.[2] However, the number of broadband subscribers tripled from last year, reaching 378,000.[3] Mobile phone penetration was notably higher, at about 61 percent of the population at the end of 2012.[4]

In 2009, mobile phone companies began providing 3G services in Syria, though the number of subscribers had reached only 80,000 by late 2010 due to the relatively high prices of almost $25 for 4 MB and $200 for unlimited data usage.[5] In addition, the service is primarily only offered in large cities. Most users connect to the internet through a fixed dial-up connection at speeds of only 256 Kbps, which severely limits their ability to download or view multimedia content. During peak times, the speed is even slower.[6] Broadband ADSL service remains limited due to the inadequate infrastructure in rural areas and relatively high prices, which remain beyond the reach of most Syrians. For example, according to a price list published by the Syrian Computer Society, the monthly cost for a connection speed of 1 Mbps was SYP 1650 (approximately $30) as of May 2012,[7] in a country where gross domestic product per capita, when taken on a monthly basis, is only $274.[8]

The country's connection to the international internet remains centralized and tightly controlled by the government. This is done under the purview of the Syrian Information Organization (SIO) and the state-owned Syrian Telecommunications Establishment (STE), which owns all fixed-line infrastructures. The STE is a government body established in 1975 as part of the Ministry of Telecommunications and Technology.[9] This centralization has also contributed to connectivity problems, as the weak and overburdened infrastructure often results in slow speeds and periodic outages. In addition to its regulatory role, the STE also serves as an ISP.[10] Private ISPs like Aya, as well as mobile phone internet providers, are required to sign a memorandum of understanding to connect via the gateways controlled by the SIO.[11]

At least 11 internet service providers (ISPs) have entered the market since the end of 2005, raising the total number of ISPs to 14.[12] Independent satellite connections are prohibited.[13] ISPs and

[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2012, accessed August 1, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[3] Ibid.
[4] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2012, accessed August 1, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[5] "Projects to transform Syria into a regional anchor point in the communication" [in Arabic], Alhayat, September 1, 2010, http://international.daralhayat.com/internationalarticle/177606; "What are SURF Postpaid Packages?" [in Arabic], SURF Wireless Broadband, accessed March 8, 2012, http://bit.ly/15EHXWb.
[6] "Internet Enemies," Reporters Without Borders, March 2011, http://bit.ly/eLXGvi.
[7] "Services and price" [in Arabic], Syrian Computer Society Network (SCS-NET), accessed March 31, 2013 http://www.scs-net.org/portal/OurConnection/OurConnections/SCSADSL/PlansPrices/tabid/493/Default.aspx.
[8] "GDP per capita (current US$)," The World Bank, 2008-12, accessed August 1, 2013, http://data.worldbank.org/indicator/NY.GDP.PCAP.CD.
[9] See the Ministry of Telecommunications and Technology's website (in Arabic) at: http://www.moct.gov.sy/moct/?q=ar/node/58.
[10] See STE's website at: http://www.in-ste.gov.sy/inindex_en.html.
[11] Jaber Baker, "Internet in Syria: experimental goods and a field of a new control," White and Black Magazine, posted on Marmarita website, August 10, 2008, http://www.dai3tna.com/nuke/modules.php?name=News&file=article&sid=6019.
[12] "STE is shifting into company in June" [in Arabic], Alwatan, June 12, 2012, http://www.alwatan.sy/dindex.php?idn=124296.

cybercafés must obtain approval from the STE and pass security vetting by the Ministry of Interior and other security services.[14] Moreover, cybercafé owners are required to monitor visitors and record their activities. There are two main mobile phone providers in Syria: Syriatel—owned by Rami Makhlouf, a cousin of President Bashar al-Assad—and MTN Syria, a subsidiary of the South African company.

During 2012 and early 2013, the Syrian government has continued to obstruct connectivity through its control of key infrastructure, at times shutting down the internet and mobile phone networks entirely or at particularly sites of unrest. A nationwide shutdown was imposed on November 29, 2012, lasting two and a half days.[15] Another nationwide shutdown was imposed in December 11, 2012.[16] More localized, but longer lasting cut-offs were reported in seven provinces all across the country. This includes, for example, a full shutdown in Aleppo on August 11, 2012.[17] According to activists, broadband is often throttled and 3G services shut off as pro-regime forces prepare to besiege a city.[18] In other instances—such as in Daraa in March 2012—the entire electrical grid has been shut down for hours at a time. The government's deliberate use of such measures was evident from a leaked document issued by the General Head of the National Security Office in May 2011 explicitly ordering that "the internet is to be completely disconnected in Daraa, Homs, and the eastern provinces starting on Wednesday at 14:00."[19]

LIMITS ON CONTENT

The Syrian government engages in extensive filtering of websites related to politics, minorities, human rights, and foreign affairs. In recent years, censorship has expanded; the blocking of websites related to government opposition, human rights groups, the Muslim Brotherhood, and activism on behalf of the Kurdish minority is very common.[20] The Syrian government is suspected of possessing sophisticated technologies for filtering and surveillance, and self-censorship is highly prevalent, particularly in areas under government control. Despite these limitations, citizen journalists continue to make use of video-uploading sites and social networks to spread information about human rights abuses and atrocities of war. Their role has become particularly important at a time when traditional journalists operate in highly unsafe conditions and foreign press visas are difficult to obtain.

---

[13] "Online Syria, Offline Syrians," The Initiative For an Open Arab Internet, accessed March 8, 2012; "One Social Network With A Rebellious Message," The Initiative For an Open Arab Internet, accessed March 8, 2012, http://old.openarab.net/en/node/1625.

[14] Ayham Saleh, "Internet, Media and Future in Syria" [in Arabic], The Syrian Center for Media and Free Expression, November 14, 2006, http://bit.ly/1hfdwWl.

[15] Darren Anstee, "Syria goes dark," DDoS and Security Reports: The Arbor Networks Security Blog, November 29th, 2012, http://ddos.arbornetworks.com/2012/11/syria-goes-dark/

[16] Darren Anstee, "Snapshot: Syria's Internet drops, returns," DDoS and Security Reports: The Arbor Networks Security Blog, December 12th, 2012, http://ddos.arbornetworks.com/2012/12/snapshot-syrias-internet-drops-returns/

[17] "News From the Ground," [in Arabic], Telecomix: Syria, August 13, 2012, http://syria.telecomix.org/

[18] Interviews with several activists in Syria wishing to remain anonymous, August 2011to March 2012.

[19] "Leaked Syrian document shows how Assad banned internet access and satellite phones," The Telegraph, June 27, 2011. http://bit.ly/mLaugR.

[20] Internet Enemies, Reporters Without Borders, March 2011, http://www.reporter-ohne-grenzen.de/fileadmin/rte/docs/2011/110311_Internetbericht_engl.pdf, visited on May 1, 2013. .

A range of websites related to regional politics are also inaccessible, including the prominent London-based news outlets *Al-Quds al-Arabi* and *Asharq al-Awsat*, as well as several Lebanese online newspapers and other websites campaigning to end Syrian influence in Lebanon. Access to the entire Israeli top-level domain ".il" was also restricted. However, the websites of most international news sources and human rights groups have remained accessible.

Censorship is implemented by the STE with the use of various commercially available software programs. Independent reports in recent years pointed to the use of ThunderCache software, which is capable of "monitoring and controlling a user's dynamic web-based activities as well as conducting deep packet inspection."[21] In 2011, evidence emerged that the Syrian authorities were also using censorship and surveillance software manufactured by the U.S. firm Blue Coat Systems. Blue Coat had reportedly sold 14 devices to an intermediary in Dubai, believing the equipment would be given to the Iraqi government, but logs obtained by the hacktivist group Telecomix in August 2011 revealed evidence of their use in Syria instead.[22] In October of that year, Blue Coat acknowledged that 13 of the above 14 devices had been redirected to the Syrian government, an inadvertent violation of a U.S. trade embargo, and that the company was cooperating with the relevant investigations.[23] Analysis of the exposed Blue Coat logs revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites.[24] The *Wall Street Journal* identified efforts to block or monitor tens of thousands of opposition websites or online forums covering the uprising. Out of a sample of 2,500 attempts to visit Facebook, the logs revealed that three-fifths were blocked and two-fifths were permitted but recorded.[25]

The Syrian government also engages in filtering of mobile phone text messages. Beginning in February 2011, such censorship was periodically reported around dates of planned protests. In February 2012, the news service *Bloomberg* reported that a series of interviews and leaked documents revealed that a special government unit known as Branch 225 had ordered Syriatel and MTN Syria to block text messages containing key words like "revolution" or "demonstration." The providers reportedly implemented the directives with the help of technology purchased from two separate Irish firms several years earlier for the alleged purpose of restricting spam.[26]

The government continues to block circumvention tools, internet security software, and applications that enable anonymous communications. Websites used to mobilize people for protests

[21] Syria," OpenNet Initiative; Reporters Without Borders, "Syria," *Internet Enemies 2010* (Paris: Reporters Without Borders, March 18, 2010), http://www.unhcr.org/refworld/publisher,RSF,,SYR,4c21f66e28,0.html; "ThunderCache Overview," Platinum, Inc., accessed August 14, 2012, http://www.platinum.sy/index.php?m=91.

[22] Andy Greenberg, "Meet Telecomix, The Hackers Bent on Exposing Those Who Censor and Surveil The Internet," Forbes, December 26, 2011, http://www.forbes.com/sites/andygreenberg/2011/12/26/meet-telecomix-the-hackers-bent-on-exposing-those-who-censor-and-surveil-the-internet/.

[23] Blue Coat, "Update on Blue Coat Devices in Syria," news statement, December 15, 2011, http://www.bluecoat.com/company/news/statement-syria.

[24] "Blue Coat device logs indicated the levels of censorship in Syria," Hellias.github.com, accessed August 14, 2012, http://hellais.github.com/syria-censorship/.

[25] Jennifer Valentino-Devries, Paul Sonne, and Nour Malas, "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web," Wall Street Journal, October 29, 2011, http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html.

[26] Ben Elgin and Vernon Silver, "Syria Disrupts Text Messaging of Protesters With Made-in-Dublin Equipment," Bloomberg, February 14, 2012, http://www.bloomberg.com/news/2012-02-15/syria-blocks-texts-with-dublin-made-gear.html.

or resistance against the regime, including pages linked to the network of Local Coordination Committees (LCCs) that have emerged, continued to be blocked as of May 2013.[27] An online initiative to gather information and raise public awareness, the Mondaseh website, also remains blocked. [28]

Facebook remained accessible in Syria after the government lifted a four-year block on the social-networking site in February 2011. The video-sharing website YouTube was also unblocked, although it was not usable from mobile phone devices due to limits on data speeds.[29] As of March 2012, both were within the top-five most visited websites in the country (more recent data is not available).[30] Some activists suspected, however, that rather than a sign of openness, the regime's motive for unblocking the sites was to track citizens' online activities and identities. Other social media platforms like Twitter are freely available, although the presence of Syrian users on them is minimal.

Despite the free access to Facebook and YouTube, a range of other Web 2.0 applications remain inaccessible in Syria, including the blog-hosting platform Blogger and the VoIP service Skype. In February 2012, the government also began restricting access to certain applications for mobile phone devices that activists had been using to circumvent other blocks. Additionally, other applications reportedly blocked were the live video-streaming service Bambuser[31] and WhatsApp, an application that allows users to send mobile phone text messages via the internet.[32] Instant messenger services such as eBuddy, Nimbuzz, and mig33 have been blocked as well. In other cases, certain online services—such as Google Maps or the photo-sharing tool Picasa—have been rendered inaccessible from Syria by their U.S.-based service providers due to restrictions related to economic sanctions against the country.[33]

Decisions surrounding online censorship lack transparency and ISPs do not publicize the details of how blocking is implemented or which websites are banned, though government officials have publicly admitted engaging in internet censorship. When a user seeks to access a blocked website, an error message appears implying a technical problem rather than deliberate government restriction. Decisions on which websites or keywords should be censored are made by parts of the security apparatus, including the abovementioned Branch 225, or by the executive branch.

In an environment of extreme violence and arbitrary "red lines," self-censorship is widespread. Sensitive topics include criticizing President Assad, his late father, the military, or the ruling Baath

[27] LCCs website: http://www.lccsyria.org/en/
[28] The Syrian, the English page is available at: http://english.the-syrian.com/
[29] Interview with activist in Syria wishing to remain anonymous, December 2011.
[30] "Top Sites in SY," Alexa.com, accessed August 14, 2012, http://www.alexa.com/topsites/countries/SY.
[31] "Bambuser now blocked in Syria," Bambuser (blog), February 17, 2012, http://bit.ly/xu2HpI.
[32] Stuart Thomas, "Syrian government blocks access to WhatsApp," Memeburn.com, March 3, 2012, http://memeburn.com/2012/03/syrian-government-blocks-access-to-whatsapp/.
[33] On May 23, 2012, Google announced that it made Google Earth, Picasa and Chrome available for download in Syria. Yet, Google said that "As a U.S. company, we remain committed to full compliance with U.S. export controls and sanctions." Activists and internet users in Syria describe Google's step as insufficient, saying that there are tens of Google services still blocked in Syria including the entire Google Play App store on Android phones. See, "Software downloads in Syria," Official Google Blog, May 23, 2012, http://googleblog.blogspot.com/2012/05/software-downloads-in-syria.html?m=1.

party. Publicizing problems faced by religious and ethnic minorities or corruption allegations related to the ruling family, such as those of Assad's cousin Rami Makhlouf, are also off limits. Most Syrian users are careful not only to avoid such sensitive topics when writing online, but also to avoid visiting blocked websites.[34] However, the period of May 2012 to April 2013 witnessed a large number of local Syrian users expressing opposition to Assad, his father, Makhlouf, the Baath party, and certain ethnic or sectarian groups.[35]

Pro-regime forces have employed a range of tactics to manipulate online content and discredit news reports or those posting them, though it is often difficult to directly link those who are carrying out these activities with the government. Most notable has been the emergence of the Syrian Electronic Army (SEA) since April 2011, a pro-government hacktivist group that targets the websites of opposition forces and human rights websites, often shutting them down (see "Violations of User Rights"). For news websites and other online forums based in the country, it is common for writers to receive phone calls from government officials offering "directions" for how to cover particular events.[36] The Syrian government also pursues a policy of supporting and promoting websites that publish pro-government materials in an attempt to popularize the state's version of events. These sites typically cite the reporting of the official state news agency SANA, with the same exact wording often evident across multiple websites. Since early 2011, this approach has also been used to promote the government's perspective about the uprising and subsequent military campaign.[37]

Social media has played a crucial role in the Syrian uprising, though its primary utility has been information sharing rather than planning street protests. The "Syrian Revolution 2011" Facebook page, which by March 2013 had over 750,000 members from both inside and outside the country, has been a vital source of information for dissidents.[38] As the Syrian government shifted to the use of heavy arms and missiles against opposition fighters, the role of citizen journalists has shifted from live event coverage to documenting the bloody aftermath of an attack. Several YouTube channels belong to armed rebels, particularly Islamist groups. Both Facebook and YouTube have removed content related to the Syrian uprising, mainly due to content that promotes violence or contains graphic content, such as videos of torture or killing. Hundreds of thousands of videos have been posted to YouTube by citizen journalists, mostly documenting attacks. A Syrian group working on categorizing YouTube videos and sharing them via a platform called "OnSyria" had posted almost 200,000 videos as of April 2013.[39]

VIOLATIONS OF USER RIGHTS

Syria's constitution provides for freedom of opinion and expression, but these are severely restricted in practice, both online and offline. Furthermore, a handful of laws are used to prosecute

[34] Email communication from a Syrian blogger. Name was hidden.
[35] Interview, via Skype, with a Syrian activist. Damascus. November 2012. Name is hidden.
[36] Guy Taylor, "After the Damascus Spring: Syrians search for freedom online."
[37] Guy Taylor, "After the Damascus Spring: Syrians search for freedom online."
[38] "The Syrian Revolution 2011 Facebook Statistics," Socialbakers.com, accessed March 31, 2013, http://www.socialbakers.com/facebook-pages/420796315726-the-syrian-revolution-2011.
[39] See http://onsyria.org/

online users who express their opposition to the government. Citizen journalists and YouTube users are detained and often tortured by both government forces and, at times, rebel fighters. Surveillance tools are used to identify and harass those who oppose the Assad government, often through targeted malware attacks against their computer systems and online accounts. Finally, the websites of opposition groups and human rights organizations are consistently targeted with cyberattacks from hackers linked to the government.

Laws such as the penal code, the 1963 State of Emergency Law, and the 2001 Press Law are used to control traditional media and arrest journalists or internet users based on vaguely worded terms such as threatening "national unity" or "publishing false news that may weaken national sentiment."[40] Defamation offenses are punishable by up to one year in prison if comments target the president and up to six months in prison for libel against other government officials, including judges, the military, or civil servants.[41] The judiciary lacks independence and its decisions are often arbitrary. Furthermore, some civilians have been tried before military courts.

Since anti-government protests broke out in February 2011, the authorities have detained hundreds of internet users, including several well-known bloggers and citizen journalists. However, many of those targeted are not known for their political activism, making the reasons behind their arrest often unclear. This arbitrariness has raised fears that users could be arrested at any time for even the simplest online activities—posting on a blog, tweeting, commenting on Facebook, sharing a photo, or uploading a video—if it is perceived to threaten the regime's control. Veteran blogger Ahmad Abu al-Khair was taken into custody in February 2011 while traveling from Damascus to Banias and was later to released, though he has remained in hiding.[42] More recently, in an effort to pressure al-Khair to turn himself in, security forces have twice detained his brother, once for a period of 60 days.[43] Bassel Khartabil, an open source activist and recipient of the 2013 Index on Censorship Digital Freedom Award, remains in prison after he was taken by authorities without explanation in March 2012.[44]

Human rights activists who work online are also targeted by the government. Authorities raided the offices of the Syrian Center for Media and Freedom of Expression (SCM) in February 2012, arresting 14 employees.[45] SCM member and civil rights blogger Razan Ghazzawi[46] was released after 22 days in detention and fled to Sweden.[47] Five members remain in prison and face up to 15 years for "publicizing terrorist acts" over their role in documenting human rights violations by the

[40] Articles 285, 286, 287 of the Syrian Penal Code.
[41] Article 378 of the Syrian Penal Code.
[42] Anas Qtiesh, "Syrian Blogger Ahmad Abu al-Khair Arrested This Morning," Global Voices Online, February 20, 2011, http://advocacy.globalvoicesonline.org/2011/02/20/syrian-blogger-ahmad-abu-al-khair-arrested-this-morning/.
[43] Email communication with activist in Syria who wished to remain anonymous, April 2012.
[44] William Echikson, "Supporting freedom of expression in all forms," Google – Europe Blog, March 23, 2013, http://googlepolicyeurope.blogspot.co.uk/2013/03/supporting-freedom-of-expression-in-all.html.
[45] Maha Assabalani, "My colleagues are in prison for fighting for free expression," UNCUT - Index on Censorship, May 11, 2012, http://uncut.indexoncensorship.org/2012/05/my-colleagues-are-in-prison-for-fighting-for-free-expression/.
[46] Jared Malsin, "Portrait of an Activist: Razan Ghazzawi, the Syrian Blogger Turned Exile," Time, April 2, 2013, http://world.time.com/2013/04/02/portrait-of-an-activist-meet-razan-ghazzawi-the-syrian-blogger-turned-exile/.
[47] An interview with Syrian blogger via Skype. February 2013, name is hidden.

Syrian regime.[48] The organization's founder and director, Mazen Darwich, remained in incommunicado detention as of March 2013.[49]

Once in custody, citizen journalists, bloggers, and other detainees reportedly suffered severe torture on behalf of government authorities. Although the precise number is unknown, it is estimated that dozens of individuals have been tortured to death for filming protests or abuses and then uploading them to YouTube.[50] In some cases, the Syrian army appeared to deliberately target online activists and photographers all across the country. In one high-profile case from February 2012, Anas al-Tarsha, a videographer who documented unrest in the besieged city of Homs, was killed by a mortar round while filming the bombardment of the city's Qarabees District.[51] At least five of the citizen journalists who worked for the Damascus-based Shaam News Network, whose videos have been used extensively by international news organizations, were killed during 2012 and early 2013. Among them were Ghaith Abd al-Jawad and Amr Badir al-Deen Junaid, both from Qaboun Media Center, a group of opposition citizen journalists who film clashes in the neighborhood of Qaboun and publish the unattributed videos online.[52] In response to such brutality, hundreds of activists have gone into hiding and dozens have fled the country, fearing that arrest may not only mean prison, but also death under torture.[53]

Attacks on activists and citizen journalists were not limited to Syrian government forces. The Free Syrian Army (FSA), the opposition armed movement, have committed many attacks on videographers and citizen journalists, mainly in the suburbs of Aleppo. Since the "liberation" of Aleppo province, activists and photographers were targeted by FSA fighters more than they were targeted by the Syrian government.[54] Further, "Al Nusra Front" (*Jabhat al Nusra*), a group of armed extremists, have arrested tens of young citizen journalists for weeks, and in one incident, opened fire on them for filming a protest in Bostan al Qaser in Aleppo.[55]

Competition among activists has also led to violations against each other. In one case, a citizen journalist used armed thugs to kidnap the administrator of a competing Facebook page for media groups, aiming to shut it down. The victim sought help from another armed group, who, in turn, abducted the first individual. Both of the kidnapped group administrators were beaten to provide passwords of their Facebook accounts. Eventually, both men were released.[56]

Anonymous communication is possible online but increasingly restricted. Registration is required upon purchasing a cell phone, though over the past year, activists have begun using the SIM cards of

[48] "Syrian free speech advocates face terrorism charges," Index on Censorship, May 17, 2013, http://www.indexoncensorship.org/2013/05/syria-there-are-not-enough-prisons-for-the-free-word/.
[49] Skype interview with Syrian activist, March 2013. The name is hidden.
[50] Interview via Skype with A.A, Human Rights Lawyer in Damascus, December 12, 2011. Name is hidden.
[51] Committee to Protect Journalists, Anas al-Tarsha, February 24, 2012. http://www.cpj.org/killed/2012/anas-al-tarsha.php , visited on December 2012.
[52] Committee to Protect Journalists, Ghaith Abd al-Jawad, March 10, 2013, available at http://www.cpj.org/killed/2013/ghaith-abd-al-jawad.php, visited March 31, 2013.
[53] Interviews with two photographers who have taken refuge in Turkey, December 2011.
[54] Interview with activist from Aleppo, via Skype, January 2013. Name is hidden.
[55] Interview with lawyer from Aleppo. Istanbul, Turkey. January 2013. Name is hidden.
[56] The author helped mediate this case, which occurred in the Damascus suburban area in February 2013. Names are hidden.

friends and colleagues killed in clashes with security forces in order to shield their identities. Cell phones of neighboring countries like Turkey and Lebanon have been widely used during 2012 and 2013, notably by Free Syrian Army fighters. Meanwhile, activists and bloggers released from custody reported being pressured by security agents to provide the passwords of their Facebook, Gmail, Skype, and other online accounts.[57]

The "Law for the Regulation of Network Communication against Cyber Crime," passed in February 2012, requires websites to clearly publish the names and details of the owners and administrators.[58] The owner of a website or online platform is also required "to save a copy of their content and traffic data to allow verification of the identity of persons who contribute content on the network" for a period of time to be determined by the government.[59] Failure to comply may cause the website to be blocked and is punishable by a fine of between SYP 100,000 and 500,000 ($1,700 to $8,600). If the violation is found to have been deliberate, the website owner or administrator may face punishment of three months to two years imprisonment as well as a fine of SYP 200,000 to 1 million ($3,400 to $17,000).[60] As of April 2013, however, the authorities were not vigorously enforcing these regulations.

Surveillance is widespread in Syria, as the government capitalizes on the centralized internet connection to intercept user communications. In early November 2011, *Bloomberg* reported that in 2009 the Syrian government had contracted Area SpA, an Italian surveillance company, to equip them with an upgraded system that would enable interception, scanning, and cataloging of all e-mail, internet, and mobile phone communication flowing in and out of the country. According to the report, throughout 2011, employees of Area SpA had visited Syria and began setting up the system to monitor user communications in near real-time, alongside graphics mapping users' contacts.[61] The exposé sparked protests in Italy and, a few weeks after the revelations, Area SpA announced that it would not be completing the project.[62] No update is available on the project's status or whether any of the equipment is now operational.

In a potential indication that the Syrian authorities were seeking an alternative to the incomplete Italian-made surveillance system, in March 2012 reports emerged of sophisticated phishing and malware attacks targeting online activists. The U.S.-based Electronic Frontier Foundation (EFF) reported that malware called "Darkcomet RAT" and "Xtreme RAT" had been found on activists' computers and were capable of capturing webcam activity, logging keystrokes, stealing passwords,

[57] Interviews with released bloggers, names were hidden.
[58] "Law of the rulers to communicate on the network and the fight against cyber crime" [in Arabic], Articles 5-12, accessed March 8, 2012, http://www.sana.sy/ara/2/2012/02/10/pr-399498.htm (site discontinued). Informal English translation: https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-law-on-Internet-regulation.html.
[59] "Law of communicating on the network and fighting against cyber crime" [in Arabic], Article 2, accessed March 8, 2012, http://www.sana.sy/ara/2/2012/02/10/pr-399498.htm.
[60] "Law of communicating on the network and fighting against cyber crime" [in Arabic], Article 8, accessed March 8, 2012, http://www.sana.sy/ara/2/2012/02/10/pr-399498.htm. English translation: https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-law-on-Internet-regulation.html.
[61] Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear," Bloomberg, November 3, 2011, http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html.
[62] Vernon Silver, "Italian Firm Said To Exit Syrian Monitoring Project," Bloomberg, November 28, 2011, http://www.bloomberg.com/news/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says.html.

and more. Both applications sent the data back to the same IP address in Syria and were circulated via e-mail and instant messaging programs.[63] Later, EFF reported the appearance of a fake YouTube channel carrying Syrian opposition videos that requested users' login information and urged them to download an update to Adobe Flash, which was in fact a malware program that enabled the stealing of data from their computer. Upon its discovery, the fake site was taken down.[64]

Cyberattacks have become increasingly common in Syria since February 2011, responding to the growing circulation of anti-Assad videos and other content online. Most notable has been the Syrian Electronic Army (SEA), a hacktivist group that emerged in April 2011. Though the group's precise relationship to the regime is unclear, evidence exists of government links or at least tacit support. These include the SEA registering its domain[65] in May 2011 on servers maintained by the Assad-linked Syrian Computer Society,[66] a June 2011 speech in which the president explicitly praised the SEA and its members,[67] and positive coverage of the group's actions in state-run media.[68]

The SEA's key activities include hacking and defacing Syrian opposition websites and Facebook accounts, as well as targeting Western or other news websites perceived as hostile to the regime. However, some foreign websites from the academic, tourism, or online marketing sectors have also been targeted.[69] On March 17, 2013, the SEA hacked the website and Twitter feed of Human Rights Watch, redirecting to the SEA homepage.[70] The Mondaseh website was also hacked by the SEA in early January 2012.[71] The SEA is known to post private information, such as the phone numbers and addresses of anti-government activists, onto its Facebook pages.[72] Most of these pages have subsequently been closed by Facebook for violating its terms of use. However, pro-government media outlets continued to publish hacked e-mails from opposition figures.

---

[63] Eva Galperin and Morgan Marquis-Boire, "How to Find and Protect Yourself Against the Pro-Syrian-Government Malware on Your Computer," Electronic Frontier Foundation, March 5, 2012, http://bit.ly/xsbmXy.
[64] Eva Galperin and Morgan Marquis-Boire, "Fake YouTube Site Targets Syrian Activists With Malware," Electronic Frontier Foundation, March 15, 2012, https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware.
[65] The Syrian Electronic Army, http://syrian-es.com/.
[66] Haroon Siddique and Paul Owen, "Syria: Army retakes Damascus suburbs," Middle East Live (blog), *The Guardian*, January 30, 2012, http://www.guardian.co.uk/world/middle-east-live/2012/jan/30/syria-army-retakes-damascus-suburbs.
[67] "Speech of H.E. President Bashar al-Assad at Damascus University on the situation in Syria," official Syrian news agency (SANA), June 21, 2011, http://www.sana.sy/eng/337/2011/06/21/353686.htm.
[68] See positive coverage on state-run websites [in Arabic]: Thawra.alwedha.gov.sy, May 15, 2011, http://thawra.alwehda.gov.sy/_print_veiw.asp?FileName=18217088020110516122043; Wehda.alwedha.gov.sy, May 17, 2011, http://wehda.alwehda.gov.sy/_archive.asp?FileName=18235523420110517121437.
[69] Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," OpenNet Initiative, accessed August 14, 2012, http://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army.
[70] Max Fisher, "Syria's pro-Assad hackers infiltrate Human Rights Watch Web site and Twitter feed", The Washington Post, March 17, 2013. http://wapo.st/1eU9nKI.
[71] See YouTube video by SEA celebrating the hacking: http://www.youtube.com/watch?v=48q34HlIBOk.
[72] Zeina Karam, "Syrian Electronic Army: Cyber Warfare From Pro-Assad Hackers," Huffington Post, September 27, 2011, http://www.huffingtonpost.com/2011/09/27/syrian-electronic-army_n_983750.html.

THAILAND

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	PARTLY FREE
Obstacles to Access (0-25)	11	10
Limits on Content (0-35)	21	21
Violations of User Rights (0-40)	29	29
Total (0-100)	**61**	**60**

* 0=most free, 100=least free

POPULATION: 70 million
INTERNET PENETRATION 2012: 27 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Thai courts issued 161 orders to block 21,000 URLs in 2012, many for criticizing the monarchy (see **LIMITS ON CONTENT**).
- A court fined Chiranuch Premchaiporn and gave her a suspended jail term for failing to delete anti-royal user comments from her news website *Prachatai* (see **VIOLATIONS OF USER RIGHTS**).
- Sexagenarian Ampol Tangnopakul died in May 2012 while jailed for anti-royal texting after a court denied medical parole (see **VIOLATIONS OF USER RIGHTS**).
- A cabinet directive implemented in mid-2012 put Computer-related Crimes Act cases under the jurisdiction of the Department of Special Investigation, which can intercept electronic communications without a court order (see **VIOLATIONS OF USER RIGHTS**).
- Activists petitioned lawmakers to reform lèse-majesté laws via social media, sparking unprecedented public debate (see **LIMITS ON CONTENT**).
- Free government-sponsored Wi-Fi hotspots helped improve access nationwide (see **OBSTACLES TO ACCESS**).

INTRODUCTION

Thai citizens have been posting online commentary since the internet was commercialized in 1995,[1] but digital communication took on a particularly significant role after the 2006 military coup. Since then, both the red-shirt supporters of former Prime Minister Thaksin Shinawatra and their royalist, yellow-shirt opponents have utilized online resources to mobilize constituents, contributing to the democratic election of the Pheu Thai Party and Thaksin's sister, Yingluck Shinawatra, as prime minister in July 2011.

Thailand's worst limitations on content and violations of user rights occur under computer crimes laws enacted after the coup, and oppressive lèse-majesté provisions in the penal code, which criminalize criticism of the nation's revered monarchy. The state has blocked tens of thousands of individual websites and social media pages, and imprisoned several people for disseminating information and opinion online or via mobile phone under these laws. Anyone can lodge a lèse-majesté complaint against anyone else in Thailand, opening the door for various actors to use the charges against political opponents or to curb civic advocacy in a highly polarized political environment.

Those expecting that Shinawatra would loosen internet restrictions have been disappointed. Censorship has continued and even become more institutionalized since she took office. Vaguely-worded legislation and lax adherence to due process has led to disproportionately harsh punishments given to ordinary users based on questionable evidence. In May 2012, news website administrator Chiranuch Premchaiporn was fined and given a suspended jail term for failing to delete comments left by readers in a verdict even the judge called unfair. She was luckier than Ampol Tangnopakul, who died in prison the same month. A court imprisoned him for 20 years in 2011 for sending anti-royal text messages from his mobile phone—though the 61-year-old denied knowing how to use SMS.

While content restrictions and legal harassment— particularly in these two widely-reported cases—increase self-censorship in online discussions, they also serve to further politicize the monarchy in the eyes of many Thais, and sparked serious civic efforts to promote lèse-majesté reform in 2012 and 2013. They have also inspired a burgeoning movement of politically conscious internet users, who favor greater protections for internet freedom.

OBSTACLES TO ACCESS

Declining prices, increased demand for alternative sources of information, and social networking tools are enticing Thais to spend more time online, and internet penetration was at 27 percent in

[1] Phansasiri Kularb, "Communicating to the Mass on Cyberspace: Freedom of Expression and Content Regulation on the Internet," in *State and Media in Thailand During Political Transition*, ed. Chavarong Limpattanapanee and Arnaud Leveau (Bangkok: Institute de Recherche sur l'Asie du Sud-Est Contemporaine, 2007).

2012.[2] Mobile telephony is more widespread, with penetration topping 120 percent, indicating some citizens own more than one device.[3]

In households with internet access, 56 percent used fixed broadband connections while 15 percent relied on a modem in 2012, official figures show. Thailand suffers from an urban-rural connectivity divide: nearly 40 percent of internet users are based in major cities, twice the percentage of users based in rural areas.[4]

The government has been slow to improve the fixed-line infrastructure and boost the development of ICTs, even though lessening the digital divide was a notable part of the Pheu Thai party's platform ahead of the July 2011 elections. This was due in part to the extensive flooding that struck Thailand in October 2011, the worst in decades. Internet penetration rose by only 2 percent in 2011 and 3 percent in 2012.[5] This is expected to change in 2013 under the government's "Smart Network" policy, which aims to expand access to 95 percent of the population by 2020.[6] The National Broadcasting and Telecommunications Commission (NBTC) has approved a THB 950 million ($31,980,000) budget for a Ministry of Information and Communication Technology (MICT) project, "ICT Free Wi-Fi," to add 300,000 internet access points across Thailand in 2013 in cooperation with service providers.[7] Northern Chiang Mai province is undergoing a similar pilot scheme sponsored by telecommunications giant TRUE.[8] The government also plans to implement free hi-speed internet access in public places such as schools and hospitals. Internet users can get online for free at many public access points by registering for an account through a website run by government agencies in cooperation with telecommunications companies.[9]

Partly as a result of efforts like this, official 2012 figures state 44 percent of Thai internet users paid nothing for access, and another 25 percent paid less than THB 200 ($6.73) a month.[10] These figures counted individuals using free public access; in households paying for monthly service, most paid THB 600-799 ($19-26). Connections reportedly function at speeds around 12 Mbps,[11] most reliably in the greater Bangkok area. In past years, users complained that connections were slower

---

[2] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[3] International Telecommunication Union," Mobile-Cellular Telephone Subscriptions, 2000-2012." See also, National Broadcasting and Telecommunications Commission, "Thailand ICT Info," accessed January 13, 2013, http://www2.nbtc.go.th/TTID/mobile_market/subscribers/.

[4] National Statistical Office, " Information and Communication Technology Survey in Household, 2012," http://web.nso.go.th/en/survey/ict/ict_house12.htm.

[5] National Broadcasting and Telecommunications Commission, "Thailand ICT Info," accessed January 2013, http://www2.nbtc.go.th/TTID/mobile_market/subscribers/.

[6] Asina Pornwasin, "'Smart Thailand' Project on Track," *The Nation*, February 28, 2012, http://www.nationmultimedia.com/technology/SMART-THAILAND-PROJECT-ON-TRACK-30176841.html.

[7] "NBTC Issues Funds for Free Wi-Fi," *Bangkok Post*, January 17, 2013, http://www.bangkokpost.com/breakingnews/331263/nbtc-issues-funds-for-free-wifi.

[8] "ICT Free Wi-Fi by TRUE With Up to 15 Hours Usage per Month," Truemove, accessed January 2013, http://truemoveh.truecorp.co.th/activity/entry/632?ln=en http://truemoveh.truecorp.co.th/activity/entry/632?ln=en

[9] "Register for Free Wi-Fi by TOT and MICT," accessed April, 2013, http://vip.totwifi.com/ict-nakhonratchasima/regis.php.

[10] National Statistical Office, "Information and Communication Technology Survey." A second official survey of nearly 24,000 internet users found 35 percent of respondents using free service. See, "Thailand's Internet Users to Double," *Bangkok Post,* July 4, 2013, http://www.bangkokpost.com/breakingnews/358289/thailand-internet-users-to-double-to-52-million-in-2013.

[11] "Download Index," Net Index, accessed June 21, 2012, http://www.netindex.com/download/2,23/Thailand/.

than advertised. However, in late 2012 and early 2013, there was no official information about user complaints, and anecdotally, speeds appeared to have improved.

Mobile phone ownership is also more common in municipalities, with penetration higher in Bangkok and other cities than in rural areas.[12] The NBTC regulated maximum service rates for inland voice service via mobile phone in 2011. As of April 2012, service providers are not allowed to charge more than an average THB 0.99 ($0.03) per minute; existing contracts had to be adjusted to match these rates by January 1, 2013.[13] While SMS messaging is popular, the percentage of people accessing the internet via mobile phone is less than 10 percent.[14]

Smartphone use is expected to change this. By late 2011, sales of smartphones surpassed those of feature phones for the first time and an estimated four million people subscribed to internet-capable third-generation (3G) services. Declining costs—smartphones averaged THB 3,000 ($100) each in early 2012—are accelerating this trend.[15] While political and legal disputes have repeatedly delayed the licensing process for 3G mobile phone service and wireless broadband, the NBTC granted three corporations, Advanced Info Service, DTAC Network and Real Future, 15-year licenses to provide users with 2.1GHz and 3G service in December 2012,[16] which is expected to drive mobile phone penetration to 130 percent in 2016.[17] The licenses are conditional on providers reducing service costs by 15 percent, increasing geographical coverage to 80 percent in 4 years, maintaining connection speeds specified by the NBTC, and protecting the rights of consumers.[18]

The government has also tried to improve access to devices and hardware through projects like the MICT's "One Tablet per Child," which aims to distribute free tablets loaded with education software to all first-year primary school students.[19] Critics argue the program distracted public attention away from other factors affecting education, such as poor teacher performance.[20]

In recent years, the Thai telecommunications market has liberalized and diversified. Out of nine National Internet Exchanges that connect to the international internet, the government-run Communication Authority of Thailand (CAT) Telecom operates two, including the country's

[12] National Statistical Office, "Information and Communication Technology Survey."
[13] "How Will the Adjustment in Mobile Phone Service Fee in Thailand Affect the Service Provider?," Phoenix Capital Group, January 29, 2013, http://www.thephoenixcapitalgroup.com/how-will-the-adjustment-in-mobile-phone-service-fee-in-thailand-affect-the-service-providers/.
[14] National Statistical Office, "Information and Communication Technology Survey."
[15] Suchit Leesa-nguansuk, "Smartphones to Rule the Roost," *Bangkok Post,* May 15, 2012, http://www.bangkokpost.com/business/telecom/293824/smartphones-to-rule-roost.
[16] Sirivish Toomgum, "NBTC clears legal hurdle, ready to issue 3G licences," *The Nation*, December 4, 2012, http://www.nationmultimedia.com/business/NBTC-clears-legal-hurdle-ready-to-issue-3G-licence-30195554.html.
[17] Business Monitor International, "Thailand Telecommunications Report Q4 2012", http://www.marketresearch.com/Business-Monitor-International-v304/Thailand-Telecommunications-Q4-7147954/; and "Thailand Telecommunications Report Q3 2012," June 12, 2012, http://www.marketresearch.com/Business-Monitor-International-v304/Thailand-Telecommunications-Q3-7027556/.
[18] Komsan Tortermvasana, "3G Rules Simplified, N-1 Rule Scrapped," *Bangkok Post*, April 11, 2012, http://www.bangkokpost.com/lite/topstories/288345/3g-rules-simplified-n-1-rule-scrapped
[19] International Telecommunication Union, "One Tablet per Child Policy: Stepping Up Education Reform in Thailand," January 18, 2013, http://bit.ly/1azRf3G.
[20] "Let Them Eat Tablets," *Economist*, July 16, 2012, http://www.economist.com/node/21556940.

largest.[21] As of mid-2012, there were over 100 ISPs with active licenses, though 10 provided most of the connection services for individual consumers and households.[22] Among them, True Internet—a subsidiary of the communications conglomerate True Corporation, which also controls Thailand's third-largest mobile phone operator True Move—had a 40 percent share of the high-speed internet market by March 2013;[23] the state-owned Telephone Organization of Thailand controlled 33 percent in late 2012,[24] while the private 3BB controlled 28 percent.[25] The three main mobile phone service providers are the Singaporean-owned Advanced Info Service, the Norwegian-controlled DTAC, and True Corporation's True Move. The first two operate under concessions from TOT and CAT, an allocation system that does not entirely enable free-market competition.

Legislation creating a single regulatory body for both the broadcast and telecommunications sectors passed parliament in late 2010. After a long and dispute-filled selection process, the senate appointed the members of the new NBTC in September 2011. From among the 11 commissioners, 5 are from the military, reflecting the army's deep interests in the communications sector. The remaining members are three former bureaucrats, two civil society representatives, and one police officer.[26] Some observers have complained that the NBTC lacks commissioners with industry experience that the regulatory structure is incapable of dealing with converging communications platforms, and that coordination across different parts of the commission is weak.[27] Despite these shortcomings, the NBTC's decisions and proposed plans regarding the telecommunications sector thus far are largely viewed as fair.[28]

LIMITS ON CONTENT

In 2012, Thai courts blocked almost 21,000 URLs, including thousands for anti-royal content. Just 5,000 URLs had been blocked the previous year. In a new development, however, activists effectively used digital tools to drive public debate on lèse-majesté. While petitions demanding reform have yet to see concrete results, the support and media coverage they attracted were unprecedented. Manipulation of online debate by paid commentators declined, a sign that the activity observed in 2011 was probably tied to the election campaigns.

Restrictions on content have expanded in recent years in both scale and scope, although the Thai government has been blocking some internet content since 2003, when it implemented controls on

[21] Internet Information Research Network Technology Lab [in Thai], National Electronics and Computer Technology, accessed July 2013, http://internet.nectec.or.th/webstats/internetmap.current.iir?Sec=internetmap_current.
22 NBTC, "List of Licensed Telecommunications Businesses" [in Thai], accessed July 2013, http://apps.nbtc.go.th/license/.
[23] "TRUE Invest Ten Thousand Million to Increase Market Share" [in Thai], *Jasmine,* March 30, 2013, http://www.jasmine.com/news_industry_detail_th.asp?ID=2805.
[24] Both CAT Telecom and TOT are supervised by the MICT.
[25] NBTC, "Telecommunication Market Report Q3 2012" [in Thai], http://bit.ly/19NLMEi.
[26] Usanee Mongkolporn, "Strong Military Role in NBTC," *The Nation*, September 6, 2011, http://www.nationmultimedia.com/home/Strong-military-role-in-NBTC-30164583.html.
[27] Don Sambandaraksa, "Thai Regulator Lacks Unity," *Telecomasia* (blog), October 7, 2011, http://www.telecomasia.net/blog/content/thai-regulator-lacks-unity.
[28] Komsan Tortermvasana, "NBTC Approves Spectrum, Broadcasting Master Plans," *Bangkok Post*, March 22, 2012, http://www.bangkokpost.com/business/telecom/285448/nbtc-approves-spectrum-broadcasting-master-plan.

pornography and gaming, among other topics.[29] The new administration has maintained vigilant monitoring of anti-royal content and extended censorship to popular social media platforms.[30]

Government bodies monitor online content and enforce censorship through court orders under the 2007 Computer-related Crime Act (CCA),[31] and extrajudicial blocking decisions by the executive branch. Online censorship is also conducted through preemptive action by ISPs and content hosts, whose cooperation is ensured because they can be held legally responsible for comments posted by third parties.[32] The 2012 conviction of the director and administrator of the *Prachatai* news website for failing to delete user comments in 2008 (see "Violations of User Rights") is expected to increase intermediary compliance with official censorship orders, though this is difficult to measure in practice. Court orders are almost always granted with minimal deliberation and little indication of which content was deemed to violate the law. As a result, website blocking lacks transparency, since the precise list of inaccessible sites is not available to the public. In addition, officials may inflate the figures for political purposes, according to one MICT source.[33]

Shinawatra's government has bolstered its monitoring capabilities in relation to lèse-majesté crimes. An MICT committee in charge of official website censorship established in 2010 is now chaired by one of her former deputy prime ministers, Chalerm Yoobamrung.[34] In 2011, local news reports criticized Chalerm for seeking a THB 400 million ($13.46 million) budget for the purchase of internet content filtering and monitoring equipment capable of censoring overseas websites without cooperation from foreign ICTs to help enforce lèse-majesté content restrictions.[35] The status of that budget is not known. The Technology Crime Suppression Division under the Royal Thai Police[36] and the MICT Cyber-Security Operation Center (CSOC) established under Shinawatra in December 2011 are also tasked with monitoring and curbing the circulation of lèse-majesté content.[37] Media reports describe the police body as several dozen computer technicians scouring thousands of websites, manually and with automated crawlers, for insults to the royal family.[38] The CSOC is an upgrade of a 2010 entity called the Internet Security Operation Center, but its precise mandate and activities remain unclear.[39]

---

[29] Karnjana Karnjanatawe, "Govt Forces ISPs to Block `Inappropriate' Web Sites," *Bangkok Post*, July 9, 2003, accessible at NARCHIVE Newsgroup Archive, http://bit.ly/19eoIgS.
[30] "MICT: More Cyber Offenders to be Arrested Soon," *Prachatai*, December 3, 2011, http://bit.ly/1fRKJt6.
[31] Journalists sometimes refer to it as the "Computer Crime Act."
[32] ISPs do not publicly acknowledge such cooperation, but it is widely accepted by freedom of expression advocates.
[33] Some counted duplications, so that a single article shared by ten internet users would be counted eleven times. Interview with mid-ranking MICT employee who requested anonymity, December 2011.
[34] Ministry of Information and Communication Technology, "ICT Policy Committee for Inappropriate Site Management" [in Thai], accessed February 2013, http://www.mict.go.th/ewt_news.php?nid=1683.
[35] "Chalerm Set to Crack Down on Websites", *Prachatai*, accessed February 12, 2013, http://bit.ly/1bRxEzF.
[36] Also called Office of Prevention and Suppression of Information Technology Crimes and referred to as a 'war room' for stopping lèse-majesté content. See, Thomas Fuller, "A High-Tech War Against Slights to a Centuries-Old Monarchy," *New York Times*, October 2, 2011, http://www.nytimes.com/2011/10/03/world/asia/03iht-thailand03.html?pagewanted=all.
[37] "MICT: More Cyber Offenders to be Arrested Soon," *Prachatai*, December 3, 2011, http://www.prachatai.com/english/node/2930.
[38] Martin Petty and Natnicha Chuwiruch, "Thais Test Taboos as War on Royal Slurs Heats Up," Reuters, December 6, 2011, http://www.reuters.com/article/2011/12/07/us-thailand-monarchy-idUSTRE7B605920111207.
[39] "Centre Starts Monitoring Lèse-Majesté," *Bangkok Post*, December 24, 2011, http://www.bangkokpost.com/lite/topstories/272260/centre-starts-monitoring-lese-majeste.

Blocking tactics have evolved over time. Most of the websites filtered prior to 2007 involved pornography, online gambling, or circumvention tools, although some politically oriented websites were also found to be inaccessible.[40] Blocking increased exponentially under the 2007 CCA, particularly in relation to anti-royal content.[41] One academic study shows that between 2007 and 2011, there were 156 court orders issued to block access to nearly 82,000 URLs,[42] an average of 980 URLs a day. All told, five years after the enforcement of the act, criminal courts have authorized a total 317 orders preventing access to 102,191 URLs.[43]

Thousands of these were blacklisted under the emergency declaration in effect from April to December 2010, when an extrajudicial mechanism granted top security officials unilateral powers to block websites.[44] While international news websites and human rights groups remained accessible, a number of domestic websites supporting the opposition red-shirt movement were blocked, as were less partisan online news outlets or human rights groups, such as Freedom Against Censorship Thailand, the online newspaper *Prachatai*, the Political Prisoners in Thailand blog, and *Asia Sentinel*.[45] Although this extrajudicial procedure was abolished with the end of the state of emergency, the censorship system in Thailand continues to lack transparency and accountability.[46]

Hopes that the Shinawatra would loosen restrictions were dashed when Chalerm Yoobamrung vowed to curb lèse-majesté content a month after taking office, demonstrating the deeply-entrenched political resistance to reforming the law, even under a new administration.[47]

While some sites blocked in 2010 are now accessible again,[48] others—including *Prachatai* and *Asia Sentinel*—remain at least partially blocked.[49] However, more are being added to the blacklist. The number of court orders authorizing website blocks rose in 2012, when courts granted 161 orders to block almost 21,000 URLs.[50] These included 5,000 URLs blocked between December and March for containing content critical of the royal family, according to police.[51] This represents a

[40] OpenNet Initiative, "Country Profile: Thailand," May 9, 2007, http://opennet.net/research/profiles/thailand.
[41] Freedom Against Censorship Thailand, "Thai Website Censorship Jumps by More Than 500 percent Since Coup!" news release, January 1, 2007, http://bit.ly/15BTWUd.
[42] Sawatree Suksri, Siriphon Kusonsinwut, and Orapin Yingyongpathana, *Impact of the Computer-related Crime Act 2007 and State Policies on the Right to Freedom of Expression* [in Thai and English] (Bangkok: Internet Dialogue on Law Reform (iLaw Project), 2012), 455. http://www.boell-southeastasia.org/downloads/computercrime_publication_thai.pdf.
[43] iLaw, "Statistics of Website Censorship in Thailand 2007 - 2012," http://bit.ly/13s5zHY.
[44] C.J. Hinke, "Thailand Now Blocking 277,610 Websites," *Global Voices Advocacy*, November 8, 2010, http://advocacy.globalvoicesonline.org/2010/11/08/thailand-now-blocking-256110-websites/
[45] Pavin Chachavalpongpun, "Thailand's Massive Internet Censorship," *Asia Sentinel*, July 22, 2010, http://asiasentinel.com/index.php?option=com_content&task=view&id=2601&Itemid=164.
[46] iLaw researchers collecting details of blocked websites found many government agencies unable or unwilling to provide data.
[47] "Chalerm Warns Lèse-Majesté Websites," *Bangkok Post*, August 26, 2011, http://www.bangkokpost.com/news/politics/253608/chalerm-to-curb-lese-majeste-websites. Joshua Kurlantzick, "Is Thailand Regressing on Lèse-Majesté?" *Asia Unbound* (blog), Council on Foreign Relations, September 12, 2011, http://blogs.cfr.org/asia/2011/09/12/is-thailand-regressing-on-lese-majeste/
[48] FACT and the Political Prisoners in Thailand websites are now available, as are websites related to the red-shirt movement as a key constituency of the ruling Pheu Thai party.
[49] Freedom House tests on *Prachatai* and *Asia Sentinel* indicated that the sites loaded more slowly than others and that some pages were inaccessible, with the user redirected to a message stating that it had been blocked by the MICT, though other pages were available.
[50] iLaw, "Statistics of Website Censorship."
[51] "Thailand Blocks 5,000 'Royal Insult' Web Pages," Agence France-Press, May 14, 2012, http://bit.ly/15BTYf0.

marked increase over 2011, when a mere 33 orders relating to 5,000 URLs were approved, and was more than the sum of court orders authorized in 2009 and 2010 together, which amounted to 142.[52] Despite this frenzy of activity, the number of individual sites affected by each order has actually declined, since the total 26,000 URLs censored in 2011 and 2012 under Prime Minister Shinawatra are considerably fewer than the number affected by orders placed during 2009 and 2010 under former Prime Minister Abhisit Vejjajiva, which was a period of significant political upheaval (28,705 and 45,357 URLs respectively).[53]

Thai courts are now much more likely to censor political opinion than pornography or other illegal content. Since 2007 criminal courts have authorized 219 orders preventing access to 77,491 URLs containing pictures and contents against lèse-majesté law or article 112 of the criminal code,[54] compared to 76 orders censoring 23,456 URLs for pornographic content.[55]

Website blocks are frequently excessive. A criminal court blocked the URL for legal website *Nitirat* based on the national-security related CCA article 20 for publishing the "First Declaration of the People's Party"—a historical treatise advocating a constitutional monarchy in Thailand[56]—even though it was available on several other uncensored websites.

In addition to blocking, the government employs administrative measures and political pressure to limit the spread of online information, especially on social media. Anecdotally, internet freedom activists report that before the 2007 Computer-related Crime Act, the government would approach service providers to cooperate in website censorship. Even after that process was formalized, the spirit of collaboration lingers, and some content is restricted without the need for a court order. The citizen journalist website *Thaiflood*—which hundreds of thousands of Thais were following for updates after 2011 floods—complained that the official relief agency sought the right to screen and potentially censor its content before publication.[57]

Censors also request assistance from international providers. In 2011, journalists reported the MICT had asked Facebook to censor over 90,000 URLs suspected of violating lèse-majesté laws,[58] and that the company had removed 10,000 URLs and 50 user accounts. Facebook did not confirm this account in published reports.[59] Google reported that the Thai government—under two prime

[52] iLaw, "Statistics of Website Censorship."
[53] iLaw, "Statistics of Website Censorship."
[54] Section 112: "Whoever, defames, insults or threatens the King, the Queen, the Heir-apparent or the Regent, shall be punished with imprisonment of three to fifteen years."
[55] iLaw, "Statistics of Website Censorship."
[56] International Network of Engaged Buddhists, "How to Achieve our Democracy", accessed February 2013, http://www.inebnetwork.org/news-and-media/6-articles/397-how-to-achieve-our-democracy; "MICT Blocks Nitirat Page on 1st Declaration of the People's Party," *Prachatai*, December 15, 2013, http://www.prachatai.com/english/node/3456.
[57] Committee to Protect Journalists, "Thailand Tries to Censor Site Devoted to Flood News," news alert, October 25, 2011, http://cpj.org/2011/10/thailand-tries-to-censor-site-devoted-to-flood-new.php.
[58] Freedom Against Censorship Thailand, "Thailand blocks 96,000 Facebook pages - Bangkok Pundit" news release, December 28, 2011, http://facthai.wordpress.com/2011/12/28/thailand-blocks-96000-facebook-pages-bangkok-pundit/.
[59] Bangkok Pundit, "Thailand: Is a Lèse-Majesté Crackdown Around the Corner? UPDATE: ICT Asks FB to Block Thousands of Sites," *Asian Correspondent*, November 25, 2011, http://asiancorrespondent.com/70492/is-a-lese-majeste-crackdown-around-the-corner/; "MICT has Requested Facebook to Delete Over 10,000 Pages Offensive to the Monarchy," *Prachatai*, November 24, 2011, http://www.prachatai.com/english/node/2913.

ministers—sent six requests between January and December 2011 to remove a total of 374 clips from its YouTube video-sharing platform for allegedly insulting the monarchy—all without a court order. Google largely complied, restricting Thai users from accessing 80 percent of them.[60] Google reported no requests between June and December 2012, though it complied with two to delete 14 items on YouTube for criticizing the government in the first half of the year.[61] And the Thai government was quick to welcome the microblogging service Twitter's new feature enabling country-specific censorship of tweets in 2012, though it is not clear if the feature has been implemented.[62]

Proactive state manipulation of online discussion happens occasionally but has not had a significant impact on online discourse. More prevalent is the use of volunteers to scrutinize suspicious websites and report their findings to the MICT. Ministry hotlines inviting users to report offensive websites were established in 2010, along with an equivalent Facebook group.[63] A joint MICT and ministry of justice "cyber scout" project to train students as web monitors was inaugurated the same year;[64] by 2011, several dozen were patrolling forums and social networks—without identifying themselves as working with the government—to warn users posting lèse-majesté content report them if they refused to delete it.[65] Such manipulation was less noticeable in 2012 and 2013, suggesting the 2011 spike may have been tied to the elections.

Not all such measures are government-sponsored. A network of users calling themselves the "Social Sanction" group has launched online campaigns to vilify individuals who express views deemed disrespectful of the monarchy, sometimes sparking official investigations of the targeted user.[66] Other internet users have launched their own countermeasures against "Social Sanction" and similar groups, posting online the personal information of individuals they believe belong to such communities.[67]

These measures, along with prosecutions and other violations of internet users' rights in recent years, has a chilling effect, and many people engage in self-censorship when communicating online, even among friends within a closed network. Official statements have encouraged this trend. In

[60] Google, "Thailand; "Removals,"" *Transparency Report*, January to June 2011 and July to December 2011, http://www.google.com/transparencyreport/removals/government/TH/.
[61] Google, "Thailand; "Removals,"" *Transparency Report*, July to December 2012, http://www.google.com/transparencyreport/removals/government/TH/.
[62] Jon Russel, "Thailand is the World's First Government to Endorse Twitter's Censorship Feature," *The Next Web*, January 30, 2012, http://tnw.co/xmXzx9.
[63] Reporting Association of Thailand Facebook page, https://www.facebook.com/reportthailand. As of August 2013, the page had over 25,000 "likes."
[64] Mong Palatino, "Cyber Scout: Thailand's Internet Police?," *Global Voices*, December 24, 2010, http://globalvoicesonline.org/2010/12/24/cyber-scout-thailandpercentE2percent80percent99s-internet-police/.
[65] Daniel Rook, "Thai 'Cyber Scouts' Patrol Web for Royal Insults," Agence France-Presse, May 10, 2011, http://bit.ly/jlUKfl.
[66] Sawatree Suksri, Siriphon Kusonsinwut, and Orapin Yingyongpathana, *Situational Report on Control and Censorship of Online Media, Through the Use of Laws and the Imposition of Thai State Policies* (Bangkok: iLaw Project, 2010), 14, http://www.boell-southeastasia.org/downloads/ilaw_report_EN.pdf
[67] Thai Netizen Network, *Thailand Internet Freedom and Online Culture Report 2011* (Bangkok: Thai Netizen Network 2012): 54-76.

2011, the ICT minister warned users that "liking" lèse-majesté content on Facebook could result in prosecution for "indirectly distributing inappropriate content" under the CCA.[68]

Online activists have proved resilient and creative in countering limits on content. Circumvention software to access blocked sites is readily available online, and content producers often republish information on alternate sites. The Thai Netizen Network advocacy group, which defends users' rights to access, free expression, and privacy, was founded in 2009.[69]

Despite constraints surrounding royal institutions, many political, social, and human rights issues are freely and passionately debated online in Thailand. Political parties mobilize supporters via ICT platforms, like a November 2012 ice-cream eating flash mob organized a red-shirt activist in protest against royalist Boonlert Kaewprasit. News reports had quoted Boonlert, a former general, advocating a five-year political "freeze," substituting military leadership for democratic rule.[70] Both red- and yellow-shirt movements used social media to organize offline actions in the run-up to 2011 elections, contributing to an opposition victory which observers considered free and fair. Since then, media experts say government or corporate advertisements are distributed to online news outlets across the political spectrum, where before the partisan allocation of resources threatened their financial stability and the diversity of views available to internet users; some red-shirt supporters created their own advertising market.

Meanwhile, advanced web applications such as YouTube, Facebook, Twitter, and international blog-hosting services like Blogger are popular and freely available, though individual pages or videos may be blocked. One 2011 study reported a huge 85 percent of Thai internet users visiting a social media website at least once a week.[71] Such sites have become important spaces for political expression and key channels for disseminating news, information, and demands for accountability. In December 2012, Facebook users prompted an airline to investigate one of its stewardesses who vented on her personal account about a passenger's political affiliation.[72]

Social media has even facilitated public discussion of lèse-majesté provisions. In the past year, a "Free Somyot" campaign was carried out on behalf of an editor imprisoned under the law,[73] and a Facebook group organized by academic Suda Rangkupan inspired some politicians to draft a bill to pardon political prisoners, including some convicted of lèse-majesté.[74] The Campaign Committee

[68] Hana Stewart-Smith, "Thai Facebook Users Warned Over Anti-Monarchy 'Likes'," *ZDNet*, November 26, 2011, http://www.zdnet.com/blog/asia/thai-facebook-users-warned-over-anti-monarchy-likes/286.
[69] Thai Netizen Network, accessed July 2013, https://thainetizen.org.
[70] "Ice-cream Protest Mocks Boonlert," *Bangkok Post*, November 16, 2012, http://www.bangkokpost.com/lite/news/321636/ice-cream-protest-mocks-pitak-siam.
[71] Simon Kemp, "Social Digital and Mobile in Thailand," *we are social* (blog), January 3, 2012, http://wearesocial.net/blog/2012/01/social-digital-mobile-thailand/.
[72] "Cathay Pacific Fires Flight Attendant in Paetongtarn Case," *The Nation*, December 4, 2012, http://www.nationmultimedia.com/politics/Cathay-Pacific-fires-flight-attendant-in-Paetongta-30195555.html
[73] Free Somyot Facebook page, accessed July 2013, https://www.facebook.com/pages/Free-Somyot/122999694453000; Free Somyot Twitter page, accessed July 2013, https://twitter.com/freesomyottrial. See also, Atapoom Ongkulna and Pimnara Pradubwit, "Rally Over 'Political Prisoners,'" *The Nation* (Bangkok), January 29, 2013, http://www.nationmultimedia.com/politics/Rally-over-political-prisoners-30198912.html.
[74] Atapoom Ongkulna and Pimnara Pradubwit, "Rally Over 'Political Prisoners.'" http://www.bangkokpost.com/news/politics/337297/critics-slam-blanket-amnesty-bill).

for the Amendment of Article 112, a coalition of academics and civil society groups, attracted 30,000 signatures to a petition demanding lèse-majesté reforms, such as reducing punishments for violations and enabling only the king's private secretary to initiate charges.[75] Parliament rejected the petition on technical grounds, but the effort prompted an unprecedented level of coverage in the traditional media.

The government is also embracing social networks to promote policy. Top leaders update the public frequently on Facebook, especially during election campaigns. In March 2013 during the election of the governor of Bangkok, candidates used Facebook and Twitter alongside billboards and speeches, though digital tools do not yet have the reach of traditional media, particularly in rural areas.[76]

VIOLATIONS OF USER RIGHTS

Under Yingluck Shinawatra, legal harassment of internet users under lèse-majesté provisions and the CCA has continued at the same rate as before the 2011 election, if not worsened. The most notorious conviction of 2012 involved Chiranuch Premchaiporn, the director and administrator of *Prachatai*, who was given a suspended jail term for failing to delete user comments in 2008. A tragic death highlighted the use of these charges to imprison citizens without known political connections, often following questionable legal proceedings. Ampol Tangnopakul died in May, just months into a 20-year sentence he was serving for allegedly sending anti-royal SMS messages. The court had rejected the elderly cancer-sufferer's defense that he couldn't use a mobile phone, along with multiple applications for bail and a medical appeal. Since a cabinet directive was implemented in May 2012, CCA investigations fall under the purview of the Department of Special Investigations who can intercept electronic communications without a court order.

The Constitution of the Kingdom of Thailand 2007, which replaced an interim charter imposed by the military government after the 2006 coup, guarantees freedom of expression in chapter three, section 45. However, other laws have been used to curtail free expression, including the Internal Security Act of 2007, the Emergency Decree on Public Administration in Emergency Situations 2005, and especially the 2007 CCA, which groups broad content violations with criminal activities like hacking, e-mail phishing, uploading personal content without consent, and posting obscene material. A range of civil society groups and scholars oppose the CCA for infringing on users' rights to privacy, information, and freedom of expression,[77] and allowing the prosecution of content providers or intermediaries—such as webmasters, administrators, and managers—accused of

[75] Under the constitution, lawmakers must consider citizen-initiated legislative changes if they receive at least 10,000 signatures. "Campaign Committee for the Amendment of Article 112" [in Thai], accessed July 2013, http://www.ccaa112.org/; Campaign Committee for the Amendment of Article 112 Facebook page, accessed July 2013, https://www.facebook.com/ccaa112.

[76] Jon Russell, "How Influential is Social Media in Thailand's Election?," *Asian Correspondent*, June 10, 2011, http://asiancorrespondent.com/56997/how-influential-is-social-media-in-thailands-election/.

[77] Sarinee Achavanuntakul, "Danger! Computer Crimes Act" [in Thai], *Fringer Blog*, July 18, 2007, http://www.fringer.org/?p=259; "Freedom of Expression (Still) Under Attack," *Political Prisoners of Thailand* (blog), June 12, 2012, https://politicalprisonersofthailand.wordpress.com/2012/06/12/freedom-of-expression-still-under-attack/.

posting or allowing the dissemination of content considered harmful to national security or public order.[78] The executive authorities are left to decide what amounts to a violation under these vaguely defined terms, and criminal courts make the final judgments.[79] In addition, harsh defamation and lèse-majesté provisions in the penal code that are generally applied to online expression, as well as traditional media, assign penalties of up to 15 years in prison for criticism of the king, the royal family, or Buddhism.[80] In 2010, 478 lèse-majesté cases were filed under Article 112.[81]

Thai authorities persistently pursue criminal prosecutions relating to online activity. A total of 325 defendants were charged under the CCA between 2007 and 2011.[82] Among those, only 19 percent involved data and computer crimes; 66 percent stemmed from content violations under articles 14-16 of the act. The nature of the charges in a remaining 48 cases is unclear.[83] Of the cases involving content, 100 were defamation charges and 46 lèse-majesté violations; only 31 were for pornography.[84] These prosecutions have drawn local and international condemnation because of the harsh pre-trial treatment of detainees, the punishments imposed, and the judges' reliance on questionable evidence. Yingluck Shinawatra's administration, instead of checking this trend, has returned guilty verdicts in cases inherited from the previous government.

On May 31, 2012, a court sentenced *Prachatai's* Chiranuch Premchaiporn to eight months in jail and a THB 20,000 ($673) fine for failing to delete reader comments in one of the most high-profile of these verdicts. While Thai authorities have prosecuted intermediaries for failing to delete content before,[85] Chiranuch—who the media sometimes refer to by her nickname, Jiew—was among first defendants prosecuted for computer crimes, the first accused solely on the basis of third-party content, and, as a 44-year-old journalist and human rights activist, represented a largely apolitical target.[86] First arrested in a raid on the site's premises in March 2009, Chiranuch was charged because the site's moderators—who, like administrators around the world, rely on the community to report offensive content posted to their dynamic discussion forums—were delinquent in deleting ten10 anti-royal remarks, although they removed them all within 20 days.[87]

---

[78] Sections 14(1), 14(3), and 14(5) and Article 15 of the 2007 Computer Crimes Act pertain to crimes that "involve import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to a third party or the public; that involve import to a computer system of any computer data related to an offense against the kingdom's security under the criminal code; that involve the dissemination or forwarding of computer data already known to be computer data [which are illegal]." The act states that "any service provider intentionally supporting or consenting to an offense…within a computer system under their control shall be subject to the same penalty as that imposed upon a person committing an offense." See, "An unofficial translation of the Computer Crime Act," *Pratachai,* July 24, 2007, http://www.prachatai.com/english/node/117.

[79] Suksri et al, *Impact of the Computer-related Crime Act,* 520.

[80] Karin Deutsch Karlekar, ed., "Thailand," in *Freedom of the Press 2010* (New York: Freedom House, 2010), http://www.freedomhouse.org/template.cfm?page=251&year=2010.

[81] "Freedom of Expression (Still) Under Attack," *Political Prisoners of Thailand*.

[82] Suksri et al, *Impact of the Computer-related Crime Act*, 467. Figures for 2012 are not yet available.

[83] Suksri et al, *Impact of the Computer-related Crime Act*.

[84] Suksri et al, *Impact of the Computer-related Crime Act*.

[85] "Nor Por Chor USA Web Designer Sentenced to 13 Years in Jail," *Prachatai*, March 16, 2011, http://www.prachatai.com/english/node/2366.

[86] James Hookway, "Conviction in Thailand Worries Web Users," *Wall Street Journal*, May 30, 2012, http://online.wsj.com/article/SB10001424052702303674004577435373324265632.html.

[87] Danny O'Brien, "Computer Crime Laws Belie Thai Claim to Modern Society," *CPJ Internet Channel,* May 31, 2012,

Police arrested her again in September 2010 on fresh counts of "defaming the royal family," violating Articles 14 and 15 of the CCA, and Article 112 of the penal code, in relation to the same handful of comments. Perhaps because of local and international attention to the case, Chiranuch, unlike many defendants in lèse-majesté cases, was granted bail of THB 200,000 ($6,730),[88] and her suspended sentence was far less than the maximum, which would not have been allowed to exceed 20 years even if she had been convicted on all counts, though some of her supporters mistakenly believed she was facing as many as 80 years behind bars.[89] In an ironic acknowledgement that Chiranuch herself had not committed a crime, the sentence was suspended, and she did not serve time.[90] The judge described the system he was perpetuating as "unfair."[91]

CCA Article 15 states that administrators who fail to stop internet users from posting banned content are "supporting or consenting to" the post and face the same penalties as if they had created it themselves.[92] This serves as a discouragement to service providers, since the constant monitoring it demands from website owners is time consuming and inefficient. Moreover, the law fails to establish time frame for service providers to delete offending content. The court's failure to clarify this omission in its interpretation of the law in Chiranuch's case is particularly problematic, and many observers in the legal, IT, and free expression sectors fear the sentence, though suspended, could increase self-censorship by media outlets and service providers in Thailand for years to come. That fear was compounded by the January 2013 sentencing of Somyot Prueksakasemsuk, editor of the *Voice of Taksin* print magazine, to 10 years imprisonment for lèse-majesté involving two articles he published, but did not author;[93] the conviction followed 20 months in detention—despite 13 attempts to obtain bail—since Somyot's 2010 arrest while campaigning to overturn lèse-majesté laws.[94]

Other recent CCA and lèse-majesté prosecutions reveal further concerning implications about the wording of the laws, and the courts' harsh interpretation of them.

- Though records compiled by lawyers and free expression groups are incomplete, most of the defendants appear to be ordinary Thais like Abhinya Sawatvarakorn, a 19-year-old university student nicknamed Kantoop, rather than well-known activists or government opponents. In February 2012, Kantoop became the youngest person to appear before a

---

https://cpj.org/internet/2012/05/computer-crime-laws-belie-thailands-claim-to-moder.php.

[88] Reporters Without Borders, "Prachatai Editor Released on Bail," September 24, 2010, http://en.rsf.org/thailand-news-website-editor-arrested-on-24-09-2010,38440.html.

[89] Political Prisoners in Thailand, "Chiranuch Premchaiporn," accessed July 2013, http://thaipoliticalprisoners.wordpress.com/decidedcases/chiranuch-premchaiporn/.

[90] Suchit Leesa-nguansuk, "Don't Shoot the Messenger," *Bangkok Post*, June 27, 2012, http://m.bangkokpost.com/business/299889.

[91] O'Brien, "Computer Crime Laws Belie Thai Claim to Modern Society."

[92] Section 15: "Any service provider intentionally supporting or consenting to an offence under Section 14 within a computer system under their control shall be subject to the same penalty as that imposed upon a person committing an offence under Section 14."

[93] Asian Human Rights Commission, "THAILAND: Verdict In Case Of Human Rights Defender Is A Serious Threat To Freedom Of Expression", January 24, 2013, http://www.humanrights.asia/news/ahrc-news/AHRC-STM-027-2013.

[94] iLaw, "Case 61" [in Thai], accessed July 2013, http://freedom.ilaw.or.th/case/61.

judge on lèse-majesté charges for a comment she had posted to Facebook in 2009.[95] She had yet to be prosecuted in May 2013, but at least one news report said she was forced to change universities after one institution refused admission in connection with the allegations.[96]

- Judges hearing the cases often display a limited understanding of the technical dimensions of digital communication, and convict users even when the evidence against them is inconclusive. Website designer Thanthawut Thaweewarodomkul was sentenced to 13 years in prison in 2011 despite discrepancies in the electronic evidence tying him to the offending content.[97]

- Convictions for lèse-majesté carry significant social stigma that affects their treatment in prison. Thanthawut and others report guards and fellow prisoners targeting them for abuse in jail.[98]

- Professional lawyers and IT experts can be reluctant to contribute to the defense of lèse-majesté and CCA crimes on grounds that it might hurt their careers. In November 2011, 61-year-old Ampol Tangnopakul was sentenced to 20 years in prison for allegedly sending text messages insulting the monarchy to a high-ranking government official.[99] The prosecutor failed to prove he had sent the offending content, and Ampol—who traditional media dubbed "Uncle SMS"[100]— said he did not even know how to text. Yet his legal team could not find an expert willing to testify that IMEI numbers, which identify mobile handsets, can be counterfeited. The court denied eight separate applications for bail running up to Ampol's trial,[101] and he died in jail of liver cancer on May 8, 2012, three days after his application for appeal on medical grounds was rejected.[102]

- Companies and individuals have also used the CCA and penal code provisions from personal motives.[103] Police interrogated two suspects reported collecting or disseminating

[95] Nirmal Ghosh, "Thai Divide Growing Over Lèse-Majesté Law," *Jakarta Globe*, January 25, 2012, http://www.thejakartaglobe.com/international/thai-divide-growing-over-lese-majeste-law/493508. Pavin Chachavalpongpun, "Kantoop and lese-majeste," New Mandala (blog), February 3, 2012, http://asiapacific.anu.edu.au/newmandala/2012/02/03/kantoop-and-lese-majeste/.
[96] iLaw, "Case 236" [in Thai], accessed July 2013, http://freedom.ilaw.or.th/case/236; Ghosh, "Thai Divide Growing Over Lèse-Majesté Law."
[97] "Nor Por Chor USA Web Designer Sentenced to 13 Years in Jail," *Prachatai*.
[98] Apilaporn Vechakij, "Thai Royal Insult Inmates 'Pariahs' in Prison," Agence France-Presse, August 23, 2012, http://www.google.com/hostednews/afp/article/ALeqM5jG1_z8WM3tNbwhxw5ceqI77glENA.
[99] Asian Human Rights Commission, "THAILAND: Twenty Years in Prison for Four SMS Messages," November 24, 2011, http://www.humanrights.asia/news/ahrc-news/AHRC-STM-180-2011.
[100] Ampol's case received more traditional media coverage than most lese majeste trials. iLaw, "Case 21" [in Thai], accessed July 2013, http://freedom.ilaw.or.th/case/21.
[101] iLaw, "Case 21."
[102] "Thailand's Lèse-Majesté Laws :An Inconvenient Death," *Economist*, May 12, 2012, http://www.economist.com/node/21554585
[103] Thai Netizen Network, "Thailand: Cybercrime Acts vs. the Right to Freedom of Expression," June 2, 2011, https://thainetizen.org/docs/thailand-cybercrime-acts-vs-the-right-to-freedom-of-expression/.

information detrimental to the monarchy in 2011.[104] Another 2011 case resulted in charges of defamation and importing "false computer data" against labor union activist Songkram Chimcherd over e-mails regarding a dispute with a company over unpaid worker compensation; a court dismissed the case in May 2012 because the prosecutor could not prove who sent the e-mail.[105]

- So strong is the law's emphasis on proof of innocence that only two computer crimes cases involving lèse-majesté law have been dismissed on these grounds since the 2006 coup. One involved Surapak Phuchaisaeng,[106] who was arrested in September 2010 for allegedly creating a Facebook page parodying a 1950 speech by King Bhumiphol Adulyadej. The court dismissed the case on October 31, 2012, yet Surapak was offered no compensation or redress for the two years he was held without bail.[107]

- In February 2012, Human Rights Watch voiced concerns over Thai courts' "politically motivated" refusal to grant bail to lèse-majesté defendants, particularly those affiliated with the red-shirt movement.[108]

- Lengthy pre-trial detentions without bail also deplete defendants' resources to fight unfair convictions. Joe Gordon (also known as Lerpong Wichaikhammat), a dual Thai-U.S. citizen,[109] was sentenced in December 2011 to two and a half years in prison for posting excerpts from the banned book *The King Never Smiles* on his blog while in the United States.[110] He pled guilty after bail was denied nine times over 84 days of pretrial detention,[111] and was eventually pardoned and released in July 2012.[112] Legal experts believe he lacked effective legal counsel and confessed in hopes of early release, but the verdict cannot be overturned, and Gordan now lives permanently in the United States.

- Prosecutors, aware of international condemnation of Thai lèse-majesté laws, can prosecute cases under other charges, though the impetus for the investigation clearly stems from anti-royal content. On December 25, 2012, internet user Katha Pachariyaphong was sentenced to four years in prison for translating a Bloomberg news agency article about the health of

[104] "Recent Crackdown on Cyber Dissidents," *Prachatai*, March 10, 2012, http://www.prachatai.com/english/node/3096.
[105] iLaw, "Case 177" [in Thai], accessed July 2013,http://freedom.ilaw.or.th/en/case/177#detail.
[106] iLaw, "Case 176" [in Thai], accessed July 2013,http://freedom.ilaw.or.th/case/176.
[107] "Netizen Freed for Lack of Evidence in Lèse-Majesté Case," *Prachatai*, November 3, 2012, http://www.prachatai.com/english/node/3418
[108] Human Rights Watch, "Thailand: Courts Denying Bail in Lèse-Majesté Cases," February 23, 2012, http://www.hrw.org/news/2012/02/24/thailand-courts-denying-bail-lese-majeste-cases.
[109] Human Rights Watch, "Thailand: Courts Denying Bail."
[110] "US Citizen Jailed for Insulting Thai Monarchy," Reuters, December 8, 2011, http://af.reuters.com/article/worldNews/idAFTRE7B709A20111208.
[111] Kocha Olarm and Jethro Mullen, "Thai-American Jailed for Insulting Monarchy Receives Royal Pardon," CNN, July 11, 2012, http://edition.cnn.com/2012/07/11/world/asia/thailand-american-pardon/index.html.
[112] "Thai King Pardons US Man Jailed for Royal Insult," BBC News, July 11, 2012, http://www.bbc.co.uk/news/world-asia-18792430.

King Bhumiphol Adulyadej and posting it to a web forum.[113] He was charged with spreading rumors under CCA article 14(2). Bloomberg, the original publisher, was not mentioned by the plaintiff.

The scale of ICT surveillance in lèse-majesté and other cases in Thailand is unclear, although the CCA requires ISPs and webmasters to retain data logs for up to 90 days and turn data over to investigators upon request. One police officer reported needing up to three days to trace the source of offensive online comments in 2009.[114] Since then, the government has strengthened its capacity to intercept private communications. A cabinet directive effective since its publication in the Royal Gazette in May 2012 placed several types of cases, including violations of the CCA, under the jurisdiction of the Department of Special Investigation (DSI).[115] Under rules regulating DSI operations, intercepting internet communications and collecting personal data in CCA cases no longer needs a court order.[116] Even in cases where court orders are still required, Thai judges—as with censorship decisions—typically approve such requests without serious deliberation. And Chalerm Yoobamrung's THB 400 million ($13.46 million) "lawful interception" system proposed in December 2011, which would have monitoring and content filtering applications, could potentially bypass the need to go through ISP staff altogether, with or without the court's sanction, by allowing law enforcement agencies direct access to user data files.[117] Aware of this trend, some internet users and political activists already exercise caution when communicating online, and employ additional security and privacy tools to evade surveillance.

Customers at cybercafes must present identification cards, though smaller businesses do not always comply with this rule. Mobile phone users are required to register their real names and national ID with their carrier upon purchasing a SIM card, whether prepaid or for a long-term subscription. Although the rule is less strictly enforced for prepaid SIM cards, those who do not register are unable to receive certain services, including roaming or mobile phone reception, in the southern provinces of Pattani, Yala, and Narathiwat.[118]

Internet users who post controversial content can face harassment outside the legal system, including physical violence. In February 2012, two unidentified men on motorbikes assaulted Worachet Pakeerut, one of several academics leading a petition campaign to amend lèse-majesté provisions. The Asian Human Rights Commission advocacy group said the attack represented an "ominous escalation of the dangers" faced by those promoting critical discussion of Article 112.[119]

---

[113] "Former Stock Broker Gets 4 Years for Posting Two Webboard Comments in 2009," *Prachatai*, December 12, 2012, http://www.prachatai.com/english/node/3468; "Translation Posted After SET Fell," *Prachatai*, November 3, 2009, http://www.prachatai3.info/english/node/1474.
[114] Freedom House interview with a senior police officer specializing in ICT crimes who requested anonymity, March, 2009.
[115] "Cabinet Approves Draft Directive for Setting Guidelines of DSI Cases," *The Nation* (Bangkok), December 19, 2011, http://www.nationmultimedia.com/breakingnews/Cabinet-approves-draft-directive-for-setting-guide-30172173.html.
[116] "DSI Added Special Case for 9 Offenses" [in Thai], VoiceTV, May 25, 2011, http://news.voicetv.co.th/thailand/40014.html.
[117] "Web Censor System Hits Protest Firewall," *Bangkok Post*, December 15, 2011, http://www.bangkokpost.com/news/local/270812/web-censor-system-hits-protest-firewall.
[118] Happy, "Register SIM Card," accessed January 2013, http://bit.ly/1fRL5ji.
[119] "Thailand's Struggle to Face its Future," *Asia Sentinel*, April 27, 2012, http://www.asiasentinel.com/index.php?option=com_content&task=view&id=4459&Itemid=189.

There have been sporadic reports of hacking attacks on online news outlets. Prachatai repeatedly faced denial-of-service (DoS) attacks during periods of political turmoil in 2009 and 2010 before being blocked by the authorities. The attacks forced the outlet to change servers and set aside large sums to pay for extra bandwidth. A web administrator for the news outlet reported in February 2012 that the site continued to face attacks but was able to stay online thanks to the bandwidth upgrade.

Hackers are also increasingly targeting government websites, which have developed a reputation for inadequate security. In September 2012, police arrested a 16-year-old for hacking the ministry of education website and altering content in protest against strict school regulations.[120] Attackers accessed a Thai navy web forum and published user names and passwords online in December 2012.[121] In January 2013, hackers added links to a gambling platform to the ministry of culture's website in order to boost traffic and search engine optimization for the illegal site;[122] a day later, an apparently separate attack on the same website added an image from a controversial political television drama which broadcasters pulled off the air due to inappropriate content, stimulating public debate about whether authorities had pressured them to censor the show.[123]

[120] "Young Student Hacked Ministry of Education Website Surrendering," *Thairath*, September 18, 2012, http://www.thairath.co.th/content/edu/292058.
[121] "Web Forum Database of Royal Thai Navy is Hacked," *Blognone*, December 22, 2012, http://bit.ly/YwxYNB.
[122] "Link to Football Bet Found on Website of Ministry of Culture," *Blognone*, 15 January, 2013, http://www.blognone.com/node/39996.
[123] "Website of Ministry of Culture is Repeatedly Hacked" [in Thai], *Spring News*, 16 January, 2013, http://news.springnewstv.tv/24030/.

TUNISIA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	14	12
Limits on Content (0-35)	12	8
Violations of User Rights (0-40)	20	21
Total (0-100)	**46**	**41**

* 0=most free, 100=least free

POPULATION: 10.8 million
INTERNET PENETRATION 2012: 42 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- State control over the internet backbone has weakened as ISPs may now bypass the Tunisian Internet Agency to access international networks directly (see **OBSTACLES TO ACCESS**).
- Online journalists received new protections through the implementation of Decree-law 115 that provides them with many of the same rights afforded to traditional journalists, although the remaining presence of laws from the Ben Ali era and delays over a new constitution continued to threaten freedom of expression online (see **VIOLATIONS OF USER RIGHTS**).
- One user had his 7.5 year prison sentence confirmed for online posts deemed offensive to Islam, while an online investigative journalist faced harsh criminal defamation charges related to a story in which she exposed government corruption (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

The internet was first launched for public use in Tunisia in 1996, and the first broadband connections were made available by the end of 2003. Despite a relatively advanced internet infrastructure and a developed telecommunications market, extensive internet filtering had hindered free web access. Former autocratic President Zine El Abidine Ben Ali's internet censorship and surveillance systems had earned Tunisia the title of "internet enemy" in 2009[1] and 2010[2] alongside Burma, China, Saudi Arabia, and Iran. Numerous websites and Web 2.0 tools such as the photo-sharing site Flickr and video-sharing site YouTube were blocked in order to deny citizens access to content critical of the ruling region. Nonetheless, internet usage continued to grow and an increasing number of netizens started employing encryption techniques and proxy servers to circumvent government censorship and surveillance.

The Tunisian internet landscape changed dramatically with the ouster of Ben Ali on January 14, 2011. His repressive censorship apparatus largely dissipated and internet users have started to enjoy an unprecedented level of web access. However, old habits die hard; fears of the comeback of Ammar404 (the nickname Tunisian netizens gave to internet censorship during the Ben Ali era, based on the 404 "file not found" message) reemerged in May 2011 with attempts to filter adult content and the blocking of five Facebook pages critical of the military institution. From May 2012 to April 2013, authorities took significant steps to open up the country's control over internet and communication technologies (ICTs). Speaking at a press conference held on September 6, 2012, ICT Minister Mongi Marzoug officially announced the "death of Ammar404."[3] That same month, Tunisia joined the Freedom Online Coalition, a group of governments "committed to collaborating to advance internet freedom."[4] In another positive development, internet service providers (ISPs) can now directly access international data traffic lines, thereby decentralizing the ICT infrastructure out of the hands of a powerful few.

Despite of these commendable steps, Tunisia's fragile internet freedom is still threatened by a number of laws dating from the Ben Ali era, including the Telecommunications Decree and the Internet Regulations. The judiciary continues to restrict free speech through the prosecution of users over content posted online, mainly regarding defamation, religion, or insults to state bodies. Finally, over the past year, bloggers, activists, and civil society groups who criticize the country's political figures or offend cultural sensitivities faced cyberattacks and personal threats from a diverse range of nonstate actors.

[1] Reporters Without Borders, "Internet Enemies, 2009," March 12, 2009, http://www.rsf.org/IMG/pdf/Internet_enemies_2009_2_-3.pdf.
[2] Reporters Without Borders, "Internet Enemies, 2010," March 12, 2010, http://en.rsf.org/IMG/pdf/Internet_enemies.pdf.
[3] All Africa, "Tunisia: Information and Communication Minister - 'Internet Censorship No Longer Implemented in Tunisia'," allafrica.com, September 6, 2012, http://allafrica.com/stories/201209070049.html.
[4] "Tunisia joins the Coalition Freedom Online & hosts the third edition of the Conference," ATI, September 2012, http://www.ati.tn/en/actus_details.php?id=291.

OBSTACLES TO ACCESS

Internet usage in Tunisia has grown rapidly in recent years, even as access remained restrictive under the Ben Ali regime. According to the International Telecommunication Union (ITU), internet penetration in the country stood at 42 percent in 2012, up from 17 percent in 2007.[5] Although the government has actively sought to improve the country's ICT sector, access is still hindered by high prices and underdeveloped infrastructure.

The Ben Ali regime attempted to increase access to ICTs through investments in infrastructure and greater competition among ISPs. In 2004, the government set up a "Family PC" initiative to encourage widespread computer use by removing customs fees, setting a price ceiling for computer hardware, arranging low interest rate loans for families to purchase ICT tools, and including an internet subscription with every computer sold. As a result, the number of computers per 100 inhabitants rose from approximately 12 in 2009 to 16 as of November 2012,[6] while the number of total internet subscriptions is estimated to have exceeded 1 million in 2012.[7]

The popularity of mobile phones is also on the rise, with over 12.8 million mobile phone subscriptions and a penetration rate of 118.6 percent as of December 2012.[8] Less common, however, is the use of mobile internet connections due to costs which remain beyond the reach of many Tunisians.

State-controlled Tunisie Télécom and mobile phone company Orange Tunisie provide 3G internet services through a plug-in USB key that enables laptops to connect to the mobile network. The device costs at least TND 59 (approximately $38), while the service costs TND 30 ($18.50) per month. Tunicell and Tunisiana also launched 3G mobile service in August 2011[9] and 2012, respectively, with the latter covering an estimated 87 percent of the population as of early 2013.[10] In early 2013, Tunisie Télécom announced plans to set up 18 new mobile 3G base stations in several regions of the country, including rural areas, and to install 500 kilometers of fiber optic

[5] "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," International Telecommunication Union (ITU), 2007 & 2012, accessed July 2, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[6] ICT ministry, "Indicateurs et données statistiques TIC—Accés et infrastructure TIC: Le nombre d'ordinateurs pour 100 habitants" [ICT Indicators and Statistical Data—ICT Access and Infrastructure: Number of Computers per 100 Inhabitants], accessed January 21, 2013, http://www.mincom.tn/index.php?id=315&L=0.

[7] ICT ministry, "Indicateurs et donnees statistiques TIC : Nombre d'abonnements au réseau Internet" [ICT indicators and Statistical Data : number of internet subscriptions], http://www.mincom.tn/index.php?id=305&L=3, accessed February 4, 2013

[8] Instance National des Télécommunications (INT), "Suivi des principaux indicateurs du marché de la téléphonie mobile en Tunisie" [Monitoring of main indicators regarding the mobile market in Tunisia], December 2012, http://www.intt.tn/upload/files/Tableau%20de%20Bord%20Mobile%20-%20D%C3%A9cembre%202012.pdf.

[9] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[10] International Telecommunication Union (ITU), "Qtel Group celebrates launch of 3G services in Tunisia," 2012, published August 14, 2012, http://www.itu.int/ITU-D/ict/newslog/Qtel+Group+Celebrates+Launch+Of+3G+Services+In+Tunisia+Tunisia.aspx

cables in the governorate of Béja in northwestern Tunisia.[11] Orange Tunisie also expanded 2G and 3G services in three rural towns.[12] These developments signal greater competition in the broadband market, extended coverage of the 3G network to rural regions of the country, and a more open internet ecosystem. The number of 3G internet subscriptions continued to increase, reaching more than 557,000 subscriptions in December 2012 compared to 254,000 subscriptions in December 2011.[13]

Most Tunisians access the internet at their workplace or at privately-owned cybercafés known as "publinets," where one hour of connection costs up to TND 1 ($0.62). Before 2011, wireless access in cafes and restaurants was not permitted by law, which allowed only licensed ISPs to offer access to the network. Nonetheless, after the revolution it has become common for cafes and restaurants in major cities to offer free internet access without any registration requirements, attracting mainly young social network users. At the same time, the law restricting the provision of wireless internet remains on the books as of mid-2013, putting those businesses that provide wireless access at risk of violating the law if the law is later enforced by regulators.

Fixed-line internet subscribers must first buy a landline package from Tunisie Télécom, which manages the country's 82.5 Gbps bandwidth capacity, before choosing an ISP. Prices range from TND 10 (approximately $6) a month for a connection speed of 1 Mbps to TND 50 ($31) for a connection speed of 20 Mbps. On top of this cost, subscribers must also pay for a separate ISP package, ranging from 10 to 25 dinars ($6-$15). Although there are no legal limits on the data capacity that ISPs can supply, the bandwidth remains very low and connectivity is highly dependent on physical proximity to the existing infrastructure. Tunisian internet users often complain of slow internet speeds hindering their ability to upload or download certain types of content, particularly videos. In September 2012, Ookla, a broadband testing company,[14] ranked Tunisia 142nd in download speeds and 151st in upload speeds.[15] Despite these slow speeds, today Tunisian users enjoy access to various internet services and applications.

Tunisia has one of the more developed telecommunications markets in the region, with 11 ISPs supported by a nationwide fiber-optic backbone network operated by the state-controlled Tunisie Télécom.[16] There are no laws that prevent ISPs from installing their own infrastructure, but huge

[11] Tunisie Tribune, "Tunisie Télécom : de nouvelles stations pour une meilleure connexion Internet,".tunisie-tribune.com, January 15, 2013, http://www.tunisie-tribune.com/2013/01/tunisie-telecom-de-nouvelles-stations-pour-une-meilleure-connexion-internet

[12] Tunisie Numérique, "Orange ouvre les services 2G/3G à Makther, Jbel El Ouset et Bir Mcherga" [Orange launches 2G/3G services in Makther, Jbel El Ouest and Bir Mcherga], tunisienumerique.com, January 28, 2013, http://www.tunisienumerique.com/orange-ouvre-les-services-2g3g-a-makther-jbel-el-ouset-et-bir-mcherga/162605 [in French]

[13] Instance National des Télécommunications (INT), "Suivi des principaux indicateurs du marché de la téléphonie mobile en Tunisie" [Monitoring of main indicators regarding the mobile market in Tunisia], December 2012, http://www.intt.tn/upload/files/Tableau%20de%20Bord%20Mobile%20-%20D%C3%A9cembre%202012.pdf.

[14] Ookla, "About page," ookla.com, http://www.ookla.com/about

[15] Tunisie Haut Débit (thd), "6éme pays arabe à avoir le pire débit de téléchargement" [Tunisia has the 6th worst internet download speed in the Arab region], thd.tn, September 12, 2012, http://www.thd.tn/index.php?option=com_content&view=article&id=2055 [in French]

[16] Mohamed Guesmi, "Tunisie Telecom's Monopoly Over Internet Infrastructure Blamed for High Bandwidth Costs," Tunisia-live.net, June 19, 2012, http://www.tunisia-live.net/2012/06/19/tunisie-telecoms-monopoly-over-internet-infrastructure-blamed-for-high-bandwidth-costs/.

costs have prevented this so far. Nevertheless, Orange Tunisie and Tunisiana are scheduled to deploy the country's first private undersea cable in 2014.[17]

In the past, the ICT market consisted of five privately-owned ISPs: Planet Tunisie, 3S Globalnet, Hexabyte, Topnet, and Tunet. However, in recent years Topnet, Tunet, and Planet Tunisie were acquired by Tunisie Télécom,[18] Tunisiana,[19] and Orange Tunisie Internet (OTI), respectively.[20] In addition, after the fall of Ben Ali, the new government confiscated 25 percent of Tunisiana shares previously owned by Ben Ali's son-in-law, Sakher El Materi. In early January 2013, 15 percent of this stake was sold to Qtel,[21] raising the Qatari group's shares in Tunisiana to 90 percent. Tunisia's interim authorities also seized a 51 percent share of Orange Tunisie that was formerly held by another son-in-law of Ben Ali, Marwan Ben Mabrouk.[22]

The Ministry of Communication Technologies is the main government body responsible for the ICT sector. Under Article 7 of the Telecommunications Decree and Article 5 of the Telecommunication Code, ISPs must obtain a license from the Ministry of Communication Technologies in order to deliver internet services.[23] The National Instance of Telecommunication (INT) is the regulator for all telecom and internet-related activities and has the responsibility of resolving technical issues and disputes between actors. The INT governance body and its president are made up of mainly government officials nominated by the ICT Minister, which activists argue leads to a lack of regulatory independence. Nevertheless, the INT has initiated some positive changes in internet policy, namely through the introduction of a more liberal domain name chart and the invitation, sent to independent arbitrators from civil society, to develop a new Alternative Domain Name Dispute Resolution Process.[24]

Internet policy is decided by the INT and executed by the Tunisian Internet Agency (ATI), a state agency governed by a board of trustees comprised of representatives from the main shareholder, Tunisie Télécom**.** The latter controls 37 percent of ATI shares and the state owns a further 18 percent, while the remaining 45 percent is divided among private banks.[25] Under the agency's new

---

[17] ITU, "Orange, Tunisiana, Interoute plan new undersea cable (Tunisia)," itu.int, May 23, 2013, http://www.itu.int/ITU-D/ict/newslog/Orange+Tunisiana+Interoute+Plan+New+Undersea+Cable+Tunisia.aspx

18 Imen, "Tunisia: 'Tunisia Telecom' Acquires 'Topnet'," AllAfrica.com, June 15, 2010, http://allafrica.com/stories/201006170303.html.

[19] "Tunisiana takes over Tunet," TMTFinance, September 15, 2011, http://tmtfinance.com/news/tunisiana-takes-over-tunet.

[20] Web Manager Center, "Planet laisse la place à OTI (Orange Tunisie Internet)" [Planet gives way to OTI (Orange Tunisie Internet)] ; webmanagercenter.com, May 17, 2011, http://www.webmanagercenter.com/actualite/technologie/2011/05/17/105968/planet-laisse-la-place-a-oti-orange-tunisie-internet

[21] "Tunisia: Qtel pockets 15% stake in capital of Tunisiana," Africanmanager.com January, 2012 http://www.africanmanager.com/site_eng/detail_article.php?art_id=19474

[22] "Tunisia seized Ben Ali family Orange Tunisie stake," Reuters, March 31, 2011, http://in.reuters.com/article/2011/03/31/idINIndia-56028120110331?feedType=RSS&feedName=technologyNews

23 "Tunisia: Background paper on Internet regulation," Article 19, legal analysis, March 2011, http://www.article19.org/data/files/medialibrary/3014/12-04-03-ANAL-ICT-tunisia.pdf.

24 "Appel a manifestation d'intérêt pour la sélection d'arbitres pour la résolution des litiges relatifs aux noms de domaines," Instance Nationale des Télécommunications, République Tunisienne, May 24, 2012, http://www.intt.tn/fr/index.php?actu=392&typeactu=89 [in French].

[25] Kapitalis: "Tunisie : L'Etat met fin au monopole de l'ATI" [Tunisia : the State puts an end to ATI's monopoly over the internet], kapitalis.com, January 10 , 2013 http://www.kapitalis.com/economie/13829-tunisie-l-etat-met-fin-au-monopole-de-l-ati.html

chairman and CEO, Moez Chakcouk, the ATI has taken steps to become a more transparent and accountable body and, most significantly, no longer practices filtering. Indeed, the ATI won an award for "best public institution in Tunisia" as presented by OpenGovTN, a civil society group seeking to promote transparency and open government in the country.[26]

Among its responsibilities, the ATI now manages the internet exchange point (IXP) between national ISPs that buy connectivity from Tunisie Télécom, the allocation of internet protocol (IP) addresses, and together with the INT, the ".tn" country domain.[27] The agency provides direct internet access to public institutions. Under the former regime, all ISPs were obliged to route their traffic via the ATI to facilitate internet filtering and surveillance. As of early 2013, however, a decision by the ICT Ministry to amend regulatory provisions resulted in Tunisiana and Orange Tunisie now being able to bypass the ATI for incoming and outgoing international internet traffic.[28]

Amendments to the 2011 Telecommunication Code, passed in early April 2013,[29] improved the legal and regulatory environment for ICTs.[30] The amended law has, for instance, put an end to the legal vacuum under which virtual mobile networks and ISPs had to operate. The text further defines an IXP as "an exchange point of national internet traffic, which also manages international traffic." The definition of an IXP did not exist in the law before. However, no amendments were proposed to Articles 14 and 30, which oblige telecom operators to make a list of their subscribers available to the public.

LIMITS ON CONTENT

Censorship has drastically reduced since the overthrow of the Ben Ali regime, which employed one of most repressive internet censorship apparatuses in the world. Over the past year, there was no evidence of politically-motivated filtering. Popular social media tools such as Facebook, YouTube, Twitter, and international blog-hosting services are freely available in the country. Crucially, the judiciary did not issued any further verdicts in favor of blocking, despite dozens of complaints lodged against the ATI to filter "defamatory" Facebook pages.[31]

Indeed, since the revolution, the judiciary has quickly found itself at the center of many censorship debates, in great deal due to its role of enforcing many of the country's not-yet-reformed laws. For

[26] Maghreb Emergent, "Tunisie - Remise des trophées « OpenGovTn Awards 2012" [Tunisia : « OpenGovTN Awards 2012 » awards ceremony], maghrebemergent.info, January 27, 2013, http://www.maghrebemergent.info/actualite/fil-maghreb/20508-tunisie-remise-des-trophees-l-opengovtn-awards-2012-r.html [in French]
[27] Agence Tunisienne d'Internet, "TunIXP : the 1st Internet exchange in the Maghreb Arab Region," ati.tn, accessed January 31, 2013, http://www.ati.tn/TunIXP
[28] Telecompaper, "Operators can bypass ATI for international internet traffic," telecompaper.com, January 14, 2013, http://www.telecompaper.com/news/operators-can-bypass-ati-for-international-internet-traffic--918597
[29] Tunisie Haut Débit, "Après un débat houleux sur l'ATI, la Constituante adopte le nouveau code des telecoms" [The Consituent Assembly adopts the new telecommunications code, following a heated debated about the ATI], thd.tn, April 4, 2013, http://thd.tn/index.php?option=com_content&view=article&id=3263:apres-un-debat-houleux-sur-l-ati-la-constituante-adopte-le-nouveau-code-des-telecoms&catid=56&Itemid=50
[30] http://www.intt.tn/upload/txts/ar/loi-01-2001-ar.pdf
[31] Index on Censorship, "The internet is freedom: Index speaks to Tunisian Internet Agency chief," indexoncensorship.org, February 3, 2012, http://www.indexoncensorship.org/2012/02/tunisia-internet-moez-chakchouk

example, in May 2011, the Tunis Permanent Military Tribunal ordered the blocking of five Facebook pages on charges of defamation against the military and its leaders.[32] The ATI could only implement the verdict for a short period of time, citing "technical issues" that occurred as a result of a 15 GB increase in internet traffic and a breakdown of filtering machinery.[33] That same month, a Tunis-based primary court ordered filtering of X-rated content based on a complaint lodged by three lawyers, who argued that the sites were a threat to minors and the country's Muslim values.[34] After the ATI lost an appeal, the verdict was eventually overturned by Tunisia's highest appeal court, the Cassation Court, in February 2012 on the grounds that the ATI lacked the technical capacity to implement the mandated filtering.[35] Explaining the reasoning behind the ATI's move to appeal the court verdicts, ATI president Moez Chakchouk stated, "This is not about pornography; it's a matter of principle. In post-revolutionary Tunisia, we are determined to break with the former regime's censorship practices." Interestingly, although the ATI was obliged to practice filtering during the former regime, there is no law that formally requires this filtering.[36]

Although the government no longer advocates censorship, several laws from the Ben Ali era continue to pose a significant threat to internet freedom, even if they are sporadically enforced. Under Article 1 of the 1997 Telecommunications Decree, [37] ISPs remain legally liable for third-party content. Furthermore, Article 9 of the 1997 Internet Regulations[38] requires ISPs to actively monitor and take down objectionable online content.[39] Laws continue to allow the government to censor internet content that is deemed obscene or threatening to public order, or is defined as "incitement to hate, violence, terrorism, and all forms of discrimination and bigoted behavior that violate the integrity and dignity of the human person, or are prejudicial to children and adolescents."[40] In the absence of any judiciary action, these provisions have not led to any major issues over the coverage period.

Although the pervasive environment of self-censorship dissipated rapidly with the fall of Ben Ali, some online activists avoid crossing "red lines" over fears that Ammar404 could be reinstated. [41] For instance, political cartoonist "_Z_" still prefers to stay anonymous because he fears that the

32 "Tunisie – Le tribunal militaire ordonne la censure de quatre pages sur Facebook" [Tunisia – The military court ordered the censorship of four pages on Facebook], Business News, May 11, 2011, http://www.businessnews.com.tn/Tunisie---Le-tribunal-militaire-ordonne-la-censure-de-quatre-pages-surFacebook,520,24752,1.

[33] Index on Censorship, "The internet is freedom: Index speaks to Tunisian Internet Agency chief," indexoncensorship.org, February 3, 2012, http://www.indexoncensorship.org/2012/02/tunisia-internet-moez-chakchouk

34 "Tunis court upholds order requiring filtering of porn sites," Reporters without Borders, August 16, 2011, http://en.rsf.org/tunisia-court-to-take-crucial-decision-for-01-07-2011,40566.html.

35 Global Voices Online, "Tunisia: Court Quashes Verdict Ordering the Filtering of Pornography," globalvoicesonline.org, February 22, 2012, http://globalvoicesonline.org/2012/02/22/tunisia-court-quashes-verdict-ordering-the-filtering-of-pornography

[36] Index on Censorship Magazine, "On the Ground : Moez Chakchouk on Tunisia," [Volume 41 Number 4 2012], December 2012, http://ioc.sagepub.com/content/41/4/60.extract

[37] Available in Arabic at: http://www.mincom.tn/fileadmin/templates/PDF/juridiques/D1997-0501_ar.pdf

[38] Available in Arabic at: http://www.mincom.tn/fileadmin/templates/PDF/juridiques/A22-03-1997_ar.pdf

39 "Tunisia: Background paper on Internet regulation," Article 19, legal analysis, March 2011.

[40] Letter from Chargé d'Affairs Dridi to Human Rights Watch, as cited in "False Freedom: Online Censorship in the Middle East and North Africa," Human Rights Watch, 2005, available at http://bit.ly/12lmFoc.

[41] IT News Africa, "Tunisia Deletes Internet Censorship Policies," itnewsafrica.com, accessed January 30, 2013, http://www.itnewsafrica.com/2012/09/tunisia-deletes-internet-censorship-policies

surveillance equipment "could still be in place today, waiting for a reactivation signal."[42] Similarly, on June 10, 2012, the organizers of the contemporary art fair "Printemps des Arts" temporarily shut down the exposition's website after ultra-conservative protesters attacked the fair's closing ceremony for exhibiting "blasphemous" artwork.[43] Still, users are more open to discussing religion, the army, and other sensitive issues on the web compared to traditional media platforms. For instance, while traditional media remained silent regarding the case of Jabeur Mejri, who received a seven-and-half year prison sentence for publishing cartoons of the prophet Muhammad on Facebook, it was covered extensively by online media outlets (for more on Mejri's case, please see "Violations of User Rights).

Since the revolution, numerous online sources of information have been launched alongside new newspapers, radio stations, and television channels, enriching the information landscape through the addition of viewpoints from a diverse range of social actors. This has been helped by the fact that there are few restrictions when it comes to online advertising or foreign investment. The abundance of online news sources has led to some cases in which partisan interests have manipulated information. There is strong suspicion that Ennahda, the ruling Islamist party, maintains a digital army of young activists and bloggers tasked with managing Facebook communities and disseminating partisan content as part of an "info war." The Ennahda apparatus was particularly active during the party's ninth congress, which took place in July 2012.[44] Nevertheless, the unprecedented openness of the Tunisian internet sphere in the post-Ben Ali era has greatly diluted the influence of such content, and there have been positive online initiatives to counter rumors that have the potential to spark riots. For instance, the Tunisian Association for Digital Liberties (ATLN) created ch9alek.org, a crowd-sourcing platform to combat rumors spread online.[45]

Tunisian youth and civil society organizations have continued to use digital media for initiatives relating to political and social issues. In April 2013, the anti-corruption organization I Watch launched Billkamcha.com, a crowd-sourced map that permits netizens to report on corruption cases.[46] In another case, the civil society organization al-Bawsala continues to track the National Constituent Assembly's progress in drafting the constitution for the second consecutive year. The group live-tweets the assembly's sessions and publishes law projects and voting records on the platform Marsad.tn.[47]

---

[42] Global Voices Online, "Tunisian Political Cartoonist _Z_: 'Nothing Has Really Changed'," globalvoicesonline.org, August 26, 2012, http://globalvoicesonline.org/2012/08/26/tunisia-nothing-has-really-changed-says-anonymous-political-cartoonist-_z_

[43] Le Journal des Arts, "Emeutes en Tunisie : les artistes dénoncent une « vaste manipulation »" [riots in Tunisia : artists condemn « an extensive manipulation campaign »], lejournaldesarts.fr, June 20, 2012, http://www.lejournaldesarts.fr/site/archives/docs_article/101360/emeutes-en-tunisie--les-artistes-denoncent-une---vaste-manipulation--.php [in French]. The exhibition's website is http://www.marsa-arts.com.

[44] Nawaat, "9éme congrès d'Ennahdha : Quand le show prend le dessus sur le fond," nawaat.org, July 20, 2012, http://nawaat.org/portail/2012/07/20/9eme-congres-dennahdha-quand-le-show-prend-le-dessus-sur-le-fond

[45] http://www.ch9alek.org/

[46] Nuqudy, "Anti-Corruption Website Launched in Tunisia", english.nuqudy.com, April 25, 2013, http://english.nuqudy.com/North_Africa/Anti-Corruption_Web-5356

[47] http://www.marsad.tn/

In May 2012, the collective blog Nawaat launched a campaign to criticize the military after an army general confiscated two cameras belonging to Ramzi Bettibi, an investigative journalist working for the blog. Bettibi was covering a military court hearing regarding protesters killed during the revolution. Nawaat criticized the military's lack of transparency and the slow pace of the investigation. The blog also reported that some army units might have been involved in the repression of protesters during the uprising, signaling a strong willingness to take on this powerful institution in Tunisian society.[48]

VIOLATIONS OF USER RIGHTS

While Tunisia has taken significant steps to promote internet access and halt online censorship, the country's legal framework remains a significant threat to internet freedom. Delays in drafting a new constitution and establishing a new legal framework based on international norms continue to hold Tunisia back. Under laws from the Ben Ali era, the judiciary has continued to prosecute users over online expression.

The National Constituent Assembly (NCA), elected in October 2011, is scheduled to adopt a new constitution over the summer of 2013. According to a draft released in April 2013, free speech is protected and "prior censorship" is prohibited. However, there is no explicit mention of the right to access the internet, despite numerous calls from activists and organizations.[49] Following negotiations with its coalition partners, Ennahda agreed to drop a clause criminalizing blasphemy in the constitution.[50] Concerns remain, however, over the possible insertion of clauses relating to the protection of religion or "the sacred." If adopted, such a clause could act as a constitutional restriction to freedom on the internet, where religious issues are currently debated more openly than in the mainstream media or on the streets.

In a move that consolidated freedom of expression online, the Tunisian government finally moved to implement Decree-law 115 on Press, Printing and Publishing of 2011,[51] following a nationwide strike by journalists in October 2012.[52] The law recognizes web journalists as "professional journalists" and entitles them to the same rights and legal protections granted to print and broadcast journalists.[53] When it comes to libel, the law abolished prison sentences for criminal defamation,

[48] Global Voices Online, "Tunisia: Protesting the Military's Lack of Transparency and Censorship," globalvoicesonline.org, June 2, 2012 http://globalvoicesonline.org/2012/06/02/tunisia-protesting-the-militarys-lack-of-transparency-and-censorship/
[49] Article 19, "Tunisia: Let's work together to formulate the Constitution," article19.org, April 4, 2012, http://www.article19.org/resources.php/resource/3017/en/tunisia:-let's-work-together-to-formulate-the-constitution
[50] The Telegraph, "Tunisia plans to outlaw blasphemy dropped," telegraph.co.uk, October 12, 2012, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/tunisia/9605965/Tunisia-plans-to-outlaw-blasphemy-dropped.html
[51] http://www.inric.tn/D%C3%A9cret-loi2011_115Arabe.pdf
[52] France 24, "Tunisian journalists strike over press freedom", france24.com, October 17, 2012, http://www.france24.com/en/20121017-tunisian-journalists-strike-over-threats-press-freedom-islamist-led-government
[53] Reporters Without Borders, "Analysis of Law No. 2011-115 dated 2 November 2011, relating to freedom of the press, printing and publication," en.rsf.org, February 14, 2012, http://en.rsf.org/IMG/pdf/120214_observations_rsf_code_de_la_presse_gb_-_neooffice_writer.pdf

places the burden of proof on the plaintiff, and excludes "statements of public interest."[54] However, journalists and free speech advocates have criticized the implementation of the decree as incomplete. In some cases, such as that of Olfa Riahi discussed below, judges and prosecutors have ignored decree 115 and instead used the 1975 press law and provisions of the penal code to prosecute bloggers and online journalists lacking formal press qualifications.

The repressive laws of the Ben Ali regime still remain the greatest threat to internet freedom. For example, Article 86 of the Telecommunications Code states that anyone found guilty of "using public communication networks to insult or disturb others" could spend up to two years in prison and may be liable to pay a fine. Articles 128 and 245 of the penal code also punish slander with two to five years imprisonment.[55] In addition, there has been no push on the part of the authorities to hold former regime members accountable for widespread offenses committed during the Ben Ali era.[56] While censorship is no longer a significant issue, these laws continued to be employed to prosecute internet users throughout late 2012 and early 2013.

In the gravest violation of user rights over the past year, on April 25, 2013, the Court of Cassation upheld Jabeur Mejri's seven and half year prison sentence for publishing cartoons depicting the prophet Mohammad on his Facebook page. He was convicted of "insulting others through public communication networks" under Article 86 of the Telecommunications Code through a post deemed as offensive to Islam and "liable to cause harm to public order or public morals" under Article 121 (3) of the Tunisian Penal Code.[57] Having previously lost another appeal in June 2012,[58] Mejri's defense team will now seek a presidential pardon for their client. Ghazi Beji, a friend of Mejri, was also sentenced after publishing an essay that satirized the Prophet Muhammad's biography on Scribd.com, a free social publishing website, in July 2011. Beji, however, was convicted in absentia since he has since fled the country.[59]

In another disturbing case, in early January 2013, an investigative judge imposed a travel ban on blogger Olfa Riahi over a blog post she published in December 2012. In the post, Riahi claimed that then-foreign minister Rafik Abdessalam misused public money by spending several nights at the luxurious Sheraton hotel in downtown Tunis and implied that he might have been involved in an extra-marital affair. On March 9, 2013, a judge lifted the travel ban. Since Riahi has not benefitted from traditional protections allotted to journalists, the blogger still faces fines and up to five years

[54] "Tunisia: Press, Printing, and Publication Code – Legal Analysis," Article 19, November 2011, available at http://bit.ly/13Eova5.
[55] "Code Penal," Juriste Tunisie, 2009, http://www.jurisitetunisie.com/tunisie/codes/cp/cp1225.htm.
[56] Nawaat, "Tunisia: Cyber-Activists to Sue Interior Ministry over Web Censorship," nawaat.org, August 21, 2012, http://nawaat.org/portail/2012/08/21/cyber-activists-to-sue-interior-ministry-over-web-censorship
[57] Amnesty International, "Tunisia: upholding of blogger's seven-year jail sentence for 'insulting Islam' condemned," amnesty.org.uk, April 26, 2013, http://www.amnesty.org.uk/news_details.asp?NewsID=20753
[58] Index on Censorship, "Verdict in Muhammad cartoon conviction upheld," uncut.indexoncensorship.org, June 25, 2012, http://uncut.indexoncensorship.org/2012/06/verdict-in-muhammad-cartoon-conviction-upheld
[59] Nawaat, "Interview avec Ghazi Béji, un antithéiste en fuite de la Tunisie" [Interview with Ghazi Beji, an antitheist who fled Tunisia], Nawaat.org, June 29, 2012, http://nawaat.org/portail/2012/06/29/interview-avec-ghazi-beji-un-antitheiste-en-fuite-de-la-tunisie

imprisonment[60] for criminal defamation,[61] offending others through public communication networks,[62] publishing false news that could disturb public order,[63] and violating privacy.[64]

On March 21, 2013, a Tunisian court sentenced rapper Ala Yacoubi (also known as "Weld El 15") to two years in prison in absentia over an anti-police video clip he published on YouTube.[65] In the song, Yacoubi describes police officers as "dogs" and says "he would like to slaughter a police officer instead of sheep at Eid al-Adha." Actress Sabrine Klibi, who appears in the video, and cameraman Mohamed Hedi Belgueyed both received six-month suspended jail sentences.[66] In a bid to reduce his sentence, Yacoubi turned himself in on June 13. Although the original verdict was initially confirmed, he was subsequently freed on July 4 and given a reduced six-month suspended sentence.[67]

In addition to government action, users must also be weary of extralegal attempts to silence online activists. Two days before the assassination of leftist opposition leader, Chokri Belaid, on February 6, 2013, a list of activists and politicians to be "slaughtered" was published on an extremist Facebook page. The list included names of opposition politicians, activists, and journalists, including blogger Olfa Riahi. [68] In March 2013, FEMEN activist Amina Tyler was threatened for posting topless pictures of herself on Facebook. Adel Almi, founder of Tunisia's Commission for the Promotion of Virtue and Prevention of Vice, said the young woman "deserves to be stoned to death."[69]

Laws that limit online anonymity also remain a concern in the post-Ben Ali era. In particular, Article 11 of the Telecommunications Decree prohibits ISPs from transmitting encrypted information without prior approval from the Minister of Communications. Furthermore, under Articles 8 and 9 of the Internet Regulations, ISPs are required to submit lists of their subscribers to the ATI and to retain archives of content for up to one year.[70] While there have been no reports of these laws being enforced, their continuing existence underscores the precarious nature of Tunisia's newfound and relatively open internet environment.

There were no reports of extralegal government surveillance of online activity in the post-Ben Ali period. However, the deep-packet inspection (DPI) technology once employed to monitor the

[60] Reporters Without Borders, "Sheratongate: Bloggers allegations against foreign minister land her in court," en.rsf.org, January 17, 2013, http://en.rsf.org/tunisia-sheratongate-blogger-s-allegations-17-01-2013,43926.html
[61] Under Articles 128 and 245 of the Tunisian Penal Code, this charge carries two years imprisonment.
[62] Article 86 of the Telecommunications code, up to two years imprisonment.
[63] Article 121 (3) of the penal code, up to five years imprisonment and, under the new press law, a fine of up to 5000 dinars.
[64] Law 63-2004 on the Protection of Personal Data, up to two years imprisonment.
[65] See https://www.youtube.com/watch?v=6owW_Jv5ng4
[66] Index on Censorship, "Free speech on hold in Tunisia as rapper faces jail," uncut.indexoncensorship.org, March 28, 2013, http://uncut.indexoncensorship.org/2013/03/free-speech-on-hold-in-tunisia-as-rapper-faces-jail/
[67] Bill Chappell, "Jailed Tunisian Rapper is Freed; Song Called Police 'Dogs'," NPR, July 2, 2013, http://www.npr.org/blogs/thetwo-way/2013/07/02/197997952/jailed-tunisian-rapper-is-freed-song-called-police-dogs.
[68] ARTE, "Tunisie: la liste noire des salafistes" [Tunisia: Salafists' black list], videos.arte.tv, March 17, 2013 http://videos.arte.tv/fr/videos/tunisie-la-liste-noire-des-salafistes--7395644.html
[69] The New Yorker, "How to Provoke National Unrest with a Facebook Photo," newyorker.com, April 8, 2013, http://www.newyorker.com/online/blogs/elements/2013/04/amina-tyler-topless-photos-tunisia-activism.html
[70] "Tunisia: Background paper on Internet regulation," Article 19, legal analysis, March 2011.

internet and intercept communications is still in place, sparking worries that the technology can be reinstated if desired. Confusion reigns over how surveillance is conducted in contemporary Tunisia, particularly in the absence of a new constitution and legal reforms that would protect citizens from mass surveillance. ICT minister Mongi Marzoug has, on several occasions, tried to reassure netizens that surveillance is being implemented "legally" and with court orders.[71] Tunisia's Data Protection Authority (known by its French acronym INPDP) is set to amend the country's 2004 privacy law in order to ensure the body's independence from any government interference.[72] As it stands, the law exempts public authorities from obtaining the consent of the INPDP to access and process personal data.

Since Ben Ali's fall, there have been no reported incidents of cyberattacks perpetrated by the government to silence ICT users. However, other groups have been employing these methods to intimidate activists and organizations with whom they do not agree. In October 2012, the award-winning collective blog Nawaat.org suffered distributed denial-of-service (DDoS) attacks after it leaked a private conversation between then-Prime Minister Hamadi Jebali and his predecessor, Beji Caid Sebsi.[73] On December 11, 2012, the website of Tunisia's largest labor union, the UGTT, suffered a DDoS attack. The attacks were allegedly perpetrated by a Tunisian hacking group called Fallega, believed to be a supporter of the Islamist party Ennahda, in protest of the union's vow to stage a nationwide strike.[74]

[71] African Manager, "Tunisie : L'Internet contrôlé ou censuré ?" [Tunisia : Is the internet monitored or censored ?], africanmanager.com, September 5, 2012, http://www.africanmanager.com/143050.html.
[72] Index on Censorship, '' New-era privacy law drafted to protect Tunisians from the surveillance state'', uncut.indexoncensorship.org, August 15, 2012, http://uncut.indexoncensorship.org/2012/08/tunisia-drafts-new-era-privacy-law.
[73] Global Voices Advocacy, "MENA Netizen Report: Porn Edition," advocacy.globalvoicesonline.org, November 14, 2012, http://advocacy.globalvoicesonline.org/2012/11/14/mena-netizen-report-porn-edition .
[74] Tunisie Haut Débit, "Tunisie : Le site de l'UGTT piraté, mot de passe admin divulgué" [Tunisia : UGTT website hacked, admin password disclosed], thd.tn, December 11, 2012, http://www.thd.tn/websphere/news/websphere/tunisie-le-site-de-lugtt-pirate-mot-de-passe-admin-divulgue .

TURKEY

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	12	12
Limits on Content (0-35)	17	18
Violations of User Rights (0-40)	17	19
Total (0-100)	**46**	**49**

* 0=most free, 100=least free

POPULATION: 74.9 million
INTERNET PENETRATION 2012: 45 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Turkish authorities added several thousand websites to its blocking list, increasing the total to almost 30,000 (See **LIMITS ON CONTENT**).
- Ruling in favor of a Turkish user, the European Court of Human Rights found Turkey in violation of Article 10 of the European Convention on Human Rights for blocking access to the hosting platform Google Sites (see **LIMITS ON CONTENT**).
- Several users received fines, prison time, or suspended sentences for comments made on social media, including renowned pianist Fazil Say. Say was handed a 10-month suspended sentence for insulting religious values on Twitter and will appeal. Meanwhile, a Turkish-Armenian linguist and columnist was handed a 10-month sentence on similar charges related to a blog post (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

This report covers events between May 1, 2012 and April 30, 2013. In late May 2013, what started as a relatively small and peaceful protest at Gezi Park in the Taksim district of central Istanbul rapidly snowballed into the largest anti-government protests that Turkey has seen in years. Demonstrations spread from Istanbul to Ankara, Izmir, Adana, and other cities across the country. While the original protest called for the halt of a plan to transform Gezi Park into a shopping mall, public outrage grew over the disproportionate police response in which water cannons and tear gas were used in an excessive display of force. The dramatic events exposed the complicity of mainstream Turkish media, which largely failed to report the massive anti-government protests that ensued. Instead, sites such as YouTube, Facebook, and Twitter arose as some of the few outlets for reliable coverage on the protests, leading Prime Minister Reçep Tayyip Erdoğan to describe social media as "the worst menace to society." Dozens of people were arrested for their social media posts, and criminal investigations are expected under the use of Articles 214 and 217 of the Turkish Penal Code concerning incitement to commit a crime and disobey the law. The government also hinted that it may introduce further measures to exercise greater control over social media, with ministers calling for companies to assist law enforcement agencies in identifying anonymous users so that they may be prosecuted for allegedly violating the country's laws.

INTRODUCTION

Internet and mobile telephone use in Turkey has grown significantly in recent years, though access remains a challenge in some parts of the country, particularly in the southeast. Until 2001, the government pursued a hands-off approach to internet regulation but has since taken considerable legal steps to limit access to certain information, including some political content. In February 2011, the Information and Communications Technologies Authority (BTK) announced plans to establish a countrywide mandatory filtering system with the aim of protecting citizens from so-called "harmful content," which included but was not limited to sexually-explicit content and terrorist propaganda.[1] Subsequent to strong opposition from the public, street demonstrations, and a legal challenge, the policy was made optional for subscribers.[2] Nonetheless, civil society organizations have continued to criticize the system since it became operational in November 2011, and a legal challenge is ongoing at the Council of State level.

According to Engelliweb, there were over 29,000 blocked websites as of April 2013, almost 10,000 more compared to February 2012.[3] Several domestic news websites and online streaming services, such as Last.fm and Metacafe, continue to be blocked in Turkey. Over the last three years, citizens have filed five separate applications to the European Court of Human Rights (ECHR) to challenge the government's blocking of YouTube, music streaming site Last.fm, and the webpage

[1] Decision No. 2011/DK-10/91 of Bilgi Teknolojileri ve İletişim Kurumu, dated February 22, 2011.
[2] Yesim Comert, "Marchers protest new Turkish Web filtering rule," CNN, May 15, 2011, http://edition.cnn.com/2011/WORLD/meast/05/15/turkey.internet.protest/index.html.
[3] Engelliweb.com is a website that documents information about blocked websites from Turkey. Site accessed April 30, 2013,

creation tool Google Sites, after appeals before the local courts were rejected.[4] YouTube was unblocked in 2010. In December 2012, ruling in the case of *Ahmet Yildirim v. Turkey*,[5] the ECHR unanimously held that there had been a violation of Article 10 of the European Convention of Human Rights in the case of the Turkish court's blocking of the hosting platform Google Sites.[6] The verdict, however, did not result in any shift in government policy related to the problematic Law No. 5651, used often to block websites. In its 2012 Progress Report for Turkey's Accession to the European Union (EU), the European Commission stated that "frequent website bans are a cause for serious concern and there is a need to revise the law on the internet."[7]

Over the past year, several social media users were prosecuted on charges related to terrorism, blasphemy, obscene content, and criticism of the state or its officials. In the most widely-covered case, the pianist and composer Fazil Say was given a suspended sentence of 10 months imprisonment for insulting religious values in a series of tweets he had posted to Twitter. A linguist and former columnist was handed 13 months for a similar offense related to a blog entry he had written on the offensive "Innocence of Muslims" video. Finally, a user was sentenced to nine years and seven months imprisonment for allegedly disseminating terrorist propaganda over Facebook. Many others received suspended sentences and fines.

OBSTACLES TO ACCESS

Despite an increasing penetration rate in the last few years, obstacles to internet access in Turkey remain. According to the International Telecommunication Union (ITU), internet penetration stood at 45 percent in 2012, up from 29 percent in 2007.[8] Total broadband subscriptions stood at over 20 million at the end of 2012, of which over 10 million were mobile broadband subscriptions.[9] In total, mobile penetration was at 91 percent in 2012 and all mobile phone operators offer third-generation (3G) data connections.[10]

Most users access the internet from workplaces, universities, and internet cafes. Poor infrastructure and a lack of electricity in certain areas, especially in the eastern and southeastern regions, have had a detrimental effect on citizens' ability to connect to the internet, particularly from home. While prices have decreased, they do remain high. Bandwidth capping has become standard practice and a part of the broadband services offered by major providers since 2011. A lack of technical literacy, particularly among older Turks, also inhibits wider internet use.

---

[4] The YouTube block was lifted in November 2010 only after disputed videos were made inaccessible from the country.
[5] Application no.3111/10.
[6] See further Turkish block on Google site breached Article 10 rights, rules Strasbourg at http://ukhumanrightsblog.com/2013/01/16/turkish-block-on-google-site-breached-article-10-rights-rules-strasbourg/
[7] European Commission, Turkey: 2012 Progress Report, COM(2012) 600, Brussels, 10.10.2012 SWD(2012) 336
[8] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2007 & 2012, accessed July 11, 2013, http://bit.ly/14IIykM.
[9] "Electronic Communications Market in Turkey – Market Data (2012 Q4)," Information and Communication Technologies Authority, March 15 2013, Slide 30, accessed July 11, 2013, http://eng.btk.gov.tr/dosyalar/2012-4-English_15_03_2013.pdf.
[10] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

There are around 150 internet service providers (ISPs) in Turkey, though the majority act as resellers for the dominant, partly state-owned Turk Telekom, which provides more than 81 percent of broadband access in the country through its subsidiary TTNET.[11] Turkcell is the leading mobile phone provider, with 51.9 percent of subscribers, followed by Vodafone and Avea.[12] Overall, delays in the liberalization of local telephony continue to undermine competition in the fixed-line and broadband markets. ISPs are required by law to submit an application for an "activity certificate" from the Telecommunications Communication Presidency (TIB), a regulatory body, before they can offer services. Internet cafes are also subject to regulation. Those operating without an activity certificate from a local municipality may face fines of TRY 3,000 to 15,000 ($1,900 to $9,600). Mobile phone service providers are subject to licensing through the Information and Communications Technologies Authority (BTK).

The Computer Center of Middle East Technical University has been responsible for managing domain names since 1991. Furthermore, the Information and Communication Technologies Authority (BTK) oversees and establishes the domain name operation policy and its bylaws. Unlike in many other countries, individuals in Turkey are not permitted to register and own ".com.tr" and ".org.tr" domain names unless they own a company or civil society organization with the same name as the requested domain. A new set of rules on domain names registration was published in the Official Gazette on November 7, 2010.

The BTK and the TIB, which it oversees, act as the regulators for ICTs and are well staffed and self-financed.[13] However, the fact that board members are government appointees is a potential threat to the authority's independence, and its decision-making process is not transparent. Nonetheless, there have been no reported instances of certificates or licenses being denied. The TIB also oversees the application of the country's website blocking law and is often criticized by pressure groups for a lack of transparency.

LIMITS ON CONTENT

Government censorship of the internet is relatively common and has increased steadily over recent years. Blocking orders related to intellectual property infringement continued in 2012 and in early 2013, particularly for file-sharing and streaming websites. In total, another several thousand websites were blocked over the past 12 months alone, including many sites that were blocked for political or social reasons. The prosecution of users for online posts has had a chilling effect on self-censorship, which remains extensive in online media as in traditional media. Finally, it is becoming increasingly difficult to find alternative sources of information, particularly related to LGBT and minority issues.

YouTube, Facebook, Twitter, and international blog-hosting services are freely available, although the government has routinely blocked access to these and other social media sites in the past.

[11] "Electronic Communications Market in Turkey – Market Data (2012 Q4)," Slide 32. Figures do not include cable internet.
[12] "Electronic Communications Market in Turkey – Market Data (2012 Q4)," Slide 38.
[13] Information and Communication Technologies Authority, http://www.tk.gov.tr/Eng/english.htm.

Currently, access to the following services is blocked: Last.fm, Metacafe, Dailymotion, Google groups, and the photo-sharing website Slide. Access to the popular digital documents sharing website Scribd was also blocked in March 2013 by an Istanbul Court.[14] In most instances, large-scale shutdowns of these websites have been blunt efforts to halt the circulation of specific content that is deemed undesirable or illegal by the government. YouTube, for example, was intermittently blocked multiple times in recent years to prevent users from accessing videos critical of Turkey's founding father Mustafa Kemal Ataturk, although it has remained accessible since October 2010. Since October 2012, YouTube operates in the country under a local "com.tr" domain which, the authorities claim, makes it easier for them to ask Google to remove objectionable content.[15]

The responsibilities of content providers, hosting companies, mass-use providers, and ISPs are delineated in Law No. 5651, enacted in May 2007 and titled "Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication."[16] The law's most important provision calls for the blocking of websites that contain certain types of content, including material that shows or promotes the sexual exploitation and abuse of children, obscenity, prostitution, or gambling. Also targeted for blocking are websites deemed to insult Mustafa Kemal Ataturk, the founding father of modern Turkey. Domestically hosted websites with proscribed content can be taken down, while websites based abroad can be blocked and filtered through ISPs. In April 2011, the TIB sent a letter to hosting companies based in Turkey with a list of 138 potentially provocative words that may not be used in domain names and websites.[17] This raised strong national and international criticism, to which the TIB responded that the list of words was intended to help hosting companies identify and remove allegedly illegal web content.[18] According to Engelliweb.com, there were over 29,000 blocked websites as of May 2013.[19]

Although Law No. 5651 was designed to protect children from illegal and harmful internet content, its broad application to date has effectively restricted adults' access to some legal content. In some instances, the courts have also made politically motivated judgments to block websites using other laws. For example, the courts have indefinitely blocked access to the websites of several alternative news sources that report news on southeastern Turkey and Kurdish issues, such as Atilim, Özgür Gündem, Azadiya Welat, Keditör, Günlük Gazetesi, and Firat News Agency. Access to the website of Richard Dawkins, a British etiologist, evolutionary biologist and popular science writer, was blocked in September 2008 after a pro-creationist Islamist claimed that the website

[14] Istanbul 12th Criminal Court of Peace, Decision No 2013/209 D., 08.03.2013.
[15] See further Reuters, "YouTube opens Turkish site, giving government more control," 02 October, 2012 at http://www.reuters.com/article/2012/10/02/net-us-turkey-youtube-idUSBRE8910T420121002
[16] Law No 5651 was published on the Turkish Official Gazette on 23.05.2007, No. 26030. A copy of the law can be found (in Turkish) at http://www.wipo.int/wipolex/en/details.jsp?id=11035.
[17] Several "controversial words" appeared on the list of "banned words" including: *Adrianne* (no one knows who she is), *Haydar* (no one knows who he is), *aayvan* (animal), *baldiz* (sister-in-law), b*uyutucu* (enlarger), *ciplak* (nude), *citir* (crispy), e*tek* (skirt), free, girl, *ateşli* (passionate), *frikik* (freekick), gay, *gizli* (confidential), *gogus* (breast), *hikaye* (story), homemade, hot, *İtiraf* (confession), *liseli* (high school student), *nefes* (breath), partner, *sarisin* (blond), *sicak* (hot), *sisman* (overweight), *yasak* (forbidden), y*erli* (local), *yetiskin* (adult), and so on.
[18] Ekin Karaca, "138 Words Banned from the Internet," Bianet, April 29, 2011, http://www.bianet.org/english/freedom-of-expression/129626-138-words-banned-from-the-internet; See also, Erisa Dautaj Senerdem, "TIB's 'forbidden words list' inconsistent with law, say Turkish web providers," Hurriyet Daily News, April 29, 2011, http://www.hurriyetdailynews.com/n.php?n=tibs-forbidden-words-list-inconsistent-with-law-2011-04-29.
[19] Engelliweb.com is a website that documents information about blocked websites from Turkey. Accessed May 8, 2013.

contents had insulted him, his work, and his religion. An Istanbul Court later lifted the blocking order and rejected the defamation claims in July 2011. As of January 2013, the case is on appeal at the Court of Appeal, but the website is currently accessible from Turkey.[20]

Access to several Redhack-related websites has also been blocked over the past year.[21] The Marxist-Socialist group is known for conducting cyberattacks on government websites in order to obtain and release sensitive and damaging information. In July 2012, there were also calls by the Ministry of Foreign Affairs to block access to the cloud-storage service Dropbox, which Redhack had used for disclosing the identities of hundreds of Turkish bureaucrats and diplomats working outside Turkey.[22]

In the past, there have been attempts to block websites that allegedly defame individuals. On September 28, 2010, the Ankara Third Criminal Court of Peace ordered the blocking of BugunKilicdaroglu.com, a website that assesses the policies and strategies of Kemal Kılıçdaroğlu, the leader of the Republican People's Party (CHP), Turkey's main opposition party. The injunction to block access to the website was requested by Mr. Kılıçdaroğlu's lawyers for reasons of defamation. The Ankara 11th Criminal Court of First Instance overturned the blocking decision in January 2011.[23]

Despite the fact that it is not illegal, sexually-explicit content is often blocked by the authorities under the guise of protecting minors. Access to 5Posta.org, a Turkish-language website which features writings of a sexual nature, was blocked by two different decisions, and an appeal is ongoing.[24] Similarly, as of early 2013, an appeal is ongoing at the Council of State level with regards to the blocking of Playboy.com in Turkey. The user-based appeal was lodged by two university professors.

The Turkish government has come under criticism from a number of European bodies for its blocking practices. Thomas Hammarberg, the Council of Europe's Commissioner for Human Rights, stressed the need to review Law No. 5651 to align the grounds for restricting access to a website with those accepted in the case law of the European Court of Human Rights.[25] Similarly, the European Commission, in its 2012 Progress Report for Turkey's Accession to the European Union, stated that "frequent website bans are a cause for serious concern and there is a need to revise the law on the internet."[26]

---

[20] "RD.net no longer banned in Turkey!" The Richard Dawkins Foundation, July 8, 2011, http://richarddawkins.net/articles/642074-rd-net-no-longer-banned-in-turkey.

[21] Note the decision of the Ankara High Criminal Court No. 11, decision no 2012/1039 with regards to kizilhack.org, redhack.deviantart.com, redhackers.org and kizilhack.blogspot.com.

[22] See http://bit.ly/R2s4NO.

[23] Yaman Akdeniz, "Fighting Political Internet Censorship in Turkey: One Site Won back, 10,000 To Go," Index on Censorship, March 4, 2011, http://bit.ly/dSxV9Z.

[24] Ankara 8th Administrative Court Decision No 2010/3103, dated 18 October 2012; Ankara 6th Criminal Court of Peace Decision No 2011/94 dated 24 January 2011.

[25] Thomas Hammarberg, "Freedom of Expression and Media Freedom in Turkey," Council of Europe, July 12, 2011, https://wcd.coe.int/ViewDoc.jsp?id=1814085.

[26] European Commission, Turkey: 2012 Progress Report, COM(2012) 600, Brussels, 10.10.2012 SWD(2012) 336

Five separate applications were made to the European Court of Human Rights (ECHR) between April 2010 and January 2011, after Turkish courts denied appeal to several cases regarding the blocking of YouTube, Google Sites, and Last.fm. In February 2011, the ECHR published the statement of facts for the appeals applications involving Google Sites and Last.fm and asked the government of Turkey to respond to a number of questions by June 2011.[27] The application related to Last.fm has yet to be decided and the YouTube applications are yet to be processed by the European court.

In December 2012, the ECHR published its decision in the case of *Ahmet Yildirim v. Turkey* concerning a criminal court's decision in Denizli, a city in southwestern Turkey, to block access to a webpage hosted by Google Sites for allegedly insulting the memory of Atatürk. Yildirim was the owner of a separate website hosted by Google Sites and, after the entire hosting platform was blocked, complained access had been restricted to his own site as an unwanted consequence. The European Court of Human Rights, finding a violation of Article 10 of the European Convention on Human Rights, held that a restriction on access to a source of information is only compatible with the Convention if a strict legal framework is in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses.[28] The ECHR ruled that by preventing access to information and preventing the means of disseminating it, the Turkish court's decision had infringed upon the right to free speech. Furthermore, the ECHR stated that local courts should have had regard for the fact that such a broad blocking measure would render large amounts of information inaccessible, thus directly affecting the rights of other internet users. After the government did not appeal, the verdict became final in March 2013. Despite this, Google Sites remains blocked within Turkey. A decision by the European Court on the Turkish government's blocking of Last.fm is expected later in 2013.

In an attempt to further increase control over the internet in Turkey, the BTK announced in February 2011 a decision to implement a mandatory countrywide filtering system with the aim of protecting families from harmful content online, such as pornography.[29] In response, the IPS Communication Foundation, which owns the alternative media website Bianet, initiated a legal challenge against the BTK in April 2011 at the Council of State, the highest administrative court in Turkey.[30] The pressure of legal action against the proposal eventually led the BTK to modify the policy in August 2011, annulling the original decision and making the adoption of the filtering system optional instead of compulsory.

---

[27] Application No. 3111/10 by Ahmet YILDIRIM against Turkey (Google Sites) introduced January 12, 2010 and Application No. 20877/10 by Yaman Akdeniz against Turkey (Last.fm) introduced April 6, 2010. Assessment of these two cases is currently ongoing as of early 2012.

[28] "Restriction of Internet access without strict legal framework amounts to violation of freedom of expression," Council of Europe, December 18, 2012, http://hub.coe.int/en/web/coe-portal/press/newsroom?p_p_id=newsroom&_newsroom_articleId=1288039&_newsroom_groupId=10226&_newsroom_tabs=newsroom-topnews&pager.offset=0.

[29] Decision No. 2011/DK-10/91 of Bilgi Teknolojileri ve İletişim Kurumu, dated February 22, 2011.

[30] On September 27, 2011, the Council of State rejected the "stay of execution" request by Bianet referring to the annulment of the February 22, 2011. The case between Bianet and BTK is currently on-going as of early 2012.

Under the new rules, ISPs are compelled to offer two filtering profiles to subscribers, the "child" and "family" options. However, the filtering criteria have been criticized as arbitrary and discriminatory.[31] For example, the child filter blocks access to several websites advocating the theory of evolution as well as the website of Richard Dawkins,[32] while some anti-evolution websites remain accessible through the same filter.[33] The filter also blocks access to Facebook and the online video-sharing website YouTube, in addition to *Yasam Radyo* (Radio Life) and the Armenian minorities' newspaper *Agos*.[34] While no detailed information is provided on the filtering process or criteria, the BTK claimed in November 2012 that over one million home subscribers were using its voluntary filtering system.[35]

On November 4, 2011, a legal challenge was launched by *Alternatif Bilişim Derneği* (the Alternative Information Technologies Association), which asked the Council of State to annul the modified BTK filtering policy on the grounds that it lacked legal basis. The Association further argued that the BTK system discourages diversity by imposing a single type of family and moral values. The case continued at the Council of State level during 2012 and a decision is expected during 2013.

During 2012, in response to a number of parliamentary written questions, the Ministry of Education acknowledged that it uses the Fortiguard web filtering software at primary education institutions. The Ministry also received public criticism for blocking access to a number of minority news websites in January 2012.[36] Furthermore, in December 2012, the administrators of the Turkish parliament rejected claims from members of parliament (MPs) that, within the parliament, access to websites pertaining to the Alevi Islamic minority was blocked. In an earlier written response dated February 27, 2012 to MP Ibrahim Binici, officials from the parliament admitted that internet access from the parliament was filtered and that access to gambling, pornographic, gaming, and terrorist websites is blocked.[37]

In addition to widespread filtering, state authorities are proactive in requesting the deletion or removal of content online. Google's Transparency Report revealed that the number of content removal requests the company received from Turkey between January and June 2012 increased by 1,013 percent compared to the previous six-month reporting period.[38] In relation to YouTube,

---

[31] "New Internet Filtering System Condemned as Backdoor Censorship," Reporters Without Borders, December 2, 2011, http://en.rsf.org/turquie-new-internet-filtering-system-02-12-2011,41498.html.
[32] Dorian Jones, "Turkey Blocks Web Pages Touting Darwin's Evolution Theory," Voice of America, December 23, 2011, http://www.voanews.com/english/news/europe/Turkey-Blocks-Web-Pages-Touting-Darwins-Evolution-Theory-136162663.html.
[33] Sara Reardon, "Controversial Turkish Internet Censorship Program Targets Evolution Sites," Science Magazine, December 9, 2011, http://news.sciencemag.org/scienceinsider/2011/12/controversial-turkish-internet-c.html?ref=hp.
[34] "Agos'u Biz Değil Sistem Engelledi" [AGOS was filtered through the Ministry of Education filter. See Haber Merkezi], Bianet, January 23, 2012, http://www.bianet.org/bianet/ifade-ozgurlugu/135645-agosu-biz-degil-sistem-engelledi.
[35] See http://www.tib.gov.tr/tr/tr-duyuru-30-guvenli_internet_hizmeti%E2%80%99nin_1._yili_dolayisiyla_ankara_ve_istanbul%E2%80%99da_etkinlikler_duzenlendi.html.
[36] See http://www.tib.gov.tr/tr/tr-duyuru-30-guvenli_internet_hizmeti%E2%80%99nin_1._yili_dolayisiyla_ankara_ve_istanbul%E2%80%99da_etkinlikler_duzenlendi.html.
[37] See response to Ibrahim Binici dated 27 February 2012, TBMM response no. A.01.0.KKB.0.10.00.00-120.07(7/3747)-79795-50631.
[38] Google, "Turkey," Google Transparency Report, accessed July 11, 2013, http://www.google.com/transparencyreport/removals/government/TR/.

Google received 148 requests from the TIB to remove 426 videos, all due to alleged criticism of Atatürk, the government, or national identity and values. Google took down 63 percent of those videos.[39] The amount of requests decreased between July and December 2012. Turkish authorities had requested to remove 17 YouTube videos and 22 Blogger posts. Google cooperated in 52 percent of cases related to YouTube, but did not remove any content on its Blogger service. In addition, the company removed 6,851 out of 8,119 search results based on an order from a Turkish court to remove copyright infringing material.[40]

The procedures surrounding decisions to block websites, whether by the courts or the TIB, are nontransparent, creating significant challenges for those seeking to appeal. Judges can issue blocking orders during preliminary investigations as well as during trials. The reasoning behind court decisions is not provided in blocking notices and the relevant rulings are not easily accessible. As a result, it is often difficult for site owners to determine why their site has been blocked and which court has issued the order. The TIB's mandate includes executing judicial blocking orders, but it can also issue administrative orders under its own authority for certain content. Moreover, in some cases it has successfully asked content and hosting providers to remove offending items from their servers, allowing it to avoid issuing a blocking order that would affect an entire website. This occurs despite the fact that intermediaries are not responsible for third party content on their sites.

According to TIB statistics as of May 2009, the courts are responsible for 21 percent of blocked websites, while 79 percent are blocked administratively by the TIB. The regulator has refused to publish blocking statistics since then.[41] In December 2011, an administrative court in Ankara rejected an appeal to obtain the official blocking statistics under Turkey's freedom of information law. A subsequent appeal to the Council of State, the highest administrative court in Turkey, was lodged in January 2012 to obtain the statistics.

Furthermore, the database and user profiles of the BTK's voluntary filtering system are controlled and maintained by the government. The "Child and Family Profiles Criteria Working Committee" was introduced in January 2012—almost three months after the new filtering system became operational—to address concerns about the establishment of filtering criteria. However, the formation of the committee itself raised concerns about its independence and impartiality: 7 of the 11 members of the committee are either from the BTK, the Family and Social Policies Ministry, or the Internet Board, and 3 experts are selected and appointed by the BTK. Moreover, the principles on which the committee will work remain unclear and there is no indication to suggest that the Child and Family Profiles Criteria Working Committee conducts meetings or performs any work.

Despite the large number of websites blocked, circumvention tools are widely available, enabling even inexperienced users to avoid filters and blocking mechanisms. Each time a new order is issued and a popular website is blocked, a large number of articles are published to instruct users on how to access the banned websites. As a demonstration of the extent of this phenomenon, during the

[39] Google, "Turkey."
[40] Google, "Turkey."
[41] Reporters Without Borders, "Telecom Authority Accused of Concealing Blocked Website Figures," news release, May 19, 2010, http://en.rsf.org/turkey-telecom-authority-accused-of-19-05-2010,37511.html.

two and a half year block of YouTube, the video-sharing website remained the eighth most-accessed site in Turkey.[42]

Turkish users increasingly rely on internet-based publications as a primary source of news, and despite the country's restrictive legal environment, the Turkish blogosphere is surprisingly vibrant and diverse. There are a wide range of blogs and websites through which citizens question and criticize Turkish politics and leaders, including issues that are generally viewed as politically sensitive. The majority of civil society groups maintain an online presence and social-networking sites such as Facebook, FriendFeed, and especially the microblogging platform Twitter are used for social and political campaigns.

In May 2011, internet users organized a major protest against the introduction of the proposed country-wide filtering system. The protest gathered approximately 50,000 people in Istanbul to demand freedom from filtering and the abolishment of Law No. 5651.[43] Arguably, the protest and its associated media coverage had a significant impact on the modification of the mandatory filtering system into a voluntary one.

Shortly after it was discovered that Turkey's largest ISP, TTNET, had installed the behavioral advertising service Phorm on its networks in July 2012,[44] the Alternative Informatics Association launched an online campaign to demand that TTNET end its relationship with the controversial company.[45] The association also submitted an official complaint with a public prosecutor's office on October 17, 2012.[46] Phorm has come under consistent criticism from governments, internet companies, and privacy experts around the world. The company collects information on users' online behavior without their knowledge, performing deep-packet inspection (DPI) to essentially monitor a user's connection line and create a profile of the individual's online activities to then sell to advertisers.[47] The campaign resulted in a decision by the BTK to investigate TTNET's use of the Phorm system in December 2012.[48]

VIOLATIONS OF USER RIGHTS

The Turkish constitution includes broad protections for freedom of expression. Article 26 states that "everyone has the right to express and disseminate his thought and opinion by speech, in writing or in pictures or through other media, individually or collectively."[49] Turkish law and court

[42] According to Alexa, a web information company, as of August 26, 2010, http://www.alexa.com/topsites/countries/TR.
[43] "Turks marched against government censorship of the Internet in Istanbul," CyberLaw Blog, July 19, 2010, http://cyberlaw.org.uk/2010/07/19/17-temmuz-2010-internette-sansuru-protesto-etmek-icin-2000-kisi-yuruduk.
[44] "Commencement of Commercial Activities in Turkey with TTNET," Press Release, Phorm, July 9, 2012, http://www.phorm.com/sites/default/files/2012.07.09%20TTNET%20Commercial%20Activities.pdf.
[45] For the online campign, please see "EmPhormAsyon," Accessed April 23, 2013 http://enphormasyon.org/english.html.
[46] "Turkey: Internet Report on Digital Rights 2012," EDRi-gram newsletter, October 24, 2012, Digital Civil Rights in Europe, http://www.edri.org/edrigram/number10.20/turkish-report-2012-digital-rights.
[47] See http://enphormasyon.org/english.html.
[48] BTK decision to investigate is available in Turkish: http://bit.ly/19ci5BR.
[49] "The Constitution of the Republic of Turkey," Constitutional Court of the Republic of Turkey, Accessed April 22, 2013, http://www.anayasa.gov.tr/index.php?l=template&id=210&lang=1&c=1.

judgments are subject to the European Convention on Human Rights and bound by the decisions of the European Court of Human Rights. The constitution also seeks to guarantee the right to privacy, although there are limitations on the use of encryption devices, and surveillance by security agencies is highly prevalent. There are no laws that specifically criminalize online activities like posting one's opinions, downloading information, sending e-mail, or transmitting text messages. Instead, many provisions of the criminal code and other laws, such as the Anti-Terrorism Law, are applicable to both online and offline activity. Over the past year, only one user was sentenced to prison, while many others received suspended sentences and fines.

Several recent court cases have illuminated how the existing laws are being used to prosecute online activity. For example, in October 2011, the Anti-Terrorism Law was used to prosecute journalist Recep Okuyucu for allegedly advocating terrorist propaganda by downloading Kurdish music files and accessing the blocked Kurdish *Firat News Agency* website.[50] A Diyarbakir court found him not guilty. More recently, Adana High Criminal Court No. 8 sentenced Metin Öztürk to nine years and seven months imprisonment for sharing and disseminating terrorist propaganda through Facebook in January 2013.[51] Ten people, including three university students, were arrested in relation to the Redhack movement and face terrorism related charges, including membership in a terrorist organization.[52] They have denied all charges and any association with Redhack, stating they do not possess the technical knowledge required to hack into government servers. Redhack has reiterated that the accused individuals have no ties with the group. Indeed, speaking through social networks, Redhack stated that the terrorism allegations are simply part of the government's ongoing targeting of its domestic opponents.[53]

Users are also prosecuted for posts that can be deemed as insulting state authorities. A 17-year-old from northwest Turkey received a suspended sentence of 11 months and 20 days for insulting the Prime Minister on Facebook in July 2012 after a five-month trial at the Balıkesir Juvenile Court.[54] In November 2012, a senior post office official named İbrahim Davutoğlu was sentenced by the Zonguldak Penal Court of First Instance No. 2 to a fine of TRY 6,080 ($3,368) on charges of "insulting a public officer due to the performance of his public duty" under Article 125 of the Turkish Penal Code. The sentence was later reduced to five years of court supervision. According to the court, Davutoğlu shared politically offensive news articles and caricatures on his Facebook wall and insulted the prime minister.[55] A previous administrative investigation by the Turkish Post and Telegraph Organization (PTT) found Davutoğlu guilty of "insulting state officers," which resulted in his forced assignment to Ordu and Bartin provinces. The house of Irem Aksoy was searched by the police subsequent to a tweet in which she criticized the Mayor of Ankara for his

[50] "Court Acquits Journalist Who Interviewed Kurdish Separatist," Reporters Without Borders, December 29, 2011, http://en.rsf.org/turkey-journalists-under-pressure-as-26-10-2011,41282.html.
[51] See http://www.evrensel.net/news.php?id=45658.
[52] See http://english.alarabiya.net/articles/2012/11/26/251896.html.
[53] See 'Terrorist organization'? Turkish hackers face quarter-century prison terms, 10 October, 2012 at http://rt.com/news/redhack-turkey-terrorism-trial-056/.
[54] Suleyman Okan, "Kid Faces Jail Term After Insulting PM Erdoğan on Facebook," Sosyalmedya.co, July 23, 2012, http://sosyalmedya.co/en/kid-insulting-erdogan/.
[55] Bianet, PM Critic Facebook User Fined, at http://ww.bianet.org/english/freedom-of-expression/142130-pm-critic-facebook-user-fined.

comments on the issue of abortion. The 17-year-old student was detained by the police and a criminal investigation was subsequently initiated. In March 2013, it was reported that she was called to provide her statement by the office of the public prosecutor, which is investigating the allegation.[56]

Even Turkish citizens living outside of the country can be targeted by state authorities. The owner of the 5posta.org website, mentioned above, was prosecuted for publishing obscene materials online. Among other topics, the author writes about issues of sexuality, the sex industry, and internet censorship from his residence in Sweden. An Ankara court acquitted him of the charges in January 2013.[57]

The case that received the most media attention over the last year relates to the composer and pianist Fazil Say. In June 2012, Say was charged with offending Muslims over posts he made on Twitter, including an April 2012 tweet in which he joked about a call to prayer lasting only 22 seconds. Say was charged in June 2012 with inciting hatred and public enmity, as well as insulting "religious values" under Section 216(3) of the criminal code.[58] He received a suspended sentence of 10 months in prison, meaning that his sentence will not come into force unless he commits another offense within five years.[59] However, subsequent to an appeal by his lawyers to annul the sentence, a retrial was ordered in April 2013.[60] Furthermore, in January 2013, the office of Istanbul's Public Prosecutor initiated a criminal investigation against the board of PEN Turkey, a division of the global writers association PEN International, related to a June 2012 article on its website in which it protested against Say's prosecution.[61] The board members were charged with insulting state authorities under the controversial Article 301 of the Turkish Penal Code.[62]

In another case related to blasphemy, Turkish-Armenian linguist and former columnist Sevan Nişanyan was sentenced to 13 months imprisonment in April 2013 for "publicly insulting the religious values of part of the population." The allegations related to a blog entry he authored in 2012 about the "Innocence of Muslims" video which sparked protests across the Arab world.[63]

---

[56] "Liseli İrem Aksoy savcılıkta ifade verdi" [High schooler Irem Aksoy testifies], Aydinlik, March 6, 2013, http://www.aydinlikgazete.com/mansetler/19772-liseli-irem-aksoy-savcilikta-ifade-verdi.html.
[57] Ankara 7th Criminal Court of First Instance, Decision no 2013/7, 21.02.2013
[58] The Guardian, Turkish pianist Fazil Say on trial for 'insulting Islam' on Twitter, 18 October 2012 at http://www.guardian.co.uk/world/2012/oct/18/turkish-pianist-fazil-say-islam.
[59] Sebnem Arsu, "Pianist's Post on Twitter Spur Penalty From Turkey," New York Times, April 5, 2013, http://www.nytimes.com/2013/04/16/world/middleeast/turkish-pianist-sentenced-for-twitter-postings.html?_r=0.
[60] Hürriyet Daily News, "Turkish pianist Fazıl Say to be retried on blasphemy charges," 26 April 2013, at http://www.hurriyetdailynews.com/turkish-pianist-fazil-say-to-be-retried-on-blasphemy-charges.aspx?pageID=238&nID=45718&NewsCatID=341.
[61] The article in question refers to "fascist developments" in Turkey. See PEN International condemns investigation against PEN Turkey for criticising the State, at http://www.pen-international.org/newsitems/pen-international-condemns-investigation-against-pen-turkey-for-criticising-the-state/.
[62] "Amendment Law Nr. 5759 of April 30, 2008 (Turkish)," April 30, 2008, http://www.tbmm.gov.tr/kanunlar/k5759.html.
[63] See "Living by the 'de jure' sword," Hurriyet Daily News, 24 May 2013 at http://www.hurriyetdailynews.com/living-by-the-de-jure-sword.aspx?pageID=238&nID=47499&NewsCatID=398 See further Sevan Nisanyan: Turkish-Armenian blogger jailed for blasphemy, http://www.globalpost.com/dispatch/news/regions/europe/turkey/130523/sevan-nisanyan-turkish-armenian-blogger-jailed-blasphemy.

The constitution states that "secrecy of communication is fundamental," and users are allowed to post anonymously online. However, the anonymous purchase of mobile phones is not allowed and buyers need to provide official identification. Turkey has yet to adopt a data protection law, though the September 2010 amendments to the Turkish Constitution included data protection provisions. In 2011, the use of encryption hardware and software became subjected to regulations introduced by the BTK. Suppliers are now required to provide encryption keys to state authorities before they can offer their products or services to individuals or companies within Turkey. Failure to comply can result in administrative fines and, in cases related to national security, prison sentences.

The constitution specifies that any action that could potentially interfere with freedom of communication or the right to privacy must be authorized by the judiciary. For example, judicial permission is required for technical surveillance under the Penal Procedural Law. Despite constitutional guarantees, most forms of telecommunication continue to be tapped and intercepted.[64] Between 2008 and 2009, several surveillance scandals received widespread media attention, and it is suspected that all communications are subject to interception by various law enforcement and security agencies, including the Gendarmerie (military police). Some reports indicate that every day, up to 50,000 phones—both mobile and land-line—are legally tapped, and 150,000 to 200,000 interception requests are made each year. During 2012, bugging related stories continued to hit the headlines and even the Prime Minister claimed that bugging devices were found in his home.

These surveillance practices have been challenged in court on at least one occasion. In 2008, responding to complaints lodged by the TIB, the Supreme Court of Appeals overruled a lower court's decision to grant both the Gendarmerie and the National Intelligence Agency (MIT) the authority to view countrywide data traffic retained by service providers.[65] Nonetheless, similar powers to access and monitor data traffic have been granted to the MIT and the National Police Department. Faced with criticism on the issue, in 2008 the parliament launched a major inquiry into illegal surveillance and interception of communications, though the inquiry concluded in January 2009 without finding any "legal deficiencies" in the interception regime. In January 2013, a new parliamentary commission was set up with a similar goal and, during its initial investigation, revealed that the Turkish Gendarmerie had intercepted the communications of 470,102 people subject to 75,478 court orders during the last 10 years.[66] The commission is expected to conclude its work later in 2013.

While government surveillance is an issue in Turkey, ISPs are not required to monitor the information that goes through their networks, nor do they have a general obligation to seek out

[64] For a history of interception of communications, see: Faruk Bildirici, *Gizli Kulaklar Ulkesi* [The Country of Hidden Ears] (Istanbul: Iletisim, 1999); Enis Coskun, *Kuresel Gozalti: Elektronik Gizli Dinleme ve Goruntuleme* [Global Custody: Electronic Interception of Communications and Surveillance] (Ankara: Umit Yayincilik, 2000).

[65] The court stated that "no institution can be granted such authority across the entire country, viewing all people living in the Republic of Turkey as suspects, regardless of what the purpose of such access might be." See, "Supreme Court of Appeals Overrules Gendarmerie Call Detail Access," Today's Zaman, June 6, 2008, http://www.todayszaman.com/tz-web/news-144038-supreme-court-of-appeals-overrules-gendarmerie-call-detail-access.html.

[66] See the Bianet article (in Turkish) at http://www.bianet.org/bianet/insan-haklari/145087-jandarma-10-yilda-470-bin-kisiyi-dinledi.

illegal activity. However, all access providers, including cybercafe operators, are required to retain all communications (traffic) data for one year. Administrative fines of TRY 10,000 to 50,000 ($6,400 to $32,200) can be imposed on access providers if they fail to comply, but no ISP or other provider has been prosecuted to date.

Although physical attacks in retribution for online posts are generally rare, technical attacks are becoming increasingly common, particularly those targeting government websites. During 2011 and in early 2012, the international hacktivist collective known as Anonymous launched a successful distributed denial-of-service (DDoS) attack against the Turkish government, taking down several official government websites, including those of the TIB[67] and Turkish Social Security Institution (SGK).[68] Furthermore, Anonymous hacked a consumer complaints website run by the BTK in February 2012 and data relating to a considerable number of users was circulated through numerous websites.[69] During 2012, the Marxist-Socialist Redhack group infiltrated several government websites and leaked confidential information. The group has over 675,000 followers on Twitter and hacked into the servers of the Ministry of Foreign Affairs, Ministry of Finance, and the Turkish Higher Education Authority, among others, during 2012 and early 2013.[70]

[67] www.tib.gov.tr
[68] www.sgk.gov.tr
[69] "Anonymous Hacked BTK Database," Bianet, February 15, 2012, http://www.bianet.org/english/world/136178-anonymous-hacked-btk-database.
[70] See among others http://redhack.tumblr.com/post/40121086113/press-release-council-of-higher-education-of-turkey and extensive media coverage of Redhack's activities through http://redhack.tumblr.com/archive.

UGANDA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	11	11
Limits on Content (0-35)	8	8
Violations of User Rights (0-40)	15	15
Total (0-100)	34	34

* 0=most free, 100=least free

POPULATION: 35.6 million
INTERNET PENETRATION 2012: 15 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- There were no reports of internet content being blocked or filtered during the coverage period, though various government officials publicly expressed the "need" to police online discussions (see **LIMITS ON CONTENT**).
- The Uganda Communications Act 2012 was passed in September, creating a new media regulatory body that has been criticized for its lack of independence from the government (see **LIMITS ON CONTENT**).
- SIM card and mobile internet registrations continued through early 2013 amid concerns that the registration requirements infringe on the right to privacy given the lack of a necessary data protection law (see **VIOLATIONS OF USER RIGHTS**).
- Government harassment for online writing was documented, while suspicions of proactive government surveillance of online communications increased in the past year (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Internet penetration has continued to grow in Uganda, and access is now estimated at 15 percent of the population, with a growing number of Ugandans accessing the internet from their mobile phones. Nevertheless, accessibility is still hindered by poor infrastructure, prohibitive costs, and poor quality of service. Moreover, recent measures have exacerbated the rural-urban divide in access to information and communication technologies (ICTs), such as a ban on counterfeit mobile phones and compulsory SIM card registration. Overall, however, freedom to access the internet via computer-based applications and mobile devices remains generally unfettered.

There were no reported incidents of government interference with ICTs in 2012 or early 2013, though there have been increasing indications that the government intends to monitor online discussions, as demonstrated by various statements made by government officials in 2012 calling for the policing of social media platforms. The main threat to Uganda's internet freedom in 2012 involved the passage of the Uganda Communications Act 2012 in September, which created a new regulatory body for all print, broadcast, and electronic media in Uganda—the Uganda Communications Regulatory Authority. Awaiting presidential assent as of mid-2013, the new law vests an undue amount of power in the ICT minister to determine the regulatory body's membership, budget, and policy guidelines.

OBSTACLES TO ACCESS

ICTs continued to expand across Uganda over the past year, resulting in increasing access to both internet and mobile phone services. By the end of 2012, there were an estimated five million internet users in the country for a penetration rate of nearly 15 percent, up from 13 percent in 2011 and just 4 percent in 2007, according to the International Telecommunications Union.[1] Broadband internet is available mostly in urban areas, with only 0.11 percent of the population estimated to have fixed-line broadband subscriptions in 2012.[2] As such, many Ugandans access the internet at cybercafés where it costs less than $1 for an hour of browsing. Meanwhile, mobile phone penetration stood at 46 percent at the end of 2012[3] with a reported 17 million subscribers, up from 4.2 million in 2007, though multiple SIM card ownership remains common.

Internet access via mobile devices is becoming increasingly popular due to the growing availability of cheap mobile internet bundles, with mobile broadband penetration estimated at 7.6 percent at the end of 2012.[4] An hour of mobile web browsing (equating to approximately 20Mb of data) costs KGX 500 ($0.20), while a limited monthly bundle of 1Gb costs between KGX 30,000 and 41,000

[1] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[2] International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2012."
[3] International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2012."
[4] International Telecommunication Union, "Uganda Profile 2012," ICT-Eye, http://www.itu.int/net4/itu-d/icteye/CountryProfile.aspx.

($12-16). Meanwhile, an unlimited mobile broadband connection[5] can cost KGX 299,000 ($115) for one month and over $600 for six months. Two service providers offer their subscribers free access to Facebook,[6] and to promote local content, Airtel Uganda began offering its customers in early 2013 free access to Uganda Goes Online—an online portal that provides information and local content ranging from news, entertainment, sports, technology and much more.[7]

The number of industry players has grown over the years, and many now offer comparable prices and technologies. Currently, there are 34 telecommunications service providers that offer both voice and data services.[8] Aside from the state-owned Uganda Electricity Transmission Company Ltd, which is a licensed public infrastructure provider that has part ownership of Uganda Telecom, all the licensed service providers are privately-owned entities.

There are no known obstacles or licensing restrictions placed by the government on entry into the ICT sector, and new players continued to enter the market in 2012 and 2013. For example, YahClick, a satellite broadband services provider was launched in February 2013,[9] while K2 mobile was launched only a monthly earlier.[10] The two joined a competitive market dominated by bigger, well-established telecommunications brands, such as MTN Uganda, Airtel and Warid Telecom. Three 4G LTE network licenses were issued in mid-2012, though the firms have yet to deploy the high-speed data transmission technology as of mid-2013.[11] Meanwhile, the quality of both voice and data services remains very low.[12]

While increasing market competition has continued to drive down internet access rates,[13] particularly on mobile phones, the cost of internet-enabled devices is still high for the majority of Ugandans who make an average monthly income of $117, according to the latest data from the Uganda Bureau of Statistics.[14] Prohibitive tax regimes remain in place despite successful moves by

---

[5] On the Orange Uganda network.
[6] MTN, "MTN Launches Facebook Zero, a Free Way to Access Facebook on your Mobile Phone," press release, May 18, 2010, http://mtn.co.ug/About-MTN/News-Room/2010/May/MTN-launches-Facebook®-ZERO,-a.aspx; Orange, "Get Facebook Free on Your Mobile Phone," accessed August 8, 2013, http://www.orange.ug/mobile-plans/facebook-for-free.php.
[7] "Airtel to Offer Free Access to Uganda Going Online," CIO East Africa via *AllAfrica*, February 7, 2013, http://allafrica.com/stories/201302071503.html; David Mugabe, "Airtel-UGO Deal to Shape Uganda's Online Image," *New Vision*, February 7, 2013, http://www.newvision.co.ug/news/639617-airtel-ugo-deal-to-shape-uganda-s-online-image.html.
[8] Uganda Communications Commission, List of Licencees in Uganda, available at http://www.ucc.co.ug/files/downloads/licensedProviders.pdf.
[9] Nicholas Kalungi, "New Player Joins Internet Market," *Daily Monitor*, February 4, 2013, http://www.monitor.co.ug/Business/Technology/New-player-joins-Internet-market/-/688612/1683212/-/yethtoz/-/index.html.
[10] "K2 Telecom Launches Mobile Phone Services in Uganda," *Telecompaper*, January 2, 2013, http://www.telecompaper.com/news/k2-telecom-launches-mobile-phone-services-in-uganda--916578.
[11] Elias Biryabarema, "Uganda Internet Users Seen Up 15-20 Pct in 2012," Reuters, May 31, 2012, http://www.reuters.com/article/2012/05/31/ozabs-uganda-telecoms-idAFJOE84U09020120531.
[12] Dorothy Nakaweesi, "Major Telecom Operators on Spot Over Poor Service Quality," *Daily Monitor*, January 24, 2013, http://www.monitor.co.ug/Business/Technology/Major-telecom-operators-on--spot-over-poor-service-quality/-/688612/1673500/-/4f1eakz/-/index.html.
[13] Nicholas Kalungi, "Competition Bringing Internet Rates Down," *Daily Monitor*, November 9, 2012, http://www.monitor.co.ug/Business/Technology/Competition-bringing-Internet-rates-down/-/688612/1616104/-/38omqaz/-/index.html.
[14] Uganda Bureau of Statistics, "Chapter 7: Household Incomes, Loans and Credit," *Uganda National Household Surveys Report 2009/2010*, accessed July 31, 2013, http://www.ubos.org/UNHS0910/chapter7.Average%20Monthly%20Household%20Income.html.

Uganda's neighbors to remove duties on the importation of hardware and software. Most recently in 2013, the government launched an effort to curb the importation of counterfeit mobile phones, which may further limit access to mobile technologies. All inactive counterfeit phones were rendered unusable as of January 31, 2013, while fake phones with preexisting subscriptions were to be disconnected beginning July 1, 2013.[15] There are no figures to indicate how many users have been and will be affected by this initiative, but it is conceivable that the number may be in the millions. In addition, a 2009 government ban on the importation of used computers remains in place.

Another impediment to increased internet usage is limited access to electricity. The national electricity distributor reports a customer base of just 458,000, most of whom are located in urban areas,[16] and alternative power sources, such as fuel-powered generators and solar energy, are very costly. Furthermore, with only about 15 percent of Ugandans living in urban areas,[17] the divide between rural and urban access to the internet is very high due to low literacy rates, including computer literacy.[18]

Uganda's national fiber backbone is connected to the EASSy international submarine fiber optic cable system that runs along the east and southern coasts of Africa. Telecommunications providers are also hooked to the TEAMs (The East African Marine System) and SEACOM marine fibers through Kenya. Connection to these fibers has led to an exponential growth in Uganda's international bandwidth, which has decreased the costs of internet access alongside an increasing demand for data services and high speed internet. Service disruptions and slow internet speeds are common, however, due to frequent repairs.[19]

Over the past few years, the government has embarked on initiatives to improve rural connectivity, and a national ICT policy was finalized in 2010 to facilitate the proliferation of ICTs across the country in both rural and urban areas.[20] Nonetheless, the national ICT sector budget allocation comprises less than one percent of the national budget.[21] Since 2007, Uganda's ICT ministry has

---

[15] Uganda Communications Commission,, "Elimination of Counterfeit Mobile Phones," December 19, 2012, http://www.ucc.co.ug/data/mreports/18/0/ELIMINATION%20OF%20COUNTERFEIT%20MOBILE%20PHONES%20.html; Nicholas Kalungi, "Blocking of Inactive Fake Phones Starts Today," *Daily Monitor*, February 1, 2013, http://www.monitor.co.ug/Business/Blocking-inactive-fake-phones-starts-today--UCC-says/-/688322/1680796/-/rdjdqez/-/index.html.

[16] Umeme "Annual Report 2011," http://www.umeme.co.ug/resources/files/Umeme%20Annual%202011%20b.pdf.

[17] Uganda Bureau of Statistics, "2012 Statistical Abstract," June 2012, http://www.ubos.org/onlinefiles/uploads/ubos/pdf%20documents/2012StatisticalAbstract.pdf.

[18] Uganda's national literacy rate stands at 73 percent among persons aged 10 years and above. See: Uganda Bureau of Statistics, "2012 Statistical Abstract."

[19] Nicolas Kalungi, "Internet Speed Slows Down Due to Repairs at Mombasa," *Daily Monitor*, January 10, 2013, http://www.monitor.co.ug/Business/Internet-speed-slows-down-due-to-repairs-at-Mombasa/-/688322/1661636/-/jntm8y/-/index.html; "Massive Internet outage in Uganda as Under Sea Cable is Chopped," *Guide2Uganda*, February 29, 2012, http://www.guide2uganda.com/news/415/Massive-Internet-outage-in-Uganda-as-undersea-cable-is-chopped.

[20] Ministry of Information and Communications Technology, "Information Technology Policy for Uganda," Republic of Uganda, February 2010, http://ict.go.ug/index.php?option=com_docman&task=doc_details&gid=48&Itemid=61.

[21] "A Peek into the East African ICT Sector Budget Allocations and Priorities for 2012/2013," Collaboration on International ICT Policy in East and Southern Africa, ICT Policy Briefing Series, June 2012, http://www.cipesa.org/?wpfb_dl=41; Edris Kisambira, "East African Countries Put IT Spending On Back Burner," *Computer World*, July 16, 2012, http://news.idg.no/cw/art.cfm?id=A95D59B0-CC4C-DC2F-8368A85290AEE888.

been developing the National Data Transmission Backbone Infrastructure, which aims to ensure the availability of high bandwidth data connection in all major towns at reasonable prices.[22] The project, now under the provision of the National Information Technology Authority (NITA-U), involves the installation of over 1,500km of fiber optic cable and related equipment.[23] However, the $106 million project has been dogged by contractual problems, government red tape, delayed funds, and unverified allegations of inferior equipment and work as of mid-2012.[24] The Chinese company, Huawei Technologies, contracted for the installation has been accused of using substandard cables, and in some cases, the wrong cables.[25]

The government has also embarked on a project to establish computer centers in all of its educational institutions across the country, with a plan to cover at least 1,000 institutions by the end of 2012.[26] In addition, the Rural Communications Development Fund was established in 2001 with the aim of providing access to basic communications services within a reasonable distance to all Ugandans, leveraging investments for rural communications, and promoting overall ICT usage.[27] The fund further supports the establishment of internet cafes, internet points of presence (rural wireless connectivity networks with a 5-10km radius with costs, speeds and types of services comparable to those in the capital city, Kampala), ICT training centers, and web portals for local government districts.

The Uganda Communications Commission (UCC), Uganda's telecommunications sector regulator, is mandated to independently coordinate, facilitate and promote the sustainable growth and development of ICTs in the country. The UCC also provides information about the regulatory process and quality of service, and it issues licenses for ICT infrastructure and service providers.[28] The commission's funds come mainly from operator license fees and a 1 percent annual levy on operator profits. There is a general perception, however, that comprehensive and coherent information about the commission's operations is not always accessible, and that the body is not entirely independent from the executive arm of the government. In addition, the UCC's current

[22] Ministry of Information and Communications Technology, "National Data Transmission Backbone and e-Government Infrastructure Project," Republic of Uganda, accessed June 29, 2012, http://www.ict.go.ug/index.php?option=com_content&view=article&id=69:national-data-transmission-backbone-and-e-government-infrastructure-project&catid=25:the-project&Itemid=93.

[23] Such as switches, optical transmission, data communication, fixed network, and video equipment, as well as computers and servers. See: "NBI/EGI Project," National Information Technology Authority – Uganda, accessed June 29, 2012, http://www.nita.go.ug/index.php/projects/nbiegi-project.

[24] Flavia Nalubega, "Govt Bureaucracy Delays Fibre Internet Backbone," *Daily Monitor*, April 20, 2012, http://www.monitor.co.ug/Business/-/688322/1390242/-/50js39/-/index.html.

[25] John Njoroge, "Forensics Dispute Quality of Uganda's Internet Cables," *Daily Monitor*, April 14, 2012, http://www.monitor.co.ug/News/National/-/688334/1385826/-/aw3qrvz/-/index.html.

[26] Elias Biryabarema, "Uganda Internet Users Seen up 15-20 Pct." Reuters, May 31, 2012, http://www.reuters.com/article/2012/05/31/ozabs-uganda-telecoms-idAFJOE84U09020120531.

[27] Uganda Communications Commission, "Rural Communications Development Policy for Uganda," January 2009, http://www.researchictafrica.net/countries/uganda/Uganda%20Rural%20Communication%202009.pdf.

[28] Uganda Communications Commission, "UCC Licensing Regime," accessed July 31, 2013, http://www.ucc.co.ug/data/qmenu/11/Licensing.html; Pursuant to the telecommunications (licensing) regulations 2005, UCC issues two types of licences: Public Service Provider (PSP) and Public Infrastructure Provider (PIP). The application fee for both license types is $2,500 dollars (a PIP license requires a one-off initial fee of $100,000), and annual fees range from $3,000-$10,000. These licenses allow holders to either set up telecommunications infrastructure or provide telecommunications services. The UCC levies a 1 percent charge on providers' annual revenue.

executive director has been regarded as overzealous in his efforts to police and rein in operators, illustrating how the personal character of the regulatory authority's leadership can in large measure determine its activities and regulations.

In September 2012, the Ugandan parliament passed the Uganda Communications Act 2012 (introduced by the ICT ministry in March 2012 as the Uganda Communications Regulatory Authority Bill), which consolidated the provisions of the 1996 Electronic Media Act and 2000 Uganda Communications Act and merged the UCC and Uganda Broadcasting Council into a new body, the Uganda Communications Regulatory Authority.[29] Awaiting presidential assent as of mid-2013, the new regulatory body has been criticized for its lack of independence from the government. In particular, the law places disproportionate power in the hands of the ICT minister, who will have the authority to approve the new regulator's budget and appoint members of its board with the approval from the Cabinet. There are no independent mechanisms in place to hold the regulator accountable to the public. While the new law provides for the creation of the Uganda Communications Tribunal, which is an appeals body with powers of the High Court, its membership and advisors are appointed by the president and ICT minister.

LIMITS ON CONTENT

There have been no reported incidents of government interference with the internet since the 2011 elections, during which the national regulator issued a directive to ISPs to temporarily block citizens' access to Facebook and Twitter. The order came in response to the mobilization of activists and opposition groups, which were largely organized through the two social media platforms. That same year, in the wake of demonstrations inspired by the Arab Spring events in North Africa, there were unconfirmed allegations that the Ugandan government had ordered telecoms to block and regulate the use of some keywords such as "bullet," "Mubarak," and "Ben Ali" in SMS texting services.[30]

There have also been no known instances of take-down notices issued for the removal of online content, and there are no issues of intermediary liability for service or content providers.[31] In the meantime, social media and blogging platforms are freely available in Uganda, with Facebook, Twitter, LinkedIn and Blogger ranking among the top 15 websites in the country, according to Alexa. The government has also begun to embrace social media platforms as a channel for public engagement, as illustrated by Uganda's Prime Minister, Amama Mbabazi, who interacts with citizens on Twitter using the hashtag #AskthePM.[32]

[29] Sheila Naturinda and Mercy Nalugo, "Parliament Adopts Media Regulatory Law," *Daily Monitor*, September 7, 2012, http://www.monitor.co.ug/News/National/Parliament-adopts-media-regulatory-law/-/688334/1498374/-/gnthq4/-/index.html.
[30] Hosni Mubarak was the embattled president of Egypt at the time, while Ben Ali was the deposed Tunisian leader.
[31] Ashnah Kalemera, Lillian Nalwoga and Wairagala Wakabi, "Intermediary Liability in Uganda," Intermediary Liability Africa Research Papers 5, Association for Progressive Communications, http://www.apc.org/en/system/files/Intermediary_Liability_in_Uganda.pdf.
[32] Amana Mbabazi's Twitter page, accessed August 8, 2013, https://twitter.com/AmamaMbabazi.

While there is no evidence of government efforts to influence or manipulate online content, previous shut downs of media houses seen as too critical of the government, in addition to reports of attacks on journalists by the national police,[33] and other routine threats by the government have engendered a culture of self-censorship among journalists both off and online. Taboo topics include the military, the president's family, issues of oil, land-grabbing, and presidential terms. In addition, there have been increasing indications that the government intends to monitor online discussions, as demonstrated in October 2012 when the Ugandan police chief called for the policing of social media networks to ensure that the platforms are not spreading "dangerous" information or are "misused for crime, worse still terrorism."[34]

The Google Uganda domain is available in five local languages, making the popular browser available to about five million Ugandans.[35] Nevertheless, Ugandans can only access news websites in three local languages (out of 40 languages and 56 native dialects) provided by the Vision Group, a media company that is partly owned by the government. The web versions of the newspapers include *Bukedde*, *Etop* and *Orumuri*. Other news sites of major privately-owned newspapers are only accessible in English, which is not widely spoken in Uganda. Moreover, the diversity of online content and the economic viability of independent outlets is constrained by advertising revenue from both government and private sources, which is generally withheld from news outlets that publish critical content.[36]

In recent years, government critics and opposition political parties have taken to the internet as a platform for political debate and an informal means of disseminating information to society. Crowdsourcing and crowd-mapping tools have given citizens the ability to monitor elections, and a diversity of civil society groups are increasingly using SMS platforms and social media for advocacy and to call for protests. In addition, blogging is on the rise among young Ugandans who are less fearful in their use of the internet as an open space to push the boundaries and comment on controversial issues such as good governance and corruption.[37]

VIOLATIONS OF USER RIGHTS

SIM card and mobile internet registrations continued through early 2013 amid concerns that the registration requirements infringe on the right to privacy given the lack of a necessary data protection law. Government harassment for online writing was documented, while suspicions of proactive government surveillance of online communications increased in the past year, with one unconfirmed case involving the interception of a private e-mail reported by an LGBT rights group in early 2013.

---

[33] Freedom House, "Uganda," *Freedom of the Press 2013*, http://www.freedomhouse.org/report/freedom-press/2013/uganda.
[34] "Uganda Police Chief Urges Increased Social Media Policing," BBC News, October 19, 2012, http://bbc.in/Qwj8yh.
[35] Tabitha Wambui, "Google Uganda Launches Two New Local Language Domains," *Daily Monitor*, August 4, 2010, http://www.monitor.co.ug/Business/Technology/-/688612/970404/-/uithj9/-/index.html.
[36] "Uganda 2012," *African Media Barometer* (Windhoek: Friedrich-Ebert-Stiftung, 2012).
[37] Joseph Elunya, "Controversial Ugandan Blogger Won't Budge," Radio Netherlands Worldwide, August 26, 2012, http://allafrica.com/stories/201208260215.html.

The Ugandan Constitution provides for freedom of expression and speech, in addition to the right to access information.[38] However, several laws—including the Press and Journalist Act, the Anti-Terrorism Act, and sections of the penal code—appear to negate these constitutional guarantees for freedom of expression. For example, the Press and Journalist Act of 2000 requires journalists to register with the statutory Media Council, whose independence is believed to be compromised by the government's hand in its composition. Meanwhile, the Anti-Terrorism Act criminalizes the publication and dissemination of content that promotes terrorism, vaguely defined, and guilty convictions can carry up to the death sentence. In addition, the penal code contains provisions on criminal libel and the promotion of sectarianism, imposing penalties that entail lengthy jail terms. While none of these laws contain specific provisions on online modes of expression, they could arguably be invoked for online communications and generally create a "chilling effect" on freedom of expression.

In the meantime, the Ugandan judiciary has been known to rule progressively in cases involving press freedom and freedom of expression. In 2004, for example, the Supreme Court struck down a penal code provision that criminalized the publication of false news, while the Constitutional Court quashed the law on sedition in 2010. Nevertheless, judicial rulings protecting constitutional guarantees for free expression have not stopped the government from taking action against fundamental rights, though prosecutions against journalists and citizens for online expression remain rare.

While there are no website registration requirements in Uganda, registration for mobile phone SIM cards and mobile internet subscriptions was instituted in March 2012 and involves the collection of personal data, including photographs and address details. The deadline to register existing SIM cards was extended through March 2013, after which point unregistered cards were deactivated. Civil society groups criticized the program for infringing on the right to privacy given the lack of a necessary data protection law,[39] and an injunction filed by the Human Rights Network for Journalists-Uganda to stop the registration exercise was thrown out by the High Court on February 25, 2013.[40]

Government monitoring and surveillance of electronic communications has become a worrisome issue in Uganda since 2010, when parliament hurriedly passed the Regulation of Interception of Communications (RIC) Act following the terrorist attacks by Al Shabab militants in Kampala in July 2010. Allowing for the interception of communications, the RIC act requires telecommunication companies to install equipment that enables the real-time electronic surveillance of suspected terrorists and gives the government permission to tap into personal communications based on

[38] The Access to Information Act provides for the right to access information pursuant to Article 41 of the constitution, the right to prescribe the classes of information referred to in that article, the procedure for obtaining access to that information, and for related matters.

[39] "Law Requiring Registration of SIM Cards in Uganda a Threat to Privacy," Human Rights Network for Journalist Uganda, September 24, 2012, http://www.ifex.org/uganda/2012/09/24/sim_card_registration/.

[40] Juliet Kigongo and Dorothy Nakaweesi, "Bid to Stop SIM Card Registration Thrown Out," *Daily Monitor*, February 26, 2013, http://www.monitor.co.ug/News/National/Court-refuses-to-block-SIM-card-registration/-/688334/1704590/-/u4hc7h/-/index.html.

national security concerns.[41] This action can be requested by the security minister and granted after an order by a High Court judge. Telecommunications service providers are further required to disclose the personal information of individuals suspected of terrorism to the authorities upon issue of a court warrant or notice from the minister on matters related to national security, national economic interests, and public safety.[42] Failure to comply with the provisions in the RIC act can entail penalties of up to five years in prison for intermediaries, in addition to license revocations.[43] Meanwhile, clauses in the Anti-Terrorism Act also give security officers the power to intercept the communications of individuals suspected of terrorism and to keep them under surveillance. This includes journalists who are suspected to have been in touch with individuals designated as terrorists by the state.

As of April 2013, it is not clear the extent to which the provisions of the 2010 RIC act have been implemented or operationalized. For instance, it is unknown whether service providers have installed monitoring equipment as required by law. It is also unclear whether the government has asked service providers to monitor communications without a court warrant. Meanwhile, telecom industry observers argue that competition between service providers makes it harder for them to readily hand over information to the government without going through legal channels, though the observers also do not rule out the possibility that some companies may cooperate quietly with government requests.

Nevertheless, a private interview conducted by Freedom House with an LBGT rights group in early 2013 uncovered a case in which an e-mail attachment sent among a private group of individuals was possibly intercepted by an unknown actor. According to a member of the LGBT group, the attachment, which included information about different groups in Uganda's LGBT community, was later published in a local tabloid, outing certain organizations involved in LGBT activism in Uganda. While details of this account could not be corroborated, the incident falls in line with Uganda's history of discrimination against the country's LGBT community that has manifested in similar cases of public naming and shaming campaigns against LGBT individuals and groups.

Journalists in the traditional media face harassment and occasional violence for their reporting in print outlets, and these types of violations are slowly beginning to seep into the online sphere. One young blogger, Racey Carlton Mujuni, reportedly received warnings from the government about his blogging activities in 2012, particularly after he wrote about the civil conflict in the ethnic Acholi region of the country.[44]

Meanwhile, politically-motivated hacking attacks are not significant in Uganda, though there was one case reported in early 2013 involving a hacking and vandalism attack against the website of the same LGBT rights group discussed above. The perpetrator behind the attack remains unknown.

[41] Amnesty International, "Uganda: Amnesty International Memorandum on the Regulation of Interception of Communications Act, 2010," December 14, 2010, http://www.amnesty.org/en/library/asset/AFR59/016/2010/en/4144d548-bd2a-4fed-b5c6-993138c7e496/afr590162010en.pdf.
[42] Ashnah Kalemera et al., "Intermediary Liability in Uganda."
[43] Ashnah Kalemera et al., "Intermediary Liability in Uganda."
[44] Joseph Elunya, "Controversial Ugandan Blogger Won't Budge."

Ugandan government websites have also been hacked from actors outside the country a number of times this past year. For example, the international hacker group "Anonymous" hacked into the office of the prime minister's website in protest against the Anti-Homosexuality Bill in August 2012.[45]

[45] Ndesanjo Macha, "Uganda: Anonymous Backs Gay Pride, Hacks Government Website," *Global Voices*, August 16, 2012, http://globalvoicesonline.org/2012/08/16/uganda-anonymous-backs-gay-pride-hacks-government-websites/.

UKRAINE

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	7	7
Limits on Content (0-35)	8	7
Violations of User Rights (0-40)	12	14
Total (0-100)	**27**	**28**

* 0=most free, 100=least free

POPULATION: 45.6 million
INTERNET PENETRATION 2012: 34 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- While there was an increase in pressure on mainstream journalists toward self-censorship on political topics, there was also an increase in the use of ICTs for political mobilization (see **LIMITS ON CONTENT**).
- Online journalist and activist Mustafa Nayyem was reportedly beat up by the guards of a member of the Party of Regions in August 2012 (see **VIOLATIONS OF USER RIGHTS**).
- DDoS attacks occurred against election monitoring websites and opposition websites on the day of parliamentary elections (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Although Ukraine has not made notable progress in using internet and digital technology to strengthen its civil society over the past few years, the citizens of Ukraine enjoy largely unhindered access to the internet. With internet infrastructure rapidly developing since the early 1990s, information and communication technologies (ICTs) have some influence over the political process, with diverse and generally independent online media and social networks playing a key role with minimal pushback from the authorities. This comes in part as a result of the 2004–2005 Orange Revolution, in which ICTs played a significant role.[1]

Though Ukraine has relatively liberal legislation governing the internet and access to information, a number of state initiatives were introduced in 2011 that aimed to control electronic media, exercise surveillance over internet content on ethical grounds, and limit other forms of ''undesirable'' content. These efforts have the potential for direct and indirect controls over political and social content online. Direct action against online piracy websites and distributed denial-of-service (DDoS) attacks against civic initiatives online, although sparse, reveal the potential of Ukrainian authorities to engage in further limiting activities. In March 2013, the National Expert Commission on the Protection of Public Morals (NECPPM) issued a statement saying they had found immoral and discriminatory content hosted on YouTube and that the Internet Association of Ukraine should avoid "violating Ukrainian internet legislation." Nonetheless, no further action was specified.

Social media platforms are popular and increasingly used by activists for organizing and promoting ideas such as election monitoring, rights campaigning, and reporting bribery and corruption. Political parties and the government also use the internet as a tool for political competition, engaging in legitimate forms of communication such as social media profiles and blogging, as well as more manipulative techniques such as trolling and "astroturfing," or making partisan content seem independent. Social media and crowdsourcing platforms were used to monitor the parliamentary elections in 2012; many of these websites were also victims of DDoS attacks.

OBSTACLES TO ACCESS

Internet penetration in Ukraine continues to grow steadily, due in part to diminishing costs and the increasing ease of access, particularly to mobile internet. According to the International Telecommunication Union (ITU), Ukraine had an internet penetration rate of 33.7 percent in 2012,[2] a major increase from 6.6 percent in 2007.[3] At the same time, statistics from InMind show

[1] Joshua Goldstein, ''The Role of Digital Networked Technologies in the Ukrainian Orange Revolution,'' Berkman Center Research Publication No. 2007-14, December 2007, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein_Ukraine_2007.pdf.

[2] Differing from ITU statistics, the research company, InMind, found that there were 14.3 million Ukrainians ages 15 and up who used the internet at least once a month in September 2011,[2] comprising 36 percent of the total population. InMind, "Рост

that 19.7 million Ukrainians over the age of 15 use the internet regularly, which is close to 50 percent of all adult Ukrainians.[4] For fixed-broadband subscriptions, the penetration rate was approximately 7 percent in 2012, while mobile broadband had a penetration rate of 4.4 percent.[5] Meanwhile, Ukraine ranks eighth in the world for download speeds, with an average download speed of 1190 Kbps,[6] and access to broadband internet in Ukraine is fairly affordable. A monthly unlimited data plan with a 1 Mb broadband channel costs UAH 80–120 ($10–15), while the average monthly wage in the country was UAH 3,377 ($414) in December 2012.[7]

Of current internet users, 56 percent live in urban areas, while internet penetration in smaller towns and rural areas is currently below 20 percent.[8] The level of infrastructure differs between urban and rural areas, contributing to the gap in number of users. Most people access the internet from home or work, though many middle- and higher-end cafes and restaurants often provide free Wi-Fi access. Access is also common in public libraries and schools. Internet cafes still exist, but are gradually losing popularity.

Mobile phone penetration has also continued to grow, reaching 132 percent in 2012.[9] Use of mobile internet is gaining in popularity, and an estimated 14 percent of Ukrainian mobile subscribers own smartphones.[10] Cost continues to be the main barrier to higher mobile internet use. Mobile operators are still waiting for access to third-generation (3G) mobile phone frequencies, which the Ministry of Defense had promised to convert for use by mobile operators in 2012, but failed to do so.[11] The only commercial 3G license was previously owned by formerly state-run Ukrtelecom, which was privatized in March 2011, and its 3G division is a separate company currently reported to be looking for a buyer, so the issue of frequency conversion remains stalled.[12]

уровня проникновения интернета в Украине существенно замедлился" [Growth of Internet Penetration Level in Ukraine Has Slowed Significantly], AIN.UA, October 19, 2011, http://ain.ua/2011/10/19/62100.

[3] International Telecommunication Union (ITU), "Percentage of individuals using the Internet," 2006 & 2012, accessed July 6, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[4] InMind, В Украине почти 20 млн пользователей интернета [Ukraine has almost 20 million Internet users], AIN.UA, October 24, 2012, http://ain.ua/2012/10/24/99561.

[5] "Broadband: State of Broadband 2012," Broadband Commission for Digital Development, September 2012, http://www.broadbandcommission.org/Documents/bb-annualreport2012.pdf.

[6] Pando Networks, "Report: U.S. Broadband Speeds Remain Slow, 26th in the World," SiliconFilter, September 20, 2011, http://siliconfilter.com/report-u-s-broadband-still-slow-ranks-26th-in-the-world/.

[7] State Statistics Service of Ukraine, "Average monthly wage by region in 2012," accessed on February 15, 2013, http://www.ukrstat.gov.ua/operativ/operativ2012/gdn/reg_zp_m/reg_zpm12_u.htm.

[8] InMind, "Рост уровня проникновения интернета в Украине существенно замедлился" [Growth of Internet Penetration Level In Ukraine Has Slowed Significantly], AIN.UA, October 19, 2011, http://ain.ua/2011/10/19/62100.

[9] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2012, accessed July 6, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[10] Olga Karpenko, "Смартфоны есть у 14% украинских абонентов, устройств Android втрое больше, чем iPhone" [14% of Ukrainian subscribers own smartphones, Android's share three times that of iPhone,] AIN.UA, February 20, 2013, http://ain.ua/2013/02/20/113303.

[11] Ihor Burdyga, "Операторов свяжут с третьим поколением" [Operators To Be Connected To Third Generation], Kommersant Ukraine, December 12, 2011, http://www.kommersant.ua/doc/1833438.

[12] Dmitry Kuznetsov, "Единственного в Украине 3G-оператора «ТриМоб» опять хотят продать?" [The only 3G operator in Ukraine up for sale again?], August 22, 2012, http://ain.ua/2012/08/22/93759.

There are no known instances of the authorities requiring internet service providers (ISPs) to block any Web 2.0 applications, protocols, or instant messaging tools. The backbone connection of UA-IX (Ukrainian internet exchange, a mechanism of traffic exchange and connection to the wider internet for Ukrainian ISPs) to the international internet is not centralized, and major ISPs each have their own channels that are managed independently.

The Ukrainian telecommunications market is fairly liberal and currently undergoing gradual development. The state previously owned 93 percent of the largest telecom company and top-tier ISP, Ukrtelecom, but in March 2011 the company was privatized.[13] Though no longer state-owned, Ukrtelecom is still the largest ISP in the country and possesses Ukraine's primary network, trunk, and zone telecom lines.[14] Other telecommunications providers are dependent on leased lines, since Ukrtelecom owns the majority of the infrastructure, and many alternative providers do not have sufficient resources to build their own networks. However, Ukrtelecom does not exert any pressure or regulatory control over these other ISPs.

Among the major private ISPs in Ukraine are Volia, Triolan, Vega, and Datagroup; however, major mobile service providers, like Kyivstar and MTS, are also starting to provide broadband internet access.[15] There are about 400 ISPs in Ukraine, according to the State Commission on Communications and Informatization.[16] Regional ISPs are usually smaller local businesses, and regional dominance largely depends on business and other connections in a specific region, making the market prone to corruption.

Ukrchastotnagliad, the Ukrainian frequencies supervisory center, reports that 86 operators have licenses to provide satellite communications services in Ukraine. Companies providing internet access using satellite technologies in Ukraine include Ukrsat, Infocom-SK, Spacegate, Adamant, LuckyNet, Ukrnet, and Itelsat. With the exception of Infocom-SK,[17] all these companies are private.[18] The three major players in the mobile communications market are Kyivstar (owned by Dutch VimpelCom Ltd.), MTS Ukraine (owned by Russian AFK Sistema), and "life:)" (owned by Astelit, whose main shareholders are the Turkish company Turkcell and Ukrainian System Capital Management). Together, these players hold 94.6 percent of the mobile communications market.[19]

There are no obvious restrictions or barriers to entry into the ICT market, but any new business venture, be it an ISP or an internet cafe, faces the usual bureaucracy and corruption, as well as the

[13] 92.8 percent of shares sold to ESU, a Ukrainian subsidiary of the Austrian company EPIC. Source: "Укртелеком продан" [Ukrtelecom Sold], Dengi.Ua, March 11, 2011, http://dengi.ua/news/77761_Ukrtelekom_prodan_.html.
[14] "Ukraine: Country Profile 2010," OpenNet Initiative, December 21, 2010, http://opennet.net/research/profiles/ukraine.
[15] "Количество пользователей широкополосного доступа в Украине достигло 5,6 млн" [Number Of Broadband Internet Users in Ukraine Reaches 5.6 Million], AIN.UA, December 16, 2011, http://ain.ua/2011/12/16/68574.
[16] "Во 2 квартале количество абонентов провайдеров Интернет увеличилось на 6,4%" [In Second Quarter Number Of Subscribers Of Internet Providers Grew By 6.4%], Delo.Ua, July 26, 2007, http://bit.ly/18A2eL4.
[17] Infocom-SK was founded in 1991 jointly by state-owned Ukrtelecom and Controlware, a German telecommunications company. "History," Infocom, accessed on June 15, 2012, http://infocom.ua/catalogue.jsp?catalogueId=3000&cataloguerId=6070&lang=3.
[18] "Ukraine: Country Profile 2010," OpenNet Initiative.
[19] iKS-Consulting, "В Украине почти 55 млн абонентов мобильной связи [Ukraine has almost 55 million mobile subscribers], AIN.UA, July 31, 2012, http://ain.ua/2012/07/31/92177.

legal and tax hurdles common to the Ukrainian business environment. In particular, the Ukrainian ICT market has been criticized for its difficult licensing procedures for operators, and under the 2003 Law on Communications, operators are required to have a license before beginning their activities.

The ICT sector is regulated by the National Commission on Communications and Informatization (NCCIR). Members of the NCCIR are appointed by the president of Ukraine.[20] Due to widespread corruption in the political system and the lucrative nature of business in the ICT sector, appointments to the commission often lack transparency. The NCCIR's work has often been obstructed by claims of non-transparent decisions and operations. For instance, in July 2011 the NCCIR (then the NCCR) refused to prolong the operating license of mobile provider Kyivstar for GSM 900/1800 frequencies.[21] Furthermore, the 2003 Law on Communications does not guarantee the independence of the NCCIR.

A new parliamentary committee on informatization and information technologies was created in December 2012,[22] ostensibly to promote the president's promise of further development of the Ukrainian ICT market.[23] So far, the committee has not made any significant decisions relating to the ICT industry.

LIMITS ON CONTENT

There is no practice of institutionalized blocking or filtering, or a regulatory framework for censorship of content online, although there have been attempts at creating legislation which could censor or limit content. Many of these initiatives present indirect threats to freedom of information online. For example, in September 2012, members of parliament introduced a draft bill which suggested implementing jail sentences of three to five years for cybercrimes such as hacking, cyberscams, and information espionage.[24] Additonally, there were calls to create a national cybersecurity system as part of the strategic law "On the main foundations of development of

[20] National Commission on Regulation of Communications and Informatization, accessed on January 10, 2012, http://en.nkrz.gov.ua/.

[21] "НКРС отказалась продлевать «Киевстар» лицензию на мобильную связь" [NCCR Refused to Prolong Kyivstar's mobile communications license], ITC.ua, July 8, 2011, http://bit.ly/19KAAt3. The NCCR said Kyivstar first acquired their license in 1996 for 15 years under the acting Law on Telecommunications, while in 2004 a new Law on Telecommunications came into power, thus making the old Law (and any agreements under it) void. NCCR believed Kyivstar was not entitled to simply pay 30 percent of the license price to prolong said license, but ought instead to pay 200 percent of the license price to acquire two new licenses for GSM 900 and GSM 1800 each. This would cost Kyivstar around 19 million UAH. As a result, in September 2011 Kyivstar had to pay the full price for two new licenses in order to continue their activities in the market. See also, "Киевстару выдали новые лицензии на мобильную связь" [Kyivstar Given New Mobile Communications Licenses], LigaNet, September 8, 2011, http://bit.ly/164BamS.

[22] "Верховна Рада України прийняла Постанову "Про комітети Верховної Ради України сьомого скликання"" [Ukrainian Parliament adopts Decree "On committees of Parliament of Ukraine, seventh session], Official Parliamentary portal, December 25, 2012, http://iportal.rada.gov.ua/news/Top-novyna/71350.html.

[23] Olga Karpenko, "В парламенте появился комитет, отвечающий за IT-отрасль" [Parliament gets committee to regulate ITC sphere], AIN.UA, December 25, 2012, http://ain.ua/2012/12/25/107173.

[24] Olga Karpenko, "За компьютерные преступления депутаты предлагают сажать на 3 года" [MPs suggest jail sentences for up to 3 years for cybercrimes], AIN.UA, September 19, 2012, http://ain.ua/2012/09/19/95861.

information society in Ukraine for 2007–2015."[25] In some cases, such laws obligate ISPs to remove or block the offensive or illegal content within 24 hours or, if such content is found to be hosted outside of Ukraine, ISPs would have to limit Ukrainian users' access to such content, effectively introducing a practice of filtering content.

The law "On Protection of Public Morals" deals with pornography, eroticism, hate speech, violence, and explicit language, and was amended in October 2011. However, these amendments have been criticized for being overly vague, since they fail to narrowly define what is considered erotic, hateful, or explicit. Critics have argued that the amended law is in violation of Article 10 of the European Convention of Human Rights and the Declaration of Human Rights, both ratified by Ukraine.[26]

Aside from the vague definitions, experts are worried that the law gives extraordinary powers to the National Expert Commission on the Protection of Public Morals (NECPPM), allowing it to issue orders to block websites and online content within 24 hours, without a court order or any means for website owners or content authors to appeal. At the moment, access providers and content hosts are not responsible for the content transmitted or hosted, and may block or require a user to remove content only when provided with a court order. The NECPPM, which has been slated for dissolution since January 2013,[27] is known for outlandish requests and recommendations, such as its letter to the Internet Association of Ukraine (INAU) in March 2013, which stated that the Commission had analyzed the website YouTube.com and discovered content which was immoral and discriminatory. The letter asked INAU to "consider avoiding [the] violation of Ukrainian Internet legislation," but did not specify further action.[28]

In one of the more notable cases of website closure, on August 6, 2012, Ukrainian authorities shut down Demonoid, one of the world's largest bittorrent tracker websites hosted in Ukraine, which was violating Ukraine's copyright laws.[29] Previously, all IP addresses within Ukraine were merely blocked from accessing the site, although the site was still available to outside users and those with circumvention tools. Many media outlets connected the shutdown to First Deputy Prime Minister Valery Khoroshkovsky's visit to the United States,[30] and portrayed it as an attempt to demonstrate

[25] "НКРЗІ пропонує зміни до Закону України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки"" [NCCIR proposes changes to the Law of Ukraine "On the main foundations of development of information society in Ukraine for 2007-2015"], National Commission on Communications and Informatization ffocial website, August 9, 2012, http://nkrzi.gov.ua/uk/activities_nkrzi/news/1344519940/.

26 "Генсек "Репортерів без кордонів" стурбований наміром депутатів обмежити ЗМІ" [Reporters Without Borders General Secretary Concerned With MP's Intention To Limit Mass Media], Ukrainska Pravda, October 28, 2011, http://www.pravda.com.ua/news/2011/10/28/6711923/.

[27] "В Украине ликвидируют Комиссию по морали" [Morals Commission to be liquidated in Ukraine], Segodnya,UA, Jaunary 31, 2013, http://www.segodnya.ua/politics/laws/V-Ukraine-likvidiruyut-Komissiyu-po-morali.html .

[28] Serhiy Pishkovtsiy, "Нацкомісії з захисту моралі не сподобався YouTube" [National Morals Protection Commission does not like YouTube], April 2, 2013, http://watcher.com.ua/2013/04/02/natskomisiyi-z-zahystu-morali-ne-spodobavsya-youtube/ .

[29] Veronica Khokhlova, "Ukraine: Authorities Shut Down BitTorrent Tracker Demonoid," Global Voices, August 14, 2012, http://globalvoicesonline.org/2012/08/14/ukraine-authorities-shut-down-bittorrent-tracker-demonoid/.

[30] Doug Palmer, "UPDATE 2-IMF to visit Ukraine to assess budget-Ukraine official," *Reuters*, August 1, 2012, http://in.reuters.com/article/2012/08/01/imf-ukraine-idINL2E8IVKRK20120801.

Ukraine's tough stance on copyright infringement.[31] In response to Demonoid's closure, the hacktivist group Anonymous launched a series of DDoS attacks on Ukrainian government websites, including the National TV and Radio Broadcasting Council, the Agency for Copyright, and the Anti-Piracy Association.[32]

In February 2013, the weekly news magazine and website *Focus* suddenly removed its latest issue from the website and stalls.[33] Journalists and observers claimed that the issue was removed because of several articles critical of the presidential administration. The four articles in question were dedicated to the third anniversary of the election of President Viktor Yanukovych and contained revealing infographics about the administration's expenses. *Focus*'s editor-in-chief, Yana Moiseenkova, disputed claims of self-censorship, claiming that the removals were due to technical reasons and that the articles would be back online later, although the articles were never returned to the website. Other explanations of why the stories were removed from the website included a speculation that *Focus* was engaging in a self-promotion campaign.

Attempts to manipulate the online news landscape are not numerous, but there are some examples of online media which support certain political figures or political ideas, in addition to progovernment news websites. Some online news websites belong to media holdings owned by oligarchs close to the ruling Party of Regions and other political forces. By and large, though, online media are varied and represent many opinions on the political spectrum, with a key cluster of independent media playing the role of watchdogs and conducting investigative journalism. Political and social issues are discussed freely on internet forums and in the comments on news sites like *Ukrainska Pravda* and *Korrespondent*. Access to international media websites is also unfettered. Prior instances of politically affiliated paid commentators trolling on news websites and social networks did not occur as frequently in 2012–2013.

YouTube, Facebook, Twitter, and international blog-hosting services such as Wordpress and LiveJournal are freely available. Increasingly, Ukrainian politicians are realizing the value of social media, and many have accounts on social media platforms in the hopes of engaging their voters.[34] During the 2012 parliamentary elections, many politicians engaged with voters on their social media platforms.

The Ukrainian blogosphere is fairly active, although less so than the Russian LiveJournal community, which houses many more politically active citizens. Around 60 percent of Ukrainian online users regularly went online in 2012 to use social networks.[35] According to Yandex, in 2011 there were 1.1 million Ukrainian blogs, up from 700,000 in 2010, and blogs are increasingly

[31] Jon Partridge, "Pirate Bay Competitor Demonoid Taken Out as a Present For the US," *Gizmodo*, August 7, 2012, http://www.gizmodo.co.uk/2012/08/pirate-bay-competitor-demonoid-taken-out-as-a-present-for-the-us/.
[32] Steve Ragan, "Anonymous Attacks Ukrainian Government After Demonoid Takedown," *Security Week*, August 8, 2012, http://www.securityweek.com/anonymous-attacks-ukrainian-government-after-demonoid-takedown.
[33] Olga Karpenko, "Журнал «Фокус» снял материалы с сайта из-за цензуры?" [Focus Magazine Removed Articles From Website Because of Censorship?], AIN.UA, February 25, 2013, http://ain.ua/2013/02/25/113849.
[34] Yelena Gladskih, "Как используют блоги украинские политики" [How Ukrainian Politicians Use Blogs], Delo.Ua, February 12, 2011, http://delo.ua/ukraine/kak-ispolzujut-blogi-ukrainski-152081/.
[35] UANet 2012 Digest, Prodigi Digital Agency, December 11, 2012, http://slidesha.re/UxQ5v7.

appearing as a genre of online news websites.[36] In addition, there are about 500,000 Ukrainian Twitter accounts, with a large majority of them in Kyiv.[37] The number of Ukrainian users on Facebook grew from nearly 2 million users as of April 2012 to 2.3 million in December 2012.[38]

Ukrainian bloggers, journalists, NGOs, and citizen activists have been joining forces and creating online projects aimed at scrutinizing government policies, monitoring elections, and uncovering corruption in the higher ranks of power.[39] During the recent parliamentary elections in October 2012, a number of NGOs and civic organizations used online tools to keep the election process transparent and accountable, providing tools for citizens to help monitor the elections. Some of these networks sprung out of the Orange Revolution, but activists are now exploring new tools to fight election corruption. The OPORA civic network, for example, created an interactive map with all 33,000 polling stations, and its 3,800 professional observers documented violations on the map.[40] Regular citizens could also submit reports of violations through an online form.

Another project called "Maidan-monitoring,"[41] launched by the online citizen-activism hub Maidan, used crowd-mapping and the Ushahidi platform to create a map of violations with textual and visual evidence supporting the reports.[42] Maidan-monitoring activists made it a point to verify all incoming information, also calling on election commission members and voters to join the People's Central Election Commission (CEC)[43] and post digital photographs of the final voting protocols that were later posted online in order to prevent any manipulations of the election results.

ElectUA,[44] a nonpartisan crowdsourced election monitoring project by Internews Ukraine, grew out of the practice of using Twitter hashtags to report possible voting violations during previous elections in 2009 and 2010.[45] Voters were able to submit messages to ElectUA in 2012 via e-mail, SMS, and phone, as well as through the project's website, Facebook or Twitter. All three election monitoring websites experienced DDoS attacks on the day of the elections, October 28, 2012.[46]

---

[36] Yandex, "Антон Волнухін, Яндекс «Дослідження української блогосфери 2011»" [Anton Volnukhin, Yandex "Research on Ukrainian Blogosphere 2011"], presented at Microsoft BlogFest 2011, shared by Microsoft Ukraine, November 19, 2011, http://docs.com/G65I.
[37] "Яндекс дружит с Твиттером" [Yandex Gets Friendly With Twitter], Yandex Company Blog, February 21, 2012, http://clubs.ya.ru/company/43938.
[38] Maksym Savanevsky, "Українська аудиторія Facebook в 2012 році зросла на 630 тис" [Ukrainian Facebook Audience in 2012 Grew by 630 Thousand], Watcher.com.ua, December 25, 2012, http://bit.ly/ZxsYKi.
[39] Examples include the New Citizen partnership's initiative ЧЕСНО (Honestly, a movement for transparent and fair parliamentary elections), and PRYAMA DIYA[39] (Direct Action, a movement of student unions organizing street protests on relevant issues).
[40] ELECTIONS 2012. Observation, OPORA network, accessed February 26, 2012, http://map.oporaua.org/en/.
[41] Natalka Zubar, New Interactive Map of Electoral Violations in Ukraine, Maidan.org, July 10, 2012, http://bit.ly/1fRTFP3.
[42] Майдан Моніторинг: Вибори 2012 [Maidan Monitoring: Elections 2012], Maidan, accessed on February 27, 2013, http://maidanua.org/vybory2012/.
[43] Запис до Народної ЦВК [Join the People's CEC], Maidan, accessed on February 27, 2013, http://bit.ly/18eUg9i.
[44] Veronica Khokhlova, Ukraine: Crowdmapping Election Violations, Global Voices, October 26, 2012, http://globalvoicesonline.org/2012/10/26/ukraine-crowdmapping-election-violations/.
[45] "(прес-реліз) 1700 повідомлень про можливі порушення – результат Twitter-трансляції місцевих виборів" [(press-release) 1700 Tweets About Possible Violations – Result of Local Elections Twittercast], Blog of Elections Twittercast Project, November 3, 2010, http://electua.blogspot.com/2010/11/1700-twitter.html.
[46] Tetyana Bohdanova, Ukraine: Election Monitors' Websites Under DDoS Attack, Global Voices, October 28, 2012, http://globalvoicesonline.org/2012/10/28/ukraine-election-monitors-websites-under-ddos-attack/.

The attacks lasted for several hours, and the sites were inaccessible for a period of time, but activists were not able to provide direct proof that these were intentional DDoS attacks.[47]

VIOLATIONS OF USER RIGHTS

The security situation for journalists and online users further declined in 2012–2013. Traditional journalists continue to face regular intimidation and threats of physical violence, although this trend has not been seen as frequently in regard to online journalists. However, in August 2012, a well-known online journalist for the internet publication *Ukrayinska Pravda* was reportedly beaten up by the guards of a member of the Party of Regions. Additionally, during the parliamentary elections in October 2012, there was an increase in the number of DDoS attacks against election monitoring and opposition websites.

The right to free speech is granted to all citizens of Ukraine in Article 34 of the constitution, although the article also specifies that the state may restrict this right in the interest of national security or public order. In practice, this right has been frequently violated. Part three of Article 15 of the constitution forbids censorship, though this norm is routinely violated, with especially grave violations observed during the time of President Leonid Kuchma, who served before the 2004–2005 Orange Revolution. In addition, Article 171 of the criminal code provides fines and detention sentences for obstructing journalists' activity. The Ukrainian judiciary, however, is prone to the same level of corruption evident in other branches of power. Many businesses, including media companies, often resort to bribes to influence the consideration of their affairs in the courts.[48]

In 2011, online journalists achieved similar status and privileges as traditional journalists, such as being able to obtain accreditation for parliamentary sessions and other official meetings frequented by the press. Nevertheless, there has been an ongoing discussion about the need for online media to register, with some suggesting that registration would provide additional mechanisms for protecting journalists, while others refute this idea, considering any form of registration to be an impediment to press freedom and internet freedom.[49]

On September 18, 2012, a draft bill calling for up to five years of jail time for defamation (both offline and online) passed the first reading in the parliament.[50] The bill caused a wave of indignation from Ukrainian journalists and activists, and international organizations such as Reporters Without Borders appealed to the parliament to reconsider adopting the bill that would recriminalize

[47] OPORA Citizen Network (Facebook page), October 28, 2012, https://www.facebook.com/cn.opora/posts/10151093684415108.

48 "Судова реформа не розвіяла сутінків у бізнес-настроях" [Judiciary reform does not banish twilight in business mood], *Deutsche Welle*, June 1, 2012, http://www.dw.de/dw/article/0,,15992775,00.html.

[49] Ukrainian Internet Association, "Підсумки прес-конференції: "Саморегулювання вітчизняних електронних медіа як альтернатива державному регулюванню в Українському сегменті Інтернет" [Summary of Press-Conference: "Self-regulation of Ukrainian Electronic Media As An Alternative To State Regulation In The Ukrainian Internet Segment"], InAU (Ukrainian Internet Association), July 19, 2011, http://www.inau.org.ua/170.3675.0.0.1.0.phtml.

[50] Tetyana Bohdanova, "Ukraine: Protesting the Controversial Defamation Bill," Global Voices, September 29, 2012, http://globalvoicesonline.org/2012/09/29/ukraine-protesting-the-controversial-defamation-bill/.

defamation.[51] A number of online media outlets and active online users launched a wide-reaching campaign against the defamation bill, creating a Facebook group with over 7,700 members, placing stark banners on the front pages of many media outlets, and posting calls to "Say 'No' to Defamation Law" throughout social networks.[52] As a result of the campaign pressure, the bill was rejected at its final reading on October 2, 2012.[53] However, some pointed out that Vitaly Zhuravsky, a member of parliament (MP), might have agreed to recall the draft bill to improve his chances in the coming parliamentary elections.[54]

In June 2012, a criminal investigation was initiated against the news website *Levy Bereg* (*Left Bank*), reportedly upon request of MP Volodymyr Landyk, who claimed the website published his private text messages without his consent.[55] Sonya Koshkina, the editor-in-chief of *Levy Bereg*, temporarily left the country, citing pressure and fears for her life. Koshkina claimed she would not return until the criminal investigation was dropped.[56] The Kyiv Prosecutor's Office later dropped the case, citing that "there was no significant harm done by the publication to the claimant."[57]

There is no obligatory registration for either internet users or mobile phone subscribers. Nevertheless, the pervasiveness of extralegal surveillance of Ukrainians users' activities is unclear. From 2002 to 2006, mechanisms for internet monitoring were in place under the State Committee on Communications' Order No. 122, which required ISPs to install so-called "black-box" monitoring systems that would provide access to state institutions. This was mainly done to monitor the unsanctioned transmission of state secrets. Caving to pressures from public protests and complaints raised by the Internet Association of Ukraine and the Ukrainian Helsinki Human Rights Union, the Ministry of Justice abolished this order in August 2006. Since then, the Security Service has seemingly acted within the limits of the Law on Operative Investigative Activity, and must obtain a court order to carry out surveillance.[58] At the same time, some human rights groups are concerned that the Security Service is still keeping intercepted messages and carrying out internet surveillance on a large scale.[59]

Physical attacks against online journalists and activists are rare; however, the intimidation and harassment of traditional journalists is a regular occurrence. In August 2012, the activist Mustafa

[51] "In Victory for Journalists, Recriminalization of Defamation Rejected," Reporters Without Borders, October 2, 2012, http://en.rsf.org/ukraine-appeal-on-parliament-about-02-08-2012,43153.html.
[52] "Скажи ні закону про наклеп. Це стосується кожного" [Say 'No' to Defamation Law. This is Everyone's Business], Facebook group, accessed on Febryary 27, 2013, https://www.facebook.com/groups/naklep/members/.
[53] "In Victory for Journalists, Recriminalization of Defamation Rejected," Reporters Without Borders, October 2, 2012, http://en.rsf.org/ukraine-appeal-on-parliament-about-02-08-2012,43153.html.
[54] Tetyana Bohdanova, "Ukraine: Protesting the Controversial Defamation Bill," Global Voices, September 29, 2012, http://globalvoicesonline.org/2012/09/29/ukraine-protesting-the-controversial-defamation-bill/.
[55] Olga Karpenko, "В отношении интернет-издания LB.ua возбуждено уголовное дело (дополнено)" [Criminal Case Started Against Online Publication Levy Bereg (updated)], AIN.UA, July 17, 2012, http://ain.ua/2012/07/18/91273.
[56] "Соня Кошкіна виїхала з України" [Sonya Koshkina Has Left Ukraine], Ukrainska Pravda, June 30, 2012, http://www.pravda.com.ua/news/2012/06/30/6967733/.
[57] "Повідомлення" [Notification], Kyiv Prosecutor's Office official website, August 3, 2012, http://www.kyiv.gp.gov.ua/ua/news.html?_m=publications&_c=view&_t=rec&id=109821.
[58] "Ukraine: Country Profile 2010," OpenNet Initiative.
[59] Kharkiv Human Rights Group, "Права людини в Україні - 2006. V. Право на приватність" [Human Rights in Ukraine in 2006. V. Privacy Rights], Human Rights in Ukraine, March 5, 2010, http://www.khpg.org/index.php?id=1186147137.

Nayyem, who is a well-known TV and online journalist, was on his way to a Party of Regions congress when he was attacked by the guards of a party member.[60] The Prosecutor's Office in Kyiv has started an investigation into the attack, in which Nayyem was beaten and had his phone stolen.

In March 2013, Andriy Dzindzya, a journalist with *Road Control*, an online crowdsourcing website documenting road police corruption, was arrested on charges of hooliganism—a common charge for activists in Ukraine.[61] Earlier, in February 2012, journalists from *Road Control* had an altercation with police. After other journalists and NGO activists arrived at the police station, Dzindzya was released on bail. Observers claimed his arrest was unwarranted, as were the hooliganism charges.[62]

On March 22, 2013, police officers arrived at the offices of the website Censor.net and claimed they had a warrant, based on a preliminary investigation, to obtain information about the website's users. They were unable to present any proof or documentation, but threatened to remove the servers from the office.[63] Further comments from the local cybercrime division officials indicated that police had acted due to a post on an online forum and comments on Censor.net criticizing a local judge for parking her car illegally in the backyard of her apartment complex.[64] The judge then instigated criminal proceedings to determine who was criticizing her on the website. Censor.net reported the actions and alleged motivations of the police on its website, after which the police dropped the matter.

Cyberattacks are not very common in Ukraine, although some recent cases were recorded during the parliamentary elections of October 2012. Several crowdsourced election monitoring websites were attacked,[65] as well as the websites of opposition parties.[66]

In March 2013, several regional news websites reported that they had been the victims of DDoS attacks. Three outlets based in Cherkassy—*Procherk*, *Provintsiya* and *Dzvin*—were taken down on March 6, 2013 during President Yanukovich's visit to the region. According to *Procherk* editor Nazariy Vivcharyk, their website was also subject to cyberattacks during most of the day.[67]

---

[60] "Мустафа Найем рассказал, кто его избил на съезде Партии регионов" [Mustafa Nayyem Told Of Who Beat Him Up At The Party Of Regions Congress], ZN.UA, August 3, 2012, http://bit.ly/18A2lpT.
[61] "Журналіста "Дорожнього контролю" арештували за рішенням суду – міліція" [Road Control Journalist Arrested on Court Warrant – Police], Ukrainska Pravda, March 15, 2013, http://www.pravda.com.ua/news/2013/03/15/6985666/.
[62] "Суд відпустив журналіста "Дорожнього контролю" під заставу" [Court Releases Road Control Journalist on Bail], Ukrainska Pravda, March 19, 2013, http://www.pravda.com.ua/news/2013/03/19/6985900/.
[63] "Міліція посягала на сервер інтернет-видання через коментарі про суддю" [Police threatened to remove server of online news outlet because of comments about a judge], Ukrainska Pravda, March 28, 2013, http://bit.ly/16U1vAO.
[64] "Судья хозяйственного суда Жанна Александровна Бернацкая своим джипом порше кайен демонстративно и нагло не дает выехать никому со двора. Как бороться с такими уродами?" [Economic court judge Zhanna Aleksandrovna Bernatskaya blocks exit from yard for everyone with her Porshe Cayenne jeep. How do we fight such bastards?], Censor.net, February 12, 2013, http://bit.ly/14rbjFe.
[65] Tetyana Bohdanova, "Ukraine: Election Monitors' Websites Under DDoS Attack," Global Voices, October 28, 2012, http://globalvoicesonline.org/2012/10/28/ukraine-election-monitors-websites-under-ddos-attack/.
[66] Maksym Savanevsky, "Сайти Тимошенко, Фронту Змін, Гриценка лягли під DDoS атакою (оновлено)" [Websites of Tymoshenko, Front Zmin, Hrytsenko Down Under DDoS Attack (updated)], Watcher.com.ua, October 28, 2012, http://watcher.com.ua/2012/10/28/sayty-tymoshenko-frontu-zmin-hrytsenka-lyahly-pid-ddos-atakoyu/.
[67] "Барометр свободи слова за березень 2013 року" [Freedom of Speech Barometer for March 2013], IMI, April 3, 2013, http://imi.org.ua/barametr/40525-barometr-svobodi-slova-za-berezen-2013-roku.html.

UNITED ARAB EMIRATES

	2012	2013
INTERNET FREEDOM STATUS	N/A	NOT FREE
Obstacles to Access (0-25)	n/a	13
Limits on Content (0-35)	n/a	22
Violations of User Rights (0-40)	n/a	31
Total (0-100)	**n/a**	**66**

* 0=most free, 100=least free

POPULATION: 8.1 million
INTERNET PENETRATION 2012: 85 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The state continued to block certain political and social websites, as well as pornography, gambling sites, and other content deemed offensive to public order, religion, or morality (see **LIMITS ON CONTENT**).
- The new cybercrime law introduced in 2012 outlined harsh punishments for users who post content that is critical of the state, is offensive to religion, or violates another's right to privacy (see **VIOLATIONS OF USER RIGHTS**).
- Scores of users were detained and given 7 to 15 year sentences for their online activity, including several belonging to the so-called "UAE 94" group of political detainees (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

The government of the United Arab Emirates (UAE) has embraced information and communications technology (ICT) as a means of developing a competitive economy and improving citizen services. The internet was introduced to the country in 1995 and internet penetration has quickly risen.[1] The UAE is ranked 25th in the World Economic Forum's 2013 Networked Readiness Index[2] and scored 28th in the United Nations 2012 E-Governance Survey.[3] However, while remaining open to receiving large amounts of foreign investment and expatriate workers, the government has actively fought to deter political discussions, demands for reforms, and criticism of public officials online.

The wealthy Gulf state has taken several moves to restrict access to online tools that challenge the government's authoritarian grip on both politics and telecommunications. Numerous websites are blocked and search results are filtered in order to prevent access to local and international voices that differ from the state line, particularly on political, religious, and sexual matters. Responding to the growing use of social media to call for political reforms and document government abuses, a new cybercrime law was issued in 2012. The law provides harsh punishments for a wide range of vague offenses, such as criticizing the country's rulers and religion. These laws, combined with a judiciary that fundamentally lacks independence, create a highly problematic legal environment where users cannot be guaranteed that their constitutional and internationally recognized rights will be upheld.

The first reported instance of law enforcement bodies targeting ICT use for political motives occurred in July 2010, when an 18-year-old named Badr al-Dhohri was held in Abu Dhabi for using his Blackberry to pass along a message that called for a protest against increases to the price of gasoline. Later, a man named "Saud" was arrested for organizing the unsuccessful protest, while five other citizens were summoned for investigation.[4] As for online users, two members of the online discussion forum UAE Hewar were arrested in April 2011 in one of the first documented cases in the country. One of those detained was the prominent blogger and activist Ahmed Mansoor, whose arrest sparked online campaigns calling for his release. A third user was arrested for criticizing the authoritarian practices of Gulf governments.[5]

More recently, dozens have been detained for their political discussions on online forums and social media. Many have indicated that they were held without charge, denied the right to an attorney,

[1] Internet in UAE. International Telecommunications Union. 2001. Accessed June 25, 2013, http://www.itu.int/arabinternet2001/documents/pdf/document25.pdf
[2] Benat Bilbao-Osorio, Soumitra Dutta, Bruno Lanvin, eds. "The Global Information Technology Report 2013," World Economic Forum, accessed June 6, 2013, http://www.weforum.org/reports/global-information-technology-report-2013/.
[3] United Nations Public Administration Network. "Emirates global leader in e-Readiness, says UN eGovernment Survey 2012." May 15, 2012. http://www.unpan.org/PublicAdministrationNews/tabid/651/mctl/ArticleView/ModuleID/1555/articleId/31395/default.aspx
[4] Reporters Without Borders. "Wave of Arrests of Blackberry messenger users." 29 July 2010. http://en.rsf.org/united-arab-emirates-wave-of-arrests-of-blackberry-29-07-2010,38048.html
[5] Reuters. "Arrested UAE blogger accused of possessing alcohol." April 12, 2011. http://www.reuters.com/article/2011/04/12/us-emirates-activists-idUSTRE73B2EP20110412

and tortured. Mobile phones must be registered and—for most of the coverage period—Voice-over-Internet-Protocol (VoIP) applications were banned to facilitate government monitoring and protect the state's monopoly on phone services. The country's two mobile phone and internet service providers are either directly or indirectly owned by the state, reflecting a lack of checks and balances in government requests for surveillance data. Numerous crackdowns on users have increased self-censorship on social media and online news outlets, of which the most prominent are government-owned.

Some Emiratis have continued to push back against government repression and intimidation by channeling their strong digital literacy into online activism, writing blogs and calling for political reform on social networks. In the face of prosecution, activists still use online tools to highlight human rights violations and pass on messages from relatives in prison. Nonetheless, the online environment in the UAE is not free, and users face many challenges to freedom of expression online.

OBSTACLES TO ACCESS

Similarly to other Gulf States, Emirati users enjoy a robust information and communications technology (ICT) infrastructure and high connection speeds. In the International Telecommunication Union's (ITU) 2012 ICT Development Index, the UAE ranked 45th in the world and among the top five in the region.[6] The number of internet users has risen rapidly from a penetration rate of 61 percent in 2007 to 85 percent in 2012.[7] As of April 2013, there were 997,675 internet subscribers, 99 percent of which had broadband connections.[8]

While the use of broadband is widespread, prices are extraordinarily high; the UAE has one of the most expensive broadband rates in the world, with high-end subscriptions costing more than AED 8,000 ($2,178) a year. However, the UAE ranks 29th in the ITU's 2012 ICT Price Basket Index, in which local broadband prices are measured against gross national income (GNI) per capita.[9] This reflects a sense that despite the high prices, the internet remains affordable for most Emiratis, though not necessarily to all migrant workers. Prices have been steadily dropping in recent years and,[10] in May 2012, the telecommunications company Etisalat announced a further 50 percent cut in broadband subscription costs.[11]

[6] International Telecommunication Union (ITU), "Measuring the Information Society 2012 – ICT Development Index (IDI)", accessed June 7, 2013, available at http://www.itu.int/ITU-D/ict/publications/idi/material/2012/IDI-ranking.pdf.
[7] International Telecommunication Union (ITU), "Percentage of individuals using the Internet," 2001 and 2012, accessed June 2, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[8] Telecommunications Regulatory Authority. "Latest Statistics." Accessed July 2, 2013. http://www.tra.gov.ae/latest_statistics.php
[9] International Telecommunications Union (ITU), "Measuring the Information Society," 2012, available at http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf.
[10] Ben Flanagan. "UAE subscribers paying high price for broadband." Aug 16, 2011 http://www.thenational.ae/business/technology/uae-subscribers-paying-high-price-for-broadban
[11] "Etisalat to cut broadband rates by 50%." Emirates 24/7. May 20, 2012. http://www.emirates247.com/news/emirates/etisalat-to-cut-broadband-rates-by-50-2012-05-20-1.459470

The UAE has one of the highest mobile phone penetration rates in the region with nearly 170 percent or 11.7 million subscribers in 2012.[12] Out of 26 countries that participated in a Google survey of smartphone penetration, the UAE was ranked first, with 61 percent of mobile phone users reporting that they own smartphones.[13]

According to UNICEF, literacy in the Emirates was reported at 94 percent among males and 97 percent among females, thereby not constituting a strong obstacle to internet use.[14] In 2006, the country decided to include computer laboratories in public schools, thereby seeking to improve computer literacy among the youth.[15]

The two internet service providers (ISPs) in the UAE are "Etisalat" and "du." Both companies have launched their own carrier-neutral international internet exchange points, Smarthub and Datamena, respectively.[16] Cuts to undersea cables have disrupted internet access for Emirati users on several occasions, though government-instituted outages are not known. In March 2013, Etisalat warned that users would face slower speeds due to the cutting of a fiber-optic cable off of the Mediterranean coast of Egypt.[17] Du suffered similar disruptions in April 2010 and March 2011 due to cuts to the SEA-ME-WE 4 cable.[18] In 2008, 1.7 million users in the UAE were affected by undersea damage to submarine cables occurring at five separate locations around the globe.[19]

Both telecommunications companies are, directly or indirectly, owned by the state. The UAE government maintains a 60 percent stake in Etisalat through its ownership in the Emirates Investment Company,[20] while a majority of du is owned by various state companies.[21] Etisalat used to dominate the telecommunication market until 2006, when du was granted a working license. Since 2006, no new providers have been licensed, though there is no information on whether new applications were submitted. The two companies are also the major mobile phone operators. Providers fall under the laws and regulations set by the TRA, which has been headed by Mohamed Nasser Al Ghanim since its establishment in 2004. Its tasks include licensing, conducting surveys, promoting investment, and assigning websites to the ".ae" top-level country domain.[22]

---

[12] International Telecommunication Union (ITU), "Percentage of individuals using mobile cellular telephones," 2012, accessed June 2, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[13] Google. "Our Mobile Planet: United Arab Emirates." Accessed April 20, 2013. http://bit.ly/MOD7dt.
[14] UNICEF. "United Arab Emirates: Statistics." Accessed at June 25, 2013. http://uni.cf/lgxga0.
[15] Library of Congress – Federal Research Division. "Country Profile: United Arab Emirates (UAE)," July 2007, http://lcweb2.loc.gov/frd/cs/profiles/UAE.pdf.
[16] "Etisalat launches internet exchange hub," CommsMEA, November 19, 2012, http://bit.ly/1hfcJEE.
[17] Claire Valdini. "UAE Etisalat users face disruption after cable cut," Arabian Business, March 28, 2013. http://www.arabianbusiness.com/uae-etisalat-users-face-disruption-after-cable-cut-495772.html
[18] SeaMeWe-4 refers to the South East Asia – Middle East – Western Europe – 4 cable. Hassan Hassan. "Cable cut may slow internet," The National, March 27, 2011. http://www.thenational.ae/news/uae-news/cable-cut-may-slow-internet
[19] Asma Ali Zain. "Cable damage hits 1.7m Internet users in UAE," Khaleej Times, February 5, 2008. http://bit.ly/1dS8tLD.
[20] Maher Chmaytelli, "Etisalat Plans to Allow Foreigners 'Soon,' Khaleej Says," Bloomberg, July 29, 2012, http://www.bloomberg.com/news/2012-07-29/etisalat-plans-to-allow-foreigners-soon-khaleej-says.html.
[21] du, "Shareholders structure," accessed June 7, 2013, http://www.du.ae/en/about/corporate-governance/shareholders.
[22] Telecommunications Regulatory Authority. "TRA's Board of Directors Endorses Several ICT Policy Issues and Approves the Authority's Budget for 2010," January 6, 2010. http://www.tra.gov.ae/news_TRA%92s_Board_of_Directors_Endorses_Several_ICT_Policy_Issues_and_Approves_the_Authority%92s_Budget_for_2010-135-36.php

LIMITS ON CONTENT

Online censorship has increased in the UAE following the Arab uprisings of 2011. The authorities have blocked numerous websites and web forums where users openly call for political reforms or criticize the government. While self-censorship is pervasive, the ongoing crackdown against online dissent points to the fact that a limited number of users continue to use their real names when addressing sensitive issues. The families of political detainees use social media to highlight human rights abuses and communicate on behalf of their loved ones. Twitter, for example, is highly important in an online media landscape that is dominated by state-run news sites that refuse to cover controversial trials or stray too far from the state's overall narrative. These factors contribute to a highly-controlled online environment in which freedom of expression and the right to information is not respected.

The availability of VoIP services in the UAE is shrouded in doubt and disputes between the country's two telecommunications companies, Etisalat and du, and the TRA. In the past, many aspects of VoIP applications were blocked by both providers and Skype was classified by the TRA as an "unlicensed VoIP." When users landed on the Skype website, a notice appeared stating, "Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy."[23] Similar products such as Viber or Apple's Facetime were also banned; [24] in fact, Apple agreed to sell its iPhone4 products to UAE mobile phone companies without the Facetime application preinstalled.[25] However, on numerous occasions the TRA has emphasized that it is up to the mobile phone providers to license these products. Etisalat and du currently offer their own prepaid VoIP cards, although their prices are higher than those listed by Skype.

Changes arrived on March 19, 2013, when du subscribers suddenly reported no obstacles in accessing the Skype website or in making Skype-to-phone calls. Etisalat announced that it would follow suit one month later.[26] After initial reports from the TRA indicated that Skype users could still face fines of AED 1 million ($272,000) or two years imprisonment, the regulatory denied that it had made these statements and reiterated that the availability of Skype is a matter for the two telecommunications companies.[27] BlackBerry services have been restricted since 2010, when the government introduced a regulation allowing only companies with more than 20 BlackBerry

[23] Kyle Sinclair, "Mobile subscribers in UAE get access to Skype calls, but for how long," The National, March 20, 2013, http://www.thenational.ae/news/uae-news/mobile-subscribers-in-uae-get-access-to-skype-calls-but-for-how-long.
[24] "Viber seeks to circumvent ban in Midle East," The National, June 10, 2013, http://www.thenational.ae/news/uae-news/viber-seeks-ways-to-circumvent-ban-in-middle-east.
[25] Reporters Without Boarders. "Countries Under Surveillance: United Arab Emirates." March 11, 2011. http://en.rsf.org/united-arab-emirates-united-arab-emirates-11-03-2011,39760.html
[26] Matt Smith, "UAE telco Etisalat says unblocks Skype website," Reuters, April 8, 2013, http://www.reuters.com/article/2013/04/08/us-emirates-etisalat-skype-idUSBRE9370HO20130408.
[27] Colin Simpson, "UAE Skype users will not face jail or Dh1 million fine, confirms telecom regulator," The National, May 12, 2013, http://www.thenational.ae/news/uae-news/uae-skype-users-will-not-face-jail-or-dh1-million-fine-confirms-telecom-regulator.

accounts to access the encrypted BlackBerry Messenger service.[28] Despite these limitations, circumvention software and proxies are commonly used by Emiratis to access blocked content[29] and VoIP services.[30]

While the TRA has claimed that it is not chiefly responsible for the unavailability of VoIP, the regulator does instruct ISPs to block content related to terrorism, pornography, and gambling, as well as websites that contain political speech threatening to the ruling order. According to a recent report from CitizenLab, ISPs in the UAE have used tools such as SmartFilter and NetSweeper to censor content. CitizenLab also found five installations of Blue Coat ProxySG in the country's network linked to Etisalat.[31] Although YouTube, Facebook, Twitter, and international blog-hosting services are freely available, controversial terms are often filtered from search results within these sites.

The TRA, working with the Ministry of Communications, has also blocked five hundred search terms.[32] For example, a Twitter user reported that a web forum on atheism, offered on the popular site Reddit, is blocked in the UAE.[33] Specific searches on the photo-sharing website Flickr are also filtered. In December 2012, searches for the Egyptian comedian and television host Bassem Youssef resulted in a generic error message, leading Twitter users to speculate that this was a result of the letters "a-s-s" appearing in the comedian's first name. Etisalat responded to the criticism by tweeting that users can submit a request for the content to be unblocked and provided a link to the "Contact Us" page of the Etisalat website. The videos have since been unblocked.[34] In September 2012, the controversial "Innocence of Muslim" film trailer was made inaccessible on YouTube.[35] A BBC report on detained Emirati activists was also blocked in July 2012, though access to other parts of the BBC website was not affected.[36]

According to Herdict, the crowdsourcing tool that lets users report blocked content, internet users from the UAE have reported several social, political, LGBTQ, and proxy sites blocked in their country.[37] For example, the Lebanese queer and feminist e-magazine *Bekhsoos*[38] and the U.S.-based Arab Lesbian e-magazine *Bint El Nas* are both blocked.[39] Many websites displaying religious content

[28] "Use of Most Secure BlackBerry System Restricted, Blogger Arrested." Reporters Without Borders. April 28, 2011. http://en.rsf.org/united-arab-emirates-use-of-most-secure-blackberry-28-04-2011,40123.html
[29] Stuart Turton, "Dubai's dubious internet censorship," September 6, 2010, http://www.pcpro.co.uk/blogs/2010/09/06/dubais-dubious-internet-censorship/
[30] Triska Hamid, "Telecoms revenues threatened by Skype," The National, April 10, 2013, http://www.thenational.ae/business/industry-insights/telecoms/telecoms-revenues-threatened-by-skype.
[31] "Appendix A: Summary Analysis of Blue Coat 'Countries of Interest'," CitizenLab, January 15, 2013, https://citizenlab.org/2013/01/appendix-a-summary-analysis-of-blue-coat-countries-of-interest/.
[32] Reporters Without Borders. "Countries Under Surveillance: United Arab Emirates," accessed in June 25, 2013, http://en.rsf.org/surveillance-united-arab-emirates,39760.html
[33] https://twitter.com/vbentley/status/326696995546882049
[34] https://twitter.com/SultanAlQassemi/status/283315170598596608
[35] Daniel Shane. "Access to anti-Islam film blocked in UAE." September 18, 2012. http://www.arabianbusiness.com/access-anti-islam-film-blocked-in-uae-473462.html
[36] https://twitter.com/ECHRIGHTS/status/230334658129321985
[37] Herdict. Quick Stats: United Arab Emirates. Accessed April 28, 2013. http://www.herdict.org/explore/indepth?fc=AE
[38] http://www.bekhsoos.com/web/
[39] http://www.bintelnas.org/

are blocked, including the famous blog of atheist Emirati blogger Ben Kerishan[40] and an Arab Christian online forum named The Church Network.[41]

In the past two years, political content has been the focus of state censorship. Examples include the Arab-American News website *Arab Times*,[42] the secular pan-Arab online forum "Modern Discussion,"[43] and the California-based Arabic online newspaper *Watan*, all blocked in September 2012.[44] A website disseminating news of the trial of 94 Emirati political detainees was also blocked in 2013.[45] The anonymous website "UAE University Watch"[46] and "UAE Prison," which exposes violations against jailed expatriates, have both been blocked.[47] "Emaraty Bedoon," the blog of the stateless individual Ahmed Abdulkhaleq who was deported to Thailand in July 2012 for his political activism, is also blocked.[48]

Authorities continue to ban inactive sites such as the political forum "UAE Hewar" and the blogs "Secret Dubai Diary"[49] and "UAE Torture."[50] The latter posted a torture video taken in 2004 in which a member of the ruling family was shown to have tortured an Afghan man. The suspect was acquitted in 2010 in a case that was widely believed to be a show trial.[51] A request to unblock UAE Hewar was rejected by the Federal Supreme Court in July 2012, [52] and its Facebook page is also blocked due to its criticism of the regime and state corruption.[53] As part of a verdict, in which five users were sentenced 7 to 15 years for violating the constitution and cooperating with foreign political organizations (see "Violations of User Rights"), a court also ordered the blocking of five websites that are already inaccessible in the country. These included the Emirates Media and Studies Center (EMASC); The Seven Emirates, which focuses on the seven activists who had their citizenship revoked for their political activities; the Watan news website; the Islah political group website; and the Yanabeea.net educational network.[54]

Under the 2012 cybercrime law, website owners and employees "may be held liable" for any violations occurring on their sites, including defamation charges.[55] In May 2012, Dubai police

[40] http://benkerishan.blogspot.com/
[41] http://www.arabchurch.com/
[42] http://www.arabtimes.com/
[43] http://www.ahewar.org/
[44] ANHRI. "Kuwait: News website blocked." March 22, 2012. http://beta1.anhri.net/en/?p=7521
[45] The Arabic Network for Human Rights Information. "UAE: ANHRI Denounces Blocking a Website Address the News of the Detainees." April 18, 2013. http://www.anhri.net/en/?p=12262
[46] http://www.uaeuniversitywatch.net/
[47] http://uaeprison.com/
[48] http://www.emaratybedoon.blogspot.com/
[49] http://secretdubai.blogspot.com/
[50] http://www.uaetorture.com/
[51] Mackey, Robert. "Abu Dhabi Royal Acquitted in Torture Trial." January 11, 2010. http://thelede.blogs.nytimes.com/2010/01/11/abu-dhabi-royal-acquitted-in-torture-trial/
[52] Magdy Zahr el-Dine, "Appeal Rejected to Unblock Website," Al-Khaleej, 5 July, 2011. http://www.rakland.net/vb/showthread.php?t=7458
[53] Reporters Without Boarders. "Countries Under Surveillance: United Arab Emirates." March 11, 2011. http://en.rsf.org/united-arab-emirates-united-arab-emirates-11-03-2011,39760.html
[54] "68 members of Islah jailed for terrorism," AlShahed newspaper, July 3, 2013. http://www.alshahedkw.com/index.php?option=com_content&id=95366:---68-----&Itemid=457
[55] Awad Mustafa and Ramona Ruiz. "Cyber-crime law to fight internet abuse and protect privacy in the UAE." November 13, 2012. http://www.thenational.ae/news/uae-news/cyber-crime-law-to-fight-internet-abuse-and-protect-privacy-in-the-uae

succeeded in shutting down 15 accounts on Facebook and Twitter for "defamation and abuse" by sending letters to both companies outlining the offenses committed under the UAE law.[56] In a case dating from July 2009, a court suspended the website and newspaper *Al Emarat Al Youm* for 20 days for running a story about the doping of a race horse owned by two sons of the country's president.[57]

Decisions to block or remove online content often lack procedural transparency or judicial oversight. The telecommunications company du details what criteria it used to block websites in a document available on its website. Prohibited content includes information related to circumvention tools, the promotion of criminal activities, the sale or promotion of illegal drugs, dating networks, pornography, homosexuality, gambling, phishing, spyware, unlicensed VoIP services, terrorism, and material that is offensive to religion. [58]

No similar list was made available by Etisalat, although the company does have a space on its website where users can request that a website be blocked or unblocked.[59] In 2005, an Etisalat spokesman stated that the company is not responsible for internet blocking and revealed that all complaints and requests are passed on to the Ministry of Information. He also claimed that a list of websites to be blocked is compiled by an American company and then implemented through a proxy server.[60] Apart from the previously mentioned unblocking of Bassem Youssef's videos, incidents of users successfully unblocking a website are not known.[61] Indeed, writing in an online forum, users have noted that their requests to have websites unblocked did not receive any response from companies.[62]

Local news websites, many of which are owned by the state, employ a large degree of self-censorship in accordance with government regulations and unofficial "red lines." Gulf News, The National, and Emirates 24/7 are among the different online media outlets suffering such restrictions. Nonetheless, since the regional uprisings of 2011, Emiratis have begun to tackle sensitive issues more boldly over the internet, particularly on social media. Users express their opinions, share information on arrests and trials, and even attempt to organize protests. However, most users remain anonymous when criticizing state officials or religion out of fears of legal action or harassment. While there is no available evidence to prove the government's involvement in hiring public relations firms or bloggers to spread propaganda, a large number of anonymous Twitter users appear dedicated to harass and intimidate political dissidents and their families online.

---

[56] http://www.huffingtonpost.com/2012/05/21/dubai-facebook-twitter-accounts-shut-down_n_1533633.html
[57] Reporters Without Borders. "Newspaper Suspended for 20 Days Over story Race Horse." July 7, 2009. http://en.rsf.org/united-arab-emirates-newspaper-suspended-for-20-days-07-07-2009,33730
[58] Du, "Prohibited Content Categories," July 29, 2008. http://www.du.ae/Documents/Annex%201-IAM%20Regulatory%20Policy%20ver%201%200%2029July2008.pdf
[59] Etisalat. "Blocking and Unblocking Internet Content." Accessed on April 28, 2013. http://www.etisalat.ae/eportal/en/corporate/blocking-unblocking.html
[60] Piers Grimley Evans. "Etisalat doesn't block websites," Gulf News, July 21, 2005. http://gulfnews.com/news/gulf/uae/media/etisalat-doesn-t-block-websites-1.294723
[61] https://twitter.com/SultanAlQassemi/status/283315170598596608
[62] Expat Forum, "Do you ever request Etisalat or Du to unblock websites?" March 24, 2011. http://bit.ly/18FPnVR.

In addition to the threat of harassment and prosecution, Emirati authorities also use financial means to limit the ability of antigovernment websites to produce content online. For example, the government reportedly pressured Dubai-based advertising agency "Echo" to end its advertising contract with the U.S.-based news outlet Watan. A complaint was also allegedly submitted to the FBI against the website, claiming it calls for the assassination of UAE rulers.[63] Nonetheless, users have access to a variety of local and international news outlets, even if there are disparate reports of blocking specific UAE-related articles from these sites.[64]

Social media use has increased in recent years, in line with regional trends. Facebook recently hit 3.4 million users in the UAE, representing a penetration of 68 percent,[65] while in 2013, 34 percent of all users possessed a Twitter account.[66] While the UAE did not witness protests on a scale similar to its Arab neighbors, Emiratis created petitions calling for reforms and conducted online activism to expose corruption and demand change. Currently, families of political prisoners rely on Twitter to speak on behalf of detainees, explaining their cases, spreading information about violations to their rights, and calling for their release. There are several examples of relatives who are active online, including Mariam al-Mansouri,[67] the wife of detained blogger Rashid al-Shamsi, and Aysha al-Thufiri, the daughter of detainee Salih al-Thufiri.[68] Social media networks have also proven useful in non-political campaigns, such as fundraising attempts to provide support to Syrian refugees.

VIOLATIONS OF USER RIGHTS

The rights of online users in the UAE are not protected by law, nor are they respected in practice. Several laws, including the penal code, publishing law, and cybercrime law, are commonly exploited to deter free expression and violate the rights of users. There is a general feeling among those who reside in the UAE that online tools are monitored and that surveillance is widely practiced with little judicial oversight. Several prominent online activists and ordinary citizens were detained in late 2012 and early 2013. In addition, this year saw numerous cases of torture, solitary confinement, and physical harassment registered against users.

Article 30 of the country's constitution states that "Freedom of opinion and expressing it verbally, in writing or by other means of expression shall be guaranteed within the limits of law."[69] However, the judicial system in the Emirates lacks independence and prosecutions are often

[63] ANHRI. "UAE Continues its Serious Violations Against the Freedom of Opinion and Expression due to Blocking "Watan" Website." September 24, 2012. http://beta1.anhri.net/en/?p=9607
[64] https://twitter.com/ECHRIGHTS/status/230334658129321985
[65] "United Arab Emirates Facebook Statistics," Socialbakers, accessed April 20, 2013. http://www.socialbakers.com/facebook-statistics/united-arab-emirates
[66] AMEinfo.com "51% of Saudi internet users are active Twitter users: study." March 13, 2013. http://www.ameinfo.com/51-saudi-internet-users-active-twitter-333929
[67] https://twitter.com/MariamMansori
[68] https://twitter.com/Aysha_75
[69] U.A.E Cabinet. "Constitution of U.A.E." accessed July 31, 2013. http://uaecabinet.ae/en/UAEGovernment/Pages/UAE-Constitution.aspx#.UfqD6I21EwA [Arabic], "Constitution of the United Arab Emirates," Refworld.org, accessed August 1, 2013, http://www.refworld.org/docid/48eca8132.html.

pursued for political reasons.[70] In 2012, the president of the UAE appointed himself as head of the judiciary, overtaking the position of the minister of justice.[71] Human rights groups have continuously criticized the UAE for violating the human rights of political detainees and failing to provide them with fair and transparent trials. Instead, many are denied access to a lawyer, held without cause for extended periods of time, or tortured.[72] Furthermore, former detainees who have since been pardoned[73] are continually harassed and do not enjoy their full rights as citizens.[74]

Articles 8 and 176 of the penal code are used to punish public "insults" of the country's top officials, although these are widely used to prosecute any users that express a desire for political reform.[75] Articles 70 and 71 of the 1980 publishing law prohibit criticism of the head of the state and of Islam or any other religion.[76] Defamation laws have been criticized by lawyers as "all-encompassing" and clouded with many grey areas. The burden of proof is also upon the defendant. Penalties can be as high as two years imprisonment or a fine of AED 20,000 ($5,444).[77] In January 2011, the editor of Hetta.com was fined and his website was blocked for a month after a court upheld a defamation suit brought by the Abu Dhabi Media Company over defamatory and offensive user comments on the website.[78] In July 2011, Abu Dhabi police warned that spreading rumors through text messages constitutes libel and can be punishable by up to three years in jail.[79]

A new cybercrime law was issued in November 2012, replacing an earlier decree from 2006 that was criticized for being too vague.[80] While the introduction of the law was fundamental in providing a sounder legal basis to combat online fraud, money laundering, hacking, and other serious cybercrimes, the law also criminalizes a wide range of online activity commonly accepted within international norms. For example, hefty fines and jail sentences await users who engage in online gambling, disseminate pornographic material, or violate another person's privacy through posting their photograph or making statements about them online, regardless of the accuracy of the accusations. Intermediaries, such as domain hosts or administrators, are also liable if their websites are used to "prompt riot, hatred, racism, sectarianism, or damage the national unity or social peace

[70] Human Rights Watch, "UAE: Investigate Threats against 'UAE 5'," November 25, 2011, http://www.hrw.org/news/2011/11/25/uae-investigate-threats-against-uae-5.
[71] Emirates 24/7, "UAE to give judiciary greater autonomy," June 27, 2012. http://www.emirates247.com/news/emirates/uae-to-give-judiciary-greater-autonomy-2012-06-27-1.464786
[72] Rori Donaghy, "Torture in the United Arab Emirates," HuffingtonPost.co.uk, September 24, 2012, http://www.huffingtonpost.co.uk/rori-donaghy/torture-in-the-united-ara_b_1908919.html.
[73] Human Rights Watch, "UAE: Free Speech Under Attack: Harassment, Arrests, Criminal Prosecutions," January 25, 2012. http://www.hrw.org/news/2012/01/25/uae-free-speech-under-attack
[74] Sara Yasin, "UAE 5 still face restrictions after pardon," Index on Censorship, accessed August 1, 2013, http://www.indexoncensorship.org/2012/01/uae5-mansoor-still-face-restrictions-after-pardon-emirates/.
[75] Human Rights Watch, "UAE: Free Speech Under Attack," January 25, 2012. http://www.hrw.org/news/2012/01/25/uae-free-speech-under-attack
[76] "Publications and Publishing Law 1980," accessed in June 25, 2013, http://nmc.gov.ae/en/MediaLawsAndRegulation/4.pdf
[77] Kevin Brass, "Defamation laws keep the aggrieved quiet," The National, November 8, 2011 http://www.thenational.ae/business/industry-insights/property/defamation-laws-keep-the-aggrieved-quiet
[78] Reporters Without Boarders. "Countries Under Surveillance: United Arab Emirates." March 11, 2011. http://en.rsf.org/united-arab-emirates-united-arab-emirates-11-03-2011,39760.html
[79] Abdulla Rasheed, "Misuse of instant messaging services punishable by law," Gulf News, July 26, 2011 http://gulfnews.com/news/gulf/uae/crime/misuse-of-instant-messaging-services-punishable-by-law-1.843047
[80] Awad Mustafa and Ramona Ruiz. "Cyber-crime law to fight internet abuse and protect privacy in the UAE." November 13, 2012. http://www.thenational.ae/news/uae-news/cyber-crime-law-to-fight-internet-abuse-and-protect-privacy-in-the-uae

or prejudice the public order and public morals."[81] The cybercrime law also contains punishments for offending the state, its rulers, and its symbols, or for insulting Islam and other religions. Calls to change the ruling system are punishable by life imprisonment. Authorities have repeatedly warned foreign nationals that they must also follow the country's restrictive laws.[82]

Authorities regularly make use of these laws to prosecute Emirati citizens and residents for their online activities. In July 2012, stateless blogger Ahmed Abdulkhaleq was forcibly deported from the UAE to Thailand.[83] Abdulkhaleq was one of the five detainees ("the UAE 5") held in prison from April to November 2011 for demanding reforms through writings on the blocked online forum UAE Hewar. In May 2012, the UAE-born stateless man was given a Comoros passport, only to be arrested the following day and given the choice to go into exile or remain in jail.[84]

In July 2012, five users were held for their online posts on Twitter and blogs. The detainees faced charges of violating the constitution and cooperating with foreign political organizations.[85] The blogger Khalifa al-Nuaimi had previously written about "the UAE 5" and had been consistently threatened prior to his arrest.[86] Rashid al-Shamsi had tweeted news of arrests and written blog posts related to politics and free speech.[87] Twitter user Musabeh al-Rumaithy was arrested for his online writings in which he expressed support for the Islamist Islah party. He had been handed a travel ban one month before his arrest.[88] Similarly, Omran al-Radhwan had tweeted about "the UAE 5" detainees and wrote several posts promoting Islah and criticizing state violations of Shariah law.[89] Finally, Abdullah al-Hajri was arrested over the contents of his blog, in which he called for more government action to combat public immorality.[90] Al-Nuaimi, al-Shamsi, and al-Rumaithy were sentenced to 10 years imprisonment in July 2013 for being a member of a banned organization, while al-Radhwan and al-Hajri received 7 year sentences.[91] The sentenced users were part of a group of 68 activists set to serve 7 to 15 years in jail for the same charges.

In December 2012, 18-year-old blogger Mohammed Salem al-Zumer was arrested in the Emirate of Sharjah.[92] His online activities were found supportive of political detainees, including his uncle,

[81] See Federal Decree-Law no. (5) of 2012 on Combating Cybercrimes, August 13, 2012, available online at: http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf.
[82] Emirates News Agency, "New UAE cyber crime laws: Jail for indecent posts," Emirates 24/7, November 14, 2012, http://www.emirates247.com/news/government/new-uae-cyber-crime-laws-jail-for-indecent-posts-2012-11-14-1.482836
[83] Aljazeera. "UAE deports online activist to Thailand." July 16, 2012. http://www.aljazeera.com/news/middleeast/2012/07/2012716172114669177.html
[84] Suzanne Trimel. "UAE Urged to Halt Arbitrary Arrests After Blogger's Forced Deportation." Amnesty. Accessed in April 28, 2013. http://bit.ly/MtGmZv.
[85] Roy Greenslade. "UAE detains journalist bloggers." 25 July 2012. http://www.guardian.co.uk/media/greenslade/2012/jul/25/united-arab-emirates-press-freedom
[86] https://kalnuaimi.wordpress.com/
[87] http://rashedalshamsi.blogspot.fr/
[88] "Another Emirati activist banned from Travel," Watan, June 28, 2012. http://bit.ly/19bVlBW.
[89] http://omran83.tumblr.com/
[90] http://alhajria.wordpress.com/
[91] Amnesty International, "UAE: Grossly unfair trial of government critics," July 2, 2013. http://www.amnesty.org/en/news/uae-critics-sentenced-2013-07-02
[92] BBC. "UAE authorities 'detain 18-year-old blogger'." 7 December 2012. http://bbc.in/VPHeYP.

Khaled al-Nuiami, who has come under torture since being held in July 2012.[93] Al-Zumer faces charges for editing and uploading videos supportive of political detainees and has yet to be tried. According to his mother, [94] the blogger has been held in solitary confinement, tortured, and pressured into making a confession stating that Khalifa al-Nuiami, another UAE94 defendant, had encouraged him to edit and upload the videos.[95] For his part, in September 2012 Khalifa al-Nuiami had embarked on a hunger strike to protest against psychological and physical torture by police officers.[96]

Saeed al-Shamsi was detained on December 14, 2012 over suspicions that he ran the anonymous Twitter account "Sout al-Haq" (@weldbudhabi). The account was targeted over allegations that it received leaked documents from the Interior Ministry, although the documents were never published. After al-Shamsi's arrest, the Sout al-Haq account sent a tweet in which he claimed the authorities had arrested the wrong person. Al-Shamsi's lawyer said that his defendant appeared distressed and disoriented in court with signs of intimidation and torture.[97] He was reportedly released in March 2013. Two other users were also arrested for having messaged South al-Haq after authorities reportedly hacked into the account. Only days after, five more Twitter users were arrested for expressing political criticism and support for detainees.[98]

On April 8, 2013, Abdulhamid al-Hadidi was sentenced to ten months in jail for allegedly "spreading false information" about the trial of the so-called UAE94, of which his father, Abdulrahman al-Hadidi, is a member.[99] Al-Hadidi had been active on social media by sharing news from detainees and the details of their trials. He was also pushing detainees' families to work together to demand fair and transparent trials for the accused, as well as an end to state violations against their rights to prison visits. He was charged under Article 46 of the cybercrime law and Article 265 of the penal code.

By mid-2013, this had brought the total of number of political detainees to 94, including the 68 mentioned above.[100] Many of the detainees are members of the Reform and Social Guidance Association, better known as al-Islah, which seeks political reform and a greater adherence to Islam in society. As mentioned, Islah members often engage in political debates online and seek to

[93] David Hearst, "The UAE's bizarre, political trial of 94 activists," The Guardian, March 6, 2013, http://www.theguardian.com/commentisfree/2013/mar/06/uae-trial-94-activists.
[94] "ANHRI Demands the Suspense of Al-Zumer's Trial," June 3, 2013. http://www.anhri.net/?p=77914
[95] Emirates Center for Human Rights, "Detained 19-year-old Emriati Activist Alleges Torture," May 5, 2013, http://www.echr.org.uk/?p=701.
[96] Emirates Center for Studies, "Al-Nuaimi in bad health," September 2, 2012. http://twitmail.com/email/533078805/4/false
[97] Rori Donaghy, "Torture in the United Arab Emirates," Huffington Post, September 24, 2012. http://www.huffingtonpost.co.uk/rori-donaghy/torture-in-the-united-ara_b_1908919.html
[98] Bill Law. "Eight online activists 'arrested in UAE'." December 19, 2012. http://www.bbc.co.uk/news/world-middle-east-20768205
[99] "UAE: Son of defendant sentenced to 10 months in prison for reporting on 'UAE94' trial," Alkarama, April 11, 2013, http://en.alkarama.org/index.php?option=com_content&view=article&id=1073:uae-son-of-defendant-sentenced-to-10-months-in-prison-for-reporting-on-uae94-trial&catid=38:communiqu&Itemid=107.
[100] "Current Political Prisoners," Emirates Centre for Human Rights, August 1, 2013, http://www.echr.org.uk/?page_id=207.

document and disseminate information on human rights violations on social media.[101] These detainees face up to 15 years in jail for being part of an organization with intent to overthrow the government and with ties to Egypt's Muslim Brotherhood.[102] Reacting to Egypt's 2011 parliamentary elections, in which the Muslim Brotherhood gained the most seats out of any other political party, Dubai's chief of police tweeted that "since Muslim Brotherhood has 'become a state,' anyone advocating its cause [in the UAE] is considered a foreign agent."[103]

Aside from arbitrary detentions, unfair prosecutions, and torture, online activists also face a range of extralegal attacks in the UAE. In October 2012, blogger Ahmed Mansour faced media harassment and physical beatings. The actions were taken in response to a pre-recorded speech he made that was later broadcast at a side event to the United Nations Human Rights Council regarding violations in the UAE, Oman, and Saudi Arabia.[104]

The high amount of prosecutions and physical harassment of users in the UAE is, in part, due to the several obstacles they face in using ICT tools anonymously. In January 2013, the country's two mobile phone providers gave a last warning to their users to register their SIM cards or have their lines cut for failing to comply.[105] The government had required every mobile user to re-register their information as part of the TRA's "My Number, My Identity"[106] campaign launched in June 2012.[107] Cybercafe customers are also required to provide their ID and personal information in order to surf the net.[108]

Internet and mobile providers are not transparent in discussing the procedures taken by authorities to access their data and users' information. Warnings from both the Abu Dhabi and Dubai police against spreading rumors through mobile messages may indicate the government's overall surveillance on users.[109] Further proving this, as previously mentioned, Twitter users were arrested

[101] "UAE: Unfair Mass Trial of 94 Dissidents," Alkarama, April 3, 2013, http://en.alkarama.org/index.php?option=com_content&view=article&id=1070:uae-unfair-mass-trial-of-94-dissidents&catid=38:communiqu&Itemid=107.
[102] Lori Plotkin Boghardt, "Interpreting Muslim Brotherhood Verdicts in the UAE," The Washington Institute, July 1, 2013, http://www.washingtoninstitute.org/policy-analysis/view/interpreting-muslim-brotherhood-verdicts-in-the-uae.
[103] Wafa Issa, "Muslim Brotherhood invading UAE social media: police chief," March 9, 2012, http://www.thenational.ae/news/uae-news/muslim-brotherhood-invading-uae-social-media-police-chief.
[104] Gulf Center for Human Rights, "UAE: Attacks and Smear Campaign against prominent human rights defender Ahmed Mansoor," October 5, 2013. http://gc4hr.org/news/view/250
[105] Nadeem Hanif. "Du and Etisalat brace for UAE users last chance to re-register Sim card." January 16, 2013. http://www.thenational.ae/news/uae-news/du-and-etisalat-brace-for-uae-users-last-chance-to-re-register-sim-card
[106] The TRA's statement reads: "Your mobile phone number is an extension of your identity. Sharing or giving away your SIM-Card to others can cause unwanted consequences, including being held accountable for any improper conduct or misuse associated with the mobile phone subscription by the authorities as well as being liable for all charges by the licensees." Telecommunications Regulatory Authority. "My Number My Identity." Accessed April 28, 2013. http://www.tra.gov.ae/mynumber.php
[107] Nadeem Hanif. "Every mobile phone user in the UAE must re-register SIM card." June 28, 2012. http://www.thenational.ae/news/uae-news/every-mobile-phone-user-in-the-uae-must-re-register-sim-card
[108] Citizen Lab. "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools." January 15, 2013. https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/
[109] [109] Abdulla Rasheed, "Misuse of instant messaging services punishable by law," Gulf News, July 26, 2011 http://gulfnews.com/news/gulf/uae/crime/misuse-of-instant-messaging-services-punishable-by-law-1.843047

for exchanging private messages with a controversial account in December 2012.[110] Incidents of providers demanding warrants or legal permissions for security bodies to gain access to user data are not known. In 2009, the makers of BlackBerry devices alleged that a software update issued by the UAE telecommunications company Etisalat was actually spyware used to "enable unauthorized access to private or confidential information stored on the user's smartphone."[111]

The UAE remains one of the top countries facing hacking attempts worldwide. The country's spam rate was recorded at 73 percent, and 46 percent of the country's social networking users fell victim to cybercrimes, compared to the global average of 39 percent.[112] In July 2012, the TRA denied claims of the hacktivist group Anonymous to "have penetrated the country's proxy server and extracted a list of blocked website addresses."[113] Anonymous has posted a list of over 24,000 words and links blocked in the UAE.[114] Also that month, a group of UAE-based hackers defaced a website of the Human Rights Commission of Pakistan (HRCP), apparently to warn Pakistani hackers against engaging in cyberattacks against the UAE and other Gulf countries.[115]

Emirati activists have also reported spyware and malware attacks against their computers. In one case from January 2013, a user received an e-mail purportedly containing a link to a video of the Dubai police chief. Instead, the link contained spyware that could monitor the victim's screen, enable the computer's webcam, steal passwords, and conduct keylogging. It was believed the Emirati government was behind the attack.[116]

[110] Bill Law. "Eight online activists 'arrested in UAE'." December 19, 2012. http://www.bbc.co.uk/news/world-middle-east-20768205
[111] Tom Arnold, "BlackBerry patch was not for spying, claims Etisalat," Arabian Business, 23 July, 2009 http://www.arabianbusiness.com/exclusive-blackberry-patch-was-not-for-spying-claims-etisalat-15618.html
[112] Arabian Gazetter, "UAE to Face Advanced Cybercrime in 2013," December 9, 2012. http://arabiangazette.com/uae-face-advanced-cybercrime-2013/
[113] Martin Croucher, "Telecoms regulator denies Anonymous hacked UAE netfilter system," The National, July 8, 2012. http://www.thenational.ae/news/uae-news/telecoms-regulator-denies-anonymous-hacked-uae-netfilter-system
[114] Anonymous, UAE list http://pastehtml.com/view/c336prjrl.rtxt
[115] Alain Hacker, "HRCP website hacked, counter-hacked By BozzErrOR & Gh()stH4x0r," February 28, 2013. http://www.alainhacker.com/2013/02/hrcp-website-hacked-counter-hacked-by.html
[116] Bill Marczak, "Hacked Website, Java Vulnerability Used to Target UAE Activist with Spyware," Bahrain Watch, January 15, 2013, https://bahrainwatch.org/blog/2013/01/15/hacked-website-java-vulnerability-used-to-target-uae-activist-with-spyware/.

UNITED KINGDOM

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	2	2
Limits on Content (0-35)	6	6
Violations of User Rights (0-40)	16	16
Total (0-100)	24†	24

* 0=most free, 100=least free

POPULATION: 63.2 million
INTERNET PENETRATION 2012: 87 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- In an effort to protect children from harmful content, filtering on mobile phones is enabled by default and has resulted in instances of over-blocking. In contrast, ISPs did not block politically orientated content on household connections (see **LIMITS ON CONTENT**).
- Revisions to the Defamation Act provided greater legal protections for intermediaries and reduced the scope for "libel tourism" (see **LIMITS ON CONTENT** and **VIOLATIONS OF USER RIGHTS**).
- The Protection of Freedoms Act of 2012 created new requirements to obtain judicial approval prior to accessing online surveillance data, although revelations surrounding the GCHQ's Tempora program have since brought many of these protections into doubt (see **VIOLATIONS OF USER RIGHTS**).
- Several web users were prosecuted or fined for breaking court injunctions, violating the privacy of crime victims, and committing libel using social networks (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

The following chapter covers developments in the United Kingdom from May 1, 2012 to April 30, 2013. However, beginning in June 2013, British daily newspaper the Guardian *published a series of revelations on secret surveillance practices by the British General Communications Headquarters (GCHQ) and American National Security Agency (NSA). Under the GCHQ's "Tempora" program, British authorities had entered into secret agreements with telecoms giants to install intercept probes on undersea cables landing on British shores. The content of this data was then filtered and stored, typically for three days, in order for GCHQ agents to comb through it for counterterrorism and law enforcement. User "metadata" was stored in a GCHQ facility for 30 days. Furthermore, details emerged surrounding close collaboration between the NSA and the GCHQ, including payments of at least £100 million ($155 million) from the former to the latter. Since UK and U.S. laws place protections on the monitoring of citizens, UK agencies were able to pass on information related to American citizens—and vice versa—thereby bypassing legal restrictions.*

Given that this surveillance has been ongoing for a number of years—including during the period covered by this report—Freedom House has decided to include it in this edition of Freedom on the Net (see Violations of User Rights).

INTRODUCTION

The United Kingdom was an early adopter of new information and communication technologies (ICTs). The University of London was one of the first international nodes of the ARPAnet, the world's introductory operational packet switching network that later came to compose the global internet, and the Queen sent her first ceremonial e-mail in 1976. Academic institutions began connecting to the network in the mid-1980s. By the beginning of the next decade, internet service providers (ISPs) emerged as more general commercial access became available.

The United Kingdom has high levels of internet penetration and online freedom of expression is generally respected. During the past year, however, there has been an attempt by ministers to introduce a new framework for monitoring and collecting online communications as part of the Draft Communications Data Bill.[1] In addition, there has been widespread concern that government proposals to improve journalism co-regulation would result in new liability risks applying to blogs.[2] While ongoing concerns about web filtering and blocking have continued, particularly on mobile platforms, greater public concern has focused on surveillance of communications, particularly after the June 2013 revelations of mass surveillance of web use, e-mail, and mobile traffic data. The Communications Capabilities Development Programme was reintroduced in May 2012, which, if implemented, would require providers to retain data on phone calls, e-mails, text messages and

† The 2012 rating for the UK was adjusted on the basis of updated scoring guidelines to best convey changes over time.
[1] See, Draft Communications Data Bill, http://www.parliament.uk/draft-communications-bill/.
[2] Michael Savage, "Bloggers fear they could be savaged by press watchdog," The Times, March 20, 2013, http://www.thetimes.co.uk/tto/news/medianews/article3717799.ece.

communications on social-networking sites, in addition to expanding the real time surveillance capabilities of the security services in order to combat terrorism and organized crime.[3] However, following the recent leaks by former NSA contractor Edward Snowden, it appeared that the existing surveillance operations were already testing the boundaries of what was permissible.

In a positive development, the government passed a bill to revise the Defamation Act, which provides greater protections for ISPs through limiting their liability for user-generated content, as well as reducing "libel tourism."[4] Additionally, the Protection of Freedoms Act of 2012 sets forth a requirement for local authorities to obtain a magistrate's approval for access to communications data, thereby placing limits on their surveillance powers.[5] The draft Communications Data Bill keeps this requirement.[6]

OBSTACLES TO ACCESS

Access to the internet has become essential to citizenship and social inclusion in the United Kingdom. The share of homes with connected devices has increased from 53 percent in 2002 to 82 percent in 2012,[7] and internet penetration grew from 70 in 2007 to 87 percent in 2012.[8] In December 2010, the government committed to promoting universal access to basic broadband, but progress to that goal remains stalled.[9] The government set a further objective of ensuring "superfast" broadband for 90 percent of households by 2015.[10] The Broadband Delivery UK program has made available £830 million ($1.32 billion) in funding for the project.[11] Although there remain significant numbers of people who for financial or literacy reasons are unable or disinclined to subscribe, broadband is widely available, with nearly 100 percent of all households within range of ADSL connections and 45 percent within reach of fiber optic cable.[12] Superfast connections are, for the most part, only available in major urban centers and not in rural areas.

Even where access is available, use and participation does not necessarily follow. In 2012, 22 percent of the UK adult population did not use the internet at home.[13] Research by the British

[3] David Barrett, "Phone and email records to be stored in new spy plan," The Telegraph, February 18, 2012, http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html.
[4] See, Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), http://services.parliament.uk/bills/2012-13/defamation.html.
[5] Protection of Freedoms Act 2012, http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted.
[6] Draft Communications Data Bill, http://www.parliament.uk/draft-communications-bill/.
[7] Ofcom, *The Consumer Experience of 2012: Research Report* (London: Ofcom, January 2013), http://stakeholders.ofcom.org.uk/binaries/research/consumer-experience/tce-12/Consumer_Experience_Researc1.pdf.
[8] "Individuals Using the Internet," International Telecommunication Union, 2000-2012, accessed August 7, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[9] See, Department for Culture, Media and Sport, *Proposed Changes to Siting Requirements for Broadband Cabinets and Overhead Lines to Facilitate the Deployment of Superfast Broadband Networks*, January 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/89449/CONDOC_fixed_bb.pdf.
[10] Ibid.
[11] Department for Culture, Media and Sport, *Next Phase of Superfast Broadband Plans Announced*, December 2010. https://www.gov.uk/government/news/next-phase-of-superfast-broadband-plans-announced--4.
[12] Ofcom, *The Consumer Experience of 2012: Research Report*.
[13] Consumer Communications Panel, "Bridging the Gap: Sustaining Online Engagement," May 2012, http://www.communicationsconsumerpanel.org.uk/smartweb/research/bridging-the-gap:-sustaining-online-engagement.

Communications Consumer Panel found that citizens with internet access may choose not to participate if they lack technical understanding, lack adequate equipment, or are reluctant to submit personal data.[14] Those in the lowest income groups are significantly less likely to have home internet subscriptions, and the gap has remained the same for the past several years. The share of people over 65 with broadband access is significantly lower than that of all other age groups, but the gap has been narrowing rapidly.[15]

Mobile telephone penetration is also universal, with a penetration rate of over 130 percent in 2012.[16] Second-generation (2G) and third-generation (3G) networks are available in over 99 percent of all households. Overall household use of mobile broadband decreased from 17 percent to 12 percent in 2012, and 6 percent of households use mobile broadband as their main internet connection. From 2011 to 2012, the average cost of all mobile service packages increased 7 percent to just over £9 pounds ($14) per month for a basic package and £43 for ($66) for an advanced package that includes internet.[17] The price of broadband declined 13 percent in the past four years to about £16 ($24) per month[18] while increasing in speed from 3.6 Mbps to an average of 12.0 Mbps.[19]

The government does not place limits on the amount of bandwidth ISPs can supply, and the use of internet infrastructure is not subject to government control. ISPs regularly engage in traffic shaping or slowdowns of certain services, such as peer-to-peer (P2P) file sharing and television streaming, while mobile providers have cut back on previously unlimited access packages for smart phones, reportedly because of concerns about network congestion. The Office of Communications (Ofcom), the country's telecommunications regulator, adopted a voluntary code of practice on broadband speeds in 2008, which it updated in 2010.[20] After holding a consultation on the subject,[21] Ofcom released a report in 2011 that called for a self-regulatory approach to network neutrality focusing on information disclosure rather than enforceable rules.[22] It described blocking of services and sites by ISPs as "highly undesirable" but said that market forces will address possible problems. In July 2012, the major ISPs published a "Voluntary code of practice in support of the open internet."[23] The code commits ISPs to transparency and confirms that traffic management practices will not be used to target and degrade the services of a competitor.

Nominet, the domain registrar in the United Kingdom that manages access to newly introduced

[14] Ibid.
[15] Ofcom, *The Consumer Experience of 2012: Research Report*.
[16] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2012, accessed August 7, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[17] Ofcom, *The Consumer Experience of 2012: Research Report*.
[18] Ibid.
[19] Ofcom, "Overview of UK Broadband Speeds," March 14, 2013.
[20] Ofcom, "2010 Voluntary Code of Practice: Broadband Speeds," July 27, 2010, http://stakeholders.ofcom.org.uk/telecoms/codes-of-practice/broadband-speeds-cop-2010/code-of-practice/.
[21] Ofcom, "Traffic Management and 'net neutrality,' A Discussion Document," June 24, 2010, http://stakeholders.ofcom.org.uk/consultations/net-neutrality/.
[22] Ofcom, "Ofcom's approach to net neutrality," November 11, 2011, http://stakeholders.ofcom.org.uk/consultations/net-neutrality/statement/.
[23] Broadband Stakeholder Group, "ISPs launch Open Internet Code of Practice," July 25, 2012, http://www.broadbanduk.org/2012/07/25/isps-launch-open-internet-code-of-practice/.

.uk, .wales, and .cymru domains, consulted on a new policy regarding the suspension of web domains at the request of law enforcement bodies.[24] The registrar had suspended thousands of domains without a court order after receiving complaints from the police and other bodies for alleged criminal and civil violations.[25] Nominet was told that failure to remove the domains may result in them being found criminally liable. Civil rights groups and ISPs expressed concerned about a lack of due process and have demanded that court orders be required under any new policy.[26]

The UK provides a competitive market for internet access, and prices for communications services compare favorably with those in other countries.[27] Through local loop unbundling, a large number of companies provide internet access on infrastructure provided mainly by British Telecom (BT) and Virgin. BT, as the sole choice for many consumers, is dominant in the provision of wholesale access. This is likely to continue with the rise of "fiber to the cabinet" and "fiber to the home" services, which currently amount to around 40 percent of subscriptions. Four major ISPs—BT, Virgin, TalkTalk, and Sky—control around 87 percent of the total market.[28] ISPs are not subject to licensing but must comply with the general conditions set by Ofcom, such as having a recognized code of practice and being a member of an alternative dispute-resolution scheme.[29] Ofcom's duties include regulating competition among communications industries, including telecommunications and wireless communications services. It is generally viewed as fair and independent in its oversight.

LIMITS ON CONTENT

There is no general law authorizing internet censorship in the UK. At the same time, the UK does operate a filtering system to block unlawful content, such as child pornography. Additionally, laws such as the Protection of Children Act are used to prosecute individuals suspected of accessing or circulating content relating to child abuse.[30] Over the past years, these filtering tools have expanded to include the blocking of content related to intellectual property violations and sites that promote extremism and terrorism. Most recently, there have also been new developments to strengthen parental controls in order to prevent children from viewing adult-oriented sites. These measures

[24] "UK police may be given domain name-suspension powers," Out-Law.com, September 5, 2011. http://www.out-law.com/en/articles/2011/september/uk-police-may-be-given-domain-name-suspension-powers/; Nominet, "Dealing with domain names used in connection with criminal activity," accessed May 21, 2013, http://www.nominet.org.uk/how-participate/policy-development/current-policy-discussions-and-consultations/dealing-domain-names.

[25] According to Open Rights Group, Nominet has said that the takedowns are for "counterfeit goods sites (83%), phishing (9.6%), drugs (6.3%) and fraud (0.8%)"; Jim Killock, "Domain seizures," Open Rights Group (blog), May 20, 2011, http://www.openrightsgroup.org/blog/2011/domain-seizures.

[26] Nominet, "Nominet direct.uk Consultation: Response Analysis," accessed May 21, 2013, http://www.nominet.org.uk/sites/default/files/NomensaAnalysisFinal.pdf; Jim Killock, "ISPA, LINX and ORG insist on Court Orders for domain suspensions," Open Rights Group (blog), November 23, 2011, http://www.openrightsgroup.org/blog/2011/ispa,-linx-and-org-insist-on-court-orders-for-domain-suspensions.

[27] Ofcom, *The Consumer Experience of 2012: Research Report*.

[28] Ofcom, "The Communications Market 2012," July 18, 2012, pp. 313, available at http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/UK_5.pdf.

[29] Ofcom, "General Conditions of Entitlement," accessed May 21, 2013, http://stakeholders.ofcom.org.uk/telecoms/ga-scheme/general-conditions/.

[30] See, Protection of Children Act 2009, http://www.legislation.gov.uk/ukpga/1999/14/contents.

have been most controversial in the realm of mobile devices, where filtering criteria can be subjective and often result in the blocking of content that poses little threat to those under the age of 18. Since these child filters are turned on by default, many mobile users navigate a web in which some legitimate websites, such as those belonging to political groups or civil society organizations, are blocked.

Under a voluntary code of practice adopted by the Internet Services Providers' Association (ISPA) in January 1999, British ISPs block sites flagged as harmful by the Internet Watch Foundation (IWF), a British charity funded by ISPs and the European Union (EU).[31] The IWF generates a blacklist of unlawful content through a citizen hotline and investigations into allegedly criminal content.[32] Previously, the IWF also received reports on materials inciting hatred, but that has since been moved to TrueVision, a new police-run website.[33] The CleanFeed filtering system, developed by BT and the IWF, blocks access to any images or websites listed in the IWF database. While ISPs are not required to implement the IWF blocking list,[34] the overwhelming majority of ISPs do so. Furthermore, in 2010 the Home Office adopted rules that prohibit government bodies from procuring services from ISPs that do not use the list.[35] Consumer awareness of CleanFeed remains very low and the list of blocked sites remains secret in order to deter access to unlawful materials.

In addition to child pornography and hate sites, the government has also taken a proactive approach in limiting access to websites that have been found in violation of copyright protections. There have been a number of cases in which courts have ordered websites, such as Newzbin and the Pirate Bay, to be blocked for copyright infringement[36] and to have their domain names seized based on the Copyright, Designs and Patents Act and other laws.[37] The CleanFeed system has been adapted to enable ISPs to enforce the blocks and the list of URLs is steadily growing.[38] The Digital Economy Act (DEA) of 2010 stipulates that websites found to have "substantial" violations of copyright can be blocked by a court order. However, a review mandated by the government and conducted by Ofcom determined that those particular blocking provisions are unlikely to be effective.[39]

---

[31] Internet Services Providers' Association, "ISPA Code of Practice," accessed August 20, 2012, http://www.ispa.org.uk/about-us/ispa-code-of-practice/.
[32] The Internet Watch Foundation (IWF) website is located at http://www.iwf.org.uk/.
[33] Homepage: http://www.report-it.org.uk/home. See, IWF, "Incitement to racial hatred removed from IWF's remit," April 11, 2011, http://www.iwf.org.uk/about-iwf/newss/post/302-incitement-to-racial-hatred-removed-from-iwfs-remit.
[34] Chris Williams, "Home Office Backs Down on Net Censorship Laws," The Register, October 16, 2009, http://www.theregister.co.uk/2009/10/16/home_office_iwf_legislation/.
[35] Ben Leach, "Ban for internet providers failing to block child sex sites," The Daily Telegraph, March 10, 2010. http://www.telegraph.co.uk/technology/facebook/7411020/Ban-for-internet-providers-failing-to-block-child-sex-sites.html.
[36] Dramatico Entertainment Ltd and others v. British Sky Broadcasting Ltd and others [2012] EWHC 1152 (Ch) (May 2, 2012); Twentieth Century Fox Film Corporation and others v. British Telecommunications plc [2011] EWHC 2714 (Ch) (October 26, 2011).
[37] Matt Warman, "Serious Organised Crime Agency closes down rnbxclusive.com filesharing website," The Telegraph, February 15, 2012, http://www.telegraph.co.uk/technology/internet/9084540/Serious-Organised-Crime-Agency-closes-down-rnbxclusive.com-filesharing-website.html.
[38] The UK's High Court has also ordered ISPs to block Kickass Torrents, H33T, and Fenopy, http://www.bbc.co.uk/news/technology-21601609.
[39] Ofcom, "'Site Blocking' to reduce online copyright infringement," May 27, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78095/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf.

A new initiative to revise the Communications Act of 2003 is expected to be announced later in 2013, which may result in substantial changes to these and other provisions that were adopted through the DEA. The government also initiated a review of intellectual property law in 2011, releasing a report which recommended significant changes to the law, including an explicit exemption for parody, which only partially exists in case law now.[40] The government endorsed the review's conclusions and has consulted on and passed laws to implement its recommendations.[41] In March 2013, the Intellectual Property Office also launched a mediation service to assist in resolving intellectual property disputes.[42] (See "Violation of User Rights" for more information on laws related to the prosecution of users).

In addition, the government has increased its efforts to limit access to "extremist" materials on the internet.[43] The Terrorism Act of 2006 allows for the takedown of terrorist material hosted in the United Kingdom if it "glorifies or praises" terrorism, is information that could be useful to conducting terrorism, or urges people to commit or help with terrorism.[44] ISPs reportedly take down material when contacted by the authorities, though statistics released by ISPs appear to be unverifiable and informal.[45] A new Counter Terrorism Internet Referral Unit (CTIRU) was set up in 2010 to investigate internet materials, and as of March 2013, the unit reported that it had successfully taken down 4,000 URLs that breach UK terrorism legislation.[46] The government released a revised Prevent Anti-Terrorism Strategy in 2011, which calls for limiting access to "extremist" materials in schools and public libraries and more efforts to remove "harmful content" from the internet.[47] The strategy also involves "sharing unlawful websites for inclusion in commercial filtering products."[48]

There has also been increased public debate about imposing measures that would more effectively prevent children from accessing adult-oriented material on the internet. The four largest ISPs announced in 2011 that they were offering systems allowing users to filter "adult" materials at the

[40] Intellectual Property Office, "Digital Opportunity: A review of Intellectual Property and Growth," May 2011, http://www.ipo.gov.uk/ipreview; See also, "Parody, pastiche & caricature Enabling social and commercial innovation in UK copyright law," Consumer Focus, July 2011, http://www.consumerfocus.org.uk/files/2012/11/Consumer-Focus-Parody-briefing.pdf.
[41] See, Intellectual Property Office, "Implementing the Hargreaves review", accessed May 25, 2013, http://www.ipo.gov.uk/types/hargreaves.htm.
[42] Intellectual Property Office, "Mediation of Intellectual Property Disputes and IPO Mediation Service," March 2013, http://www.ipo.gov.uk/ipenforce/ipenforce-dispute/ipenforce-mediation.htm.
[43] See, Home Affairs Committee, "MPs urge internet providers to tackle on-line extremism," February 6, 2012. http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/news/120206-rvr-rpt-publication/.
[44] Terrorism Act 2006 (c. 11), §3, available at Office of Public Sector Information, http://www.legislation.gov.uk/ukpga/2006/11/contents; See, "Reporting extremism and terrorism online," DirectGov, http://www.direct.gov.uk/en/CrimeJusticeandtheLaw/CounterTerrorism/DG_183993.
[45] See, e.g., Google Transparency Report, Removal Requests, accessed May 27, 2013, http://www.google.com/transparencyreport/removals/government/.
[46] Home Office, "CONTEST: The United Kingdom's Strategy for Countering Terrorism: Annual Report," March 2013, https://www.gov.uk/government/publications/contest-annual-report-2012.
[47] Home Office, "Prevent Strategy," June 2011, http://www.homeoffice.gov.uk/publications/counter-terrorism/prevent/prevent-strategy/prevent-strategy-review?view=Binary.
[48] Home Office, "CONTEST: The United Kingdom's Strategy for Countering Terrorism: Annual Report."

ISP level and issued a code of practice aimed at educating consumers about parental controls.[49] In June 2011, the Department of Education sponsored a review, which recommended that ISPs provide an "active choice" to parents to limit children's access to adult materials.[50] While the government opposed the use of default filtering, it asked ISPs to encourage their subscribers to make an active choice to switch on parental controls if children are in the household.[51] By the end of 2013, the four major ISPs will also implement a system that automatically e-mails account holders when those parental controls are changed.[52] Regulators also launched the ParentPort website in October 2011 to receive complaints about materials "unsuitable for children" across all forms of media and to provide a resource for parents for tips on house to use parental controls.[53]

With the rapid rise of mobile access to the internet, the issue of mobile filtering has become increasingly controversial. Due to concerns over the unsupervised use of data-enabled mobile phones by children under the age of 18, mobile internet subscriptions are sold to customers with child filters enabled by default and, depending on the provider, require either the disabling of the filters or a deliberate "opt-in" to adult content. Customers can verify their age and remove the filters by contacting their provider with proof of age such as payment details. Blocked content includes pornography, so-called "hate sites," and in some cases, web forums that could potentially allow minors to interact with older users.[54] The practice is conducted in accordance with a 2004 code of conduct established by the Mobile Broadband Group (MBG), consisting of the providers Vodafone, Three, EE, and O2.[55] In turn, the Independent Mobile Classification Body (IMCB), appointed by the MBG, sets the criteria for which websites are deemed to be unsuitable for children under the age of 18. However, the process has been criticized by the Open Rights Group (ORG) as subjective, insufficiently transparent, and generally problematic.

The ORG, in collaboration with the London School of Economics (LSE) Media Policy Project, created the website "Blocked.org.uk" to allow users to report cases of "over-blocking," in which mobile phone providers blocked access to content that poses little or no threat to child welfare, including civil society and political websites. The ORG-LSE report found that websites as diverse as Tor, eHow.com, the French digital rights advocacy group "La Quadrature du Net," a website critical of alleged BBC bias, and a community website for the town of St. Margarets in Middlesex were all blocked. The website of the British National Party, an extreme right-wing political organization, was also blocked. It was classified as a "hate site" by O2, the only provider that

[49] "Code of Practice on Parental Controls—BT, TalkTalk, Virgin Media and Sky," Virgin Media, October 28, 2011, http://mediacentre.virginmedia.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=1245.
[50] "Update on the implementation of 'Letting Children be Children,'" Department for Education, April 26, 2012, http://www.education.gov.uk/childrenandyoungpeople/healthandwellbeing/b0074315/bailey-review.
[51] Department of Education, "The Government's response to the consultation on parental internet controls," December 2012, http://www.education.gov.uk/ukccis/news/a00218633/parental-internet-controls-consultation.
[52] See, United Kingdom Council for Child Internet Safety, "Executive Board Notes February 2013," accessed May 24, 2013, http://www.education.gov.uk/ukccis/about/b0076378/executive-board.
[53] Homepage: http://www.parentport.org.uk/.
[54] See a report published by LSE/ Open Rights Group http://www.openrightsgroup.org/assets/files/pdfs/MobileCensorship-webwl.pdf and a discussion here: http://blogs.lse.ac.uk/mediapolicyproject/2012/05/17/response-to-mobile-censorship-report-mobile-fixed-internet-are-different/
[55] "Who We Are," Mobile Phone Group, accessed September 3, 2013, http://www.mobilebroadbandgroup.com/whoweare.htm.

operates a "URL checker" page to look-up how a given website is classified.[56] The owners and operators of websites are not notified that they have been blocked and it is not clear from mobile providers what process they must go through to request to be unblocked.[57]

Similarly, the filtering system for fixed-line connections has encountered its own faults. On several occasions, due to technical difficulties at the ISP level, blocking decisions designed to prevent access to harmful content also temporarily disabled users from accessing popular sites such as Wikipedia.[58] In 2011, the IWF identified a single URL at the popular cloud server site Fileserve to be blocked; however, due to technical problems, BT and Virgin subscribers were prevented from using the entire service for several days.[59]

Finally, under the EU 2002 E-Commerce Directive, hosts can be held liable if they are found to have had knowledge of illicit material, including defamatory content, but have failed to remove it.[60] This caused hosting companies to quickly take down material when asked, with little inquiry as to the legitimacy of the demand.[61] In April 2013, the government updated the Defamation Act, which now provides greater protections for ISPs by limiting their liability for user-generated content.[62] (For more on UK libel law and the issue of libel tourism, please see "Violation of User Rights.")

Following the revelation of phone hacking practices by journalists and news organizations, the government launched an inquiry into press ethics.[63] The government is currently seeking to promote a stronger scheme for self-regulation that encompasses traditional news platforms as well as news websites. To encourage participation, publishers that join a self-regulatory body receive greater protection from punitive damages.[64] Publishers that decline to join, including news blogs, remain exposed to punitive damages if the publication features multiple authors and is subject to editorial control. There are exceptions to punitive damages exposure for certain types of publishers, including broadcasters, personal blogs, and special interest publications. While barriers to entry in news markets remain theoretically very low, the reality is that recent years have seen a consolidation of online news into a smaller number of providers, with large providers such as News

---

[56] Tom Brewster, "O2 Blocks BNP Website as 'Hate Site'," Tech Week Europe, May 18, 2012, http://www.techweekeurope.co.uk/news/o2-blocks-bnp-website-as-hate-site-78653.

[57] Peter Bradwell, Gemma Craggs, Alessandra Cappuccini, and Joana Kamenova, *Mobile Internet censorship: What's happening and what we can do about it,* Open Rights Group and the LSE Media Policy Project, May 2012, available at http://www.openrightsgroup.org/assets/files/pdfs/MobileCensorship-webwl.pdf.

[58] "Wikipedia Child Image Censored," BBC News, December 8, 2008, http://news.bbc.co.uk/2/hi/uk_news/7770456.stm.

[59] "UK ISP Block of Fileserve Site Blamed on Internet Watch Foundation Filter," ISPreview, November 19, 2011.

[60] Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013). See, *Metropolitan International Schools Ltd v. (1) Designtechnica Corporation (2) Google UK Ltd & (3) Google Inc* [2009] EWHC 1765 (QB) (search engine not liable for excerpts); *Bunt v. Tilly* [2006] EWHC 407 (QB) (ISP not liable if just provides connection); *Twentieth Century Fox Film Corporation v. Newzbin* [2010] EWHC 608 (Ch) (company that provides indexing of copyrighted files liable); *Kaschke v. Gray & Anor* [2010] EWHC 690 (QB) (host that moderates user comments liable). See also Electronic Commerce Directive (Hatred against Persons on Religious Grounds or the Grounds of Sexual Orientation) Regulations.

[61] Saskia Walzel, "European Commission Consults on Notice and Takedown," Media Policy Project (blog), August 24, 2012, http://blogs.lse.ac.uk/mediapolicyproject/2012/08/24/european-commission-consults-on-notice-and-takedown/.

[62] See, Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), http://services.parliament.uk/bills/2012-13/defamation.html.

[63] The Report into the Culture, Practice and Ethics of the Press, November 29, 2012, http://www.levesoninquiry.org.uk/about/the-report/.

[64] See, Section 41, Crime and Courts Act 2013, http://www.legislation.gov.uk/ukpga/2013/22/contents/enacted.

International and Associated Newspapers, as well as the publicly-owned BBC, garnering more control over online news markets.[65] Evidence taken from the Leveson Inquiry revealed that there were close links between these news providers and government actors.

Users in the United Kingdom continue to enjoy wide access to free or low-cost blogging services, allowing them to express their views on the internet. Users and nongovernmental organizations also employ various forms of online communication to organize political activities, protests, and campaigns. Civil society organizations maintain a significant presence online and have used internet platforms to promote various causes. For example, organizations such as Avaaz[66] and 38 Degrees have millions of members who use social media to campaign successfully on issues.[67] An online petition against UK libel laws received over 60,000 signatures, including support from numerous high profile public figures. "The Libel Reform Campaign," the joint project by the Index on Censorship, English PEN, and Sense About Science, successfully campaigned for changes in the libel laws that were introduced in April 2013.[68]

However, there have been discussions about whether it is appropriate to limit access to social media if necessary to prevent violence. Following the London riots in 2011, Prime Minister David Cameron and other public officials suggested a need to prevent individuals from using social media sites such as Twitter and Facebook for the purposes of organizing public disorder. The government backed away from the statement after public and industry protests, and no specific steps were ever taken that would restrict use of social media.[69]

VIOLATIONS OF USER RIGHTS

The United Kingdom has no written constitution or comprehensive bill of rights. The European Convention on Human Rights is incorporated into UK law through the Human Rights Act of 1998, and British courts have increasingly recognized freedom of expression and other human rights. Over the past year, a new graduated response scheme was introduced by Ofcom in a bid to combat online piracy. Changes to the Defamation Act have also resulted in more protections for intermediaries and defendants, while seeking to reduce libel tourism. Despite these increasing protections, several users were fined for a range of posts on social media, an issue which the public prosecutor has looked to re-examine. In total, there were 653 criminal charges filed against Twitter and Facebook users in England and Wales during 2012.[70] Finally, leaked documents concerning the Tempora program and UK collaboration with U.S. intelligence agencies have brought new

[65] See the Open Society Foundation Mapping Digital Media UK Report http://www.opensocietyfoundations.org/reports/mapping-digital-media-united-kingdom.
[66] See, http://www.avaaz.org/.
[67] See, "Current Campaigns," 38 Degrees (blog), accessed May 27, 2013, http://www.38degrees.org.uk/campaigns.
[68] See, "The Libel Reform Campaign," http://www.libelreform.org/index.php, accessed June 24, 2013.
[69] "PM statement on disorder in England," The official site of the British Prime Minister's Office, August 11, 2011, http://www.number10.gov.uk/news/pm-statement-on-disorder-in-england/; "England riots: Government mulls social media controls," BBC News, August 11, 2011. http://www.bbc.co.uk/news/technology-14493497.
[70] Brian Wheeler, "Twitter users: A guide to the law," BBC News Magazine, February 26, 2013, http://www.bbc.co.uk/news/magazine-20782257.

information to light on the government's widespread surveillance of ICTs for counterterrorism and law enforcement purposes. Privacy groups have criticized the measures as disproportionate and lacking legal oversight.

After much controversy, the Digital Economy Act (DEA) was adopted in April 2010.[71] The DEA grants the government the power to impose rules on ISPs, such as monitoring and notifying their users after they receive information or reports containing evidence of infringement, even if these allegations are not proven in a court or independent hearing. If surveys and data indicate that this does not result in an overall reduction of infringement in the UK, the DEA provides for a second phase that allows the government to authorize "technical measures," such as limiting access speeds and cutting off access altogether. The ISPs BT and TalkTalk, together with free expression and consumer groups, filed a legal challenge to the DEA in 2010.[72] However, the High Court rejected most of the challenge in April 2011[73] and the decision was upheld by the Court of Appeal in March 2012.[74]

In June 2012, communications regulator Ofcom published an Obligations Code, which specifies when and how ISPs will issue warning notices to their customers who are thought to be illegally accessing copyright-protected material.[75] The code provides for a graduated response, where ISPs must monitor IP addresses and send notifications to users of possible copyright infringement. After a user receives three notifications in a year, copyright owners may request users' personal details and initiate legal action against them. The code allows customers to appeal any such allegation for a £20 ($31) fee. The cost has been criticized as unjust,[76] particularly given the courts' skepticism about the reliability of identifying infringers using IP addresses.[77]

Ofcom clarified in June 2012 that only those ISPs providing service to over 400,000 broadband-enabled lines are required to implement the graduated response scheme explained above.[78] Therefore, most libraries and providers of wireless hotspots would not be obligated to monitor and notify users. Additionally, the "technical measures" phase of the DEA cannot be initiated until the

[71] The Digital Economy Act 2010 (c. 24), available at Office of Public Sector Information, accessed May 25, 2013, http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1.
[72] "ISPs Take Digital Economy Act to the Courts," Out-Law.com, July 8, 2010, http://www.out-law.com/default.aspx?page=11211; "Skeleton Argument on Behalf of Consumer Focus and ARTICLE 19," ARTICLE 19, March 10, 2011. http://www.article19.org/data/files/pdfs/submissions/skeleton-argument-on-behalf-of-consumer-focus-and-article-19.pdf.
[73] British Telecommunications Plc & Anor, R (on the application of) v. The Secretary of State for Business, Innovation and Skills [2011] EWHC 1021 (Admin) (April 20, 2011). See also, Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012] EWHC 268 (Ch) (February 20, 2012); Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012] EWHC 1152 (Ch) (May 2, 2012).
[74] British Telecommunications Plc, R (on the application of) v. BPI (British Recorded Music Industry) Ltd & Ors [2012] EWCA Civ 232 (March 6, 2012).
[75] Ofcom, "Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations," June 26, 2012, http://stakeholders.ofcom.org.uk/consultations/infringement-notice/.
[76] "O2 disclosure ruling could impact on workings of imminent new anti-piracy code, campaigners say," Out-Law.com, March 29, 2012, http://www.out-law.com/en/articles/2012/march1/o2-disclosure-ruling-could-impact-on-workings-of-imminent-new-anti-piracy-code-campaigners-say/.
[77] See, Golden Eye (International) Ltd & Anor v. Telefonica UK Ltd [2012] EWHC 23 (Ch) (March 26, 2012).
[78] Ofcom, "Online Infringement of Copyright and the Digital Economy Act 2010.

Obligations Code is in force for 12 months.[79] Delays in implementation of the Code have made it unlikely that ISPs will be required to take these measures earlier than 2015.[80]

In recent years, threats of libel suits were causing significant chilling effects on both content producers and ISPs, particularly due to the heavy financial and evidentiary burden on defendants.[81] This worsened due to an increase in "libel tourism," a practice in which foreign litigants with little or no connection to the country exploit the ubiquity of online content to invoke plaintiff-friendly English libel laws against their critics.[82] In a positive sign, updates to the Defamation Act passed in April 2013[83] place restrictions on libel tourism by requiring claimants to show that, of all the places in which the statement has been published, England and Wales are clearly the most appropriate places in which to bring legal action.[84] The act also codifies defenses of "truth," "honest opinion," and "publication on matters of public interest."

Nonetheless, there has also been an increased use of libel law for offending Twitter posts, with some cases resulting in substantial damages. In April 2013, it was reported that a British woman was being sued by a Qatari company for defamatory tweets. The dispute arose after the woman took to Twitter to complain of an outstanding payment of £146 ($226), and later £25 ($39), for services rendered. If found guilty, the woman could be ordered to pay up to £120,000 ($186,000) in libel damages.[85]

In addition to questions surrounding intellectual property enforcement and libel, the government has taken strong measures against users who post or download information perceived as a security threat. General laws such as the Public Order Act and the 2003 Communications Act are increasingly being used to charge individuals with crimes for posting threatening or harassing materials on the internet. For example, Paul Chambers had been convicted in 2010 under Section 127 of the Communications Act of 2003, which prohibits sending "by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character."[86] Chambers had used Twitter to express dismay at the closing of the local airport, jokingly writing that he would blow up the airport if it did not reopen within a week.[87] The High Court overruled his conviction in July 2012, finding that the statement was not one of a menacing character.[88]

---

[79] The Digital Economy Act 2010 (c. 24), section 10(2).
[80] Peter Bradwell, "Even more delays to the Digital Economy Act," Open Rights Group (blog), February 4, 2013, http://www.openrightsgroup.org/blog/2013/even-more-delays-to-the-digital-economy-act.
[81] Section 1, Defamation Act 1996; see Jo Glanville and Jonathan Heawood, eds., *Free Speech Is Not for Sale: The Impact of English Libel Law on Freedom of Expression* (London: Index on Censorship/English PEN, 2009), http://bit.ly/8bC7BX.
[82] "Libel Tourism: Writ Large," The Economist, January 8, 2009, http://www.economist.com/world/international/displaystory.cfm?story_id=12903058.
[83] See, Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), http://services.parliament.uk/bills/2012-13/defamation.html.
[84] Defamation Act 2013 (c. 26).
[85] "Lesley Kemp faces libel suit over Twitter comments," BBC News, April 22, 2013, http://bbc.in/14CqEnO.
[86] Section 127, Communications Act 2003, http://www.legislation.gov.uk/ukpga/2003/21/section/127.
[87] David Allen Green, "Paul Chambers: A Disgraceful and Illiberal Judgment," Jack of Kent (blog), May 11, 2010, http://jackofkent.blogspot.com/2010/05/paul-chambers-disgraceful-and-illiberal.html.
[88] Chambers v Director of Public Prosecutions [2012] EWHC 2157 (QB), July 27, 2012.

In December 2012, the Director of Public Prosecutions launched a three-month consultation on guidelines for prosecuting cases involving communications sent via social media. The proposed guidelines include robust prosecution of communications that may be perceived as credible threats, specifically target an individual or individuals, or amount to a breach of a court order.[89] In contrast, communications that are offensive, indecent, obscene, or false, are unlikely to be subject to prosecution.[90] Article 19, a human rights organization that focuses on promoting freedom of expression, welcomed the guidelines but cautioned that they could still leave room for abuse of prosecutorial discretion.[91]

Speaking in June 2011, the Attorney General stated that social media users who violate court injunctions, such as those that aim to prevent the publication of information about pending court cases in which one of the parties is not named, could face criminal charges for contempt of court.[92] For example, legal proceedings were reportedly launched in February 2013 against several online users for publishing photos of a convicted killer, despite a court injunction to ban the publication of anything which could reveal the killer's identity.[93] In a similar case from late 2012, nine users were each ordered to pay a fine of £624 ($967) for revealing the identity of a rape victim over social networks. According to the 1992 Sexual Offences Act, victims and alleged victims of rape have a right to anonymity.[94] Social media users can also face punishments from their employers for statements made online. A police officer was forced to resign after posting a series of tweets celebrating the death of the late prime minister Margaret Thatcher.[95]

There is continued concern about surveillance as authorities have increasingly used or misused the powers granted under the Regulation of Investigatory Powers Act (RIPA).[96] The law covers the interception of communications; the acquisition of communications data, including billing data; intrusive surveillance, such as on residential premises or in private vehicles; covert surveillance in the course of specific operations; the use of covert human intelligence sources like agents, informants, and undercover officers; and access to encrypted data. A Secretary of State may also require that communications providers maintain interception capabilities, including systems to record internet traffic on a large scale. Under current rules, RIPA allows national government agencies and over 400 local bodies to access communication records for a variety of reasons, from national security to tax collection. Orders for interception and access to the content of

[89] "Interim guidelines on prosecuting cases involving communications sent via social media," Director of Public Prosecutions, December 19, 2012, http://www.cps.gov.uk/consultations/social_media_consultation.html.
[90] "Interim guidelines on prosecuting cases involving communications sent via social media," Director of Public Prosecutions.
[91] Article 19, "UK: Social media guidelines for prosecutors welcomed but practical application remains to be seen," Dec. 19, 2012, http://www.article19.org/resources.php/resource/3569/en/uk:-social-media-guidelines-for-prosecutors-welcomed-but-practical-application-remains-to-be-seen.
[92] Tara Conlan, "Twitter users who breach injunctions risk legal action, warns attorney general," Guardian, June 7, 2011, http://www.guardian.co.uk/media/2011/jun/07/twitter-users-injunctions-legal-action.
[93] Brian Wheeler, "Twitter users: A guide to the law," BBC News Magazine, February 26, 2013, http://www.bbc.co.uk/news/magazine-20782257.
[94] Press Association, "Ched Evans Rape Case: Twitter Users Who Named Victim Fined £624 Each in Landmark Case," November 5, 2012, Huffington Post UK, http://www.huffingtonpost.co.uk/2012/11/05/ched-evans-twitter-users-fined_n_2077186.html.
[95] "Thatcher: Policeman Quits Over Tweets," Sky News, April 12, 2013, http://news.sky.com/story/1077308/thatcher-policeman-quits-over-tweets.
[96] See generally, the Explanatory Notes to Regulation of Investigatory Powers Act, accessed January 2009, http://www.legislation.gov.uk/ukpga/2000/23/notes/contents.

communications require approval from a Secretary of State, such as the Home Secretary or Foreign Secretary. In 2011, there were 494,078 requests for communications data from telephone companies (including mobile phone service providers) and ISPs—a decrease of 11 percent from the previous year.[97] According to the Interception Commissioner, there were nearly 900 instances where records were incorrectly obtained by authorities and two persons were incorrectly detained based on mistakes in the communications data.[98]

According to amendments to RIPA that were introduced through the Protection of Freedoms Act, local authorities must acquire the approval of a magistrate in order to access communications data.[99] The act, approved on May 1, 2012, seemingly imposed important limits on surveillance powers. However, from June 2013 onwards, details have emerged over the secret surveillance practices of the Government Communications Headquarters (GCHQ), often in collaboration with the National Security Agency (NSA) of the United States. These revelations indicate that a significant amount of surveillance is currently taking place outside of this particular legal framework.

Through a series of leaks obtained by the *Guardian* newspaper, it was revealed that the GCHQ has been conducting a secret surveillance project, codenamed "Tempora," since the fall of 2011. A part of the GCHQ's larger "Mastering the Internet" program, Tempora was launched to create an "internet buffer" consisting of massive amounts of user data obtained from undersea fiber-optic cables landing in the UK. Under Tempora, the content of communications—phone calls, e-mails, social networking posts, private messages, and more—can be stored for three days while it is processed by intelligence agents; metadata is stored for 30 days. The intercept probes—referred to in GCHQ documents as "special source exploitation"—reportedly gave the agency access to 200 fiber-optic cables by 2012, each carrying a load of 10 Gbps of data. An obscure clause within RIPA served as the legal basis for this practice. Under the provision, this sort of broad surveillance may be signed off by the foreign secretary or home secretary if communications data is arriving from or departing to foreign soil. [100] However, since the UK's fiber-optic network often provides for domestic traffic to be routed through international cables before returning to the island, the provision allows for the GCHQ to conduct widespread surveillance over most, if not all of UK citizens.[101]

Furthermore, by collaborating with their U.S. government partners, the GCHQ is able to bypass legal protections coded in RIPA in order to obtain information on British citizens from the NSA's PRISM program, which gave the NSA access to the private communications of foreign nationals

[97] Rt Hon Sir Paul Kennedy, "2011 Annual Report of the Interception of Communications Commissioner," House of Commons, June 13, 2012, http://www.intelligencecommissioners.com/docs/0496.pdf.
[98] Ibid; Alan Travis, "Snooping errors twice led to wrongful detention, watchdog reveals," Guardian, July 13, 2012, http://www.guardian.co.uk/uk/2012/jul/13/snooping-errors-wrongful-detention-watchdog.
[99] Protection of Freedoms Act, http://www.legislation.gov.uk/ukpga/2012/9/enacted.
[100] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," The Guardian, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
[101] Nick Hopkins, "NSA and GCHQ spy programmes face legal challenge," The Guardian, July 8, 2013, http://www.theguardian.com/uk-news/2013/jul/08/nsa-gchq-spy-programmes-legal-challenge.

through secret information sharing agreements with major U.S. internet companies. At the same time, the arrangement allowed the GCHQ to pass on information to the NSA regarding U.S. citizens, thereby bypassing American restrictions on domestic surveillance. Indeed, according to leaked internal documents, the GCHQ facility in Cheltenham reportedly "produces larger amounts of metadata collection than the NSA."[102] In another internal document, the GCHQ praised its intelligence collecting and information sharing efforts, stating that the NSA was "delighted by our unique contributions against the [unsuccessful] Times Square and Detroit bombers."[103] Documents also revealed that the U.S. government has provided at least £100 million ($155 million) in funding to the GCHQ over the past few years, leading some observers to conclude that the U.S. government was essentially paying to use information obtained by the UK government.[104] Privacy advocates, such as Privacy International, have criticized the programs as "blanket surveillance," lacking judicial oversight and disproportionately affecting the rights guaranteed in Article 8 of the European Convention of Human Rights.[105]

In 2009, regulations to implement the EU Data Retention Directive were adopted.[106] Under the directive, providers must retain communications data on all users for 12 months, including mobile phone location and e-mail logs, but excluding the content of the communications. ISPs can also continue to "voluntarily" store web-access logs and government agencies may access this information through the procedures in RIPA.[107] In May 2012, the government announced the Communications Capabilities Development Programme (CCDP), a proposal to require ICT service providers to retain data on phone calls, e-mails, text messages, and communications on social-networking sites in order to combat terrorism and organized crime.[108] This was incorporated into a draft Communications Data Bill, which if passed would also expand the real-time surveillance capabilities of the security services and require ISPs to monitor users.[109] Progress on the bill has stalled, however, and on April 25, 2013, Deputy Prime Minister Nick Clegg announced that the bill was unlikely to be implemented during the current government.[110] According to the *Guardian*, British telecommunications giants BT and Vodafone Cable, as well as several other international companies, have been collaborating with the GCHQ under secret agreements to tap into

[102] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, and James Ball, "Mastering the internet: how GCHQ set out to spy on the world wide web, " The Guardian, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet?INTCMP=SRCH.
[103] Nick Hopkins, Julian Borger, Luke Harding, "GCHQ: inside the top secret world of Britain's biggest spy agency," The Guardian, August 1, 2013, http://www.theguardian.com/world/interactive/2013/aug/01/gchq-spy-agency-nsa-edward-snowden#part-six.
[104] Nick Hopkins and Luke Harding, "GCHQ accused of selling its services after revelations of funding by NSA," The Guardian, August 2, 2013, http://www.theguardian.com/uk-news/2013/aug/02/gchq-accused-selling-services-nsa.
[105] Nick Hopkins, "NSA and GCHQ spy programmes face legal challenge," The Guardian, July 8, 2013, http://www.theguardian.com/uk-news/2013/jul/08/nsa-gchq-spy-programmes-legal-challenge.
[106] The Data Retention (EC Directive) Regulations 2009 (SI 2009 No. 859), April 2, 2009, http://www.legislation.gov.uk/ukdsi/2009/9780111473894.
[107] See, The Retention of Communications Data (Code of Practice) Order 2003, http://www.legislation.gov.uk/uksi/2003/3175/made.
[108] David Barrett, "Phone and email records to be stored in new spy plan," The Telegraph, February 18, 2012, http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html.
[109] See, Draft Communications Data Bill, http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/.
[110] Kelly Fiveash, "Nick Clegg: Snooper's Charter 'isn't going to happen,'" The Register, April 25, 2013, http://bit.ly/10eLMYz.

transatlantic cables. The companies have responded to the allegations by stating that they are obliged to hand over user data under UK and European Union law.[111]

There are no public restrictions on the use of encryption technologies. However, under Part 3 of RIPA, it is a crime not to disclose an encryption key upon an order from a senior policeman or a High Court judge. The Court of Appeal held in 2008 that such disclosure would not necessarily violate the privilege against self-incrimination.[112] There has been increasing use of the provision to obtain court orders to force disclosure of keys. Between April 2011 and March 2012, there were 33 court orders for decryption, 14 people charged with refusing to disclose their keys, and 2 convictions for refusal to disclose.[113]

There have been numerous cyber-hacking incidents in the UK in the previous year. Apart from intrusions for fraud and other criminal purposes, activist hacking groups have targeted both commercial[114] and government bodies[115] In addition, police have launched two major investigations—Operation Tuleta and Operation Kalmyk—into whether News International illegally hacked the e-mails of various persons, resulting in a number of arrests.[116]

[111] James Ball, Luke Harding, Juliette Garside, "BT and Vodafone among telecoms companies passing details to GCHQ," The Guardian, August 2, 2013, http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq?INTCMP=SRCH.
[112] S & Anor, R v [2008] EWCA Crim 2177 (October 09, 2008).
[113] Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2011-2012* (London: Stationary Office, July 2012), http://www.official-documents.gov.uk/document/hc1213/hc04/0498/0498.pdf; Chris Williams, "UK Jails Schizophrenic for Refusal to Decrypt Files," The Register, November 24, 2009, http://www.theregister.co.uk/2009/11/24/ripa_jfl/.
[114] Rupert Steiner, "City Focus: Hacking Britain – Cyber crime costs UK up to £27bn a year," This is Money, February 19, 2013, http://www.thisismoney.co.uk/money/news/article-2280777/CITY-FOCUS-Hacking-Britain--Cyber-crime-costs-UK-27bn-year.html/.
[115] Josh Halliday, "Anonymous hits UK government websites over Julian Assange row," The Guardian, August 21, 2012, http://www.guardian.co.uk/technology/2012/aug/21/anonymous-hits-government-websites-julian-assange.
[116] See, The Report into the Culture, Practices and Ethics of the Press, Volume I, Part E, Chapter 5, November 29, 2012, http://www.levesoninquiry.org.uk/about/the-report/; "Leveson Inquiry: Police reveal 'likely' victim numbers," BBC News, February 6, 2012, http://www.bbc.co.uk/news/uk-16905465.

UNITED STATES

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	4	4
Limits on Content (0-35)	1	1
Violations of User Rights (0-40)	7	12
Total (0-100)	12	17

* 0=most free, 100=least free

POPULATION: 313.9 million
INTERNET PENETRATION 2012: 81 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Leaked documents revealed widespread surveillance by the U.S. National Security Agency (see **VIOLATIONS OF USER RIGHTS**).
- The U.S. House of Representatives voted in favor of the Cyber Information Sharing and Protection Act (CISPA), a piece of proposed legislation that threatened to undermine user privacy. The bill was subsequently shelved by the Senate (see **VIOLATIONS OF USER RIGHTS**).
- Aggressive prosecution of Aaron Swartz, who committed suicide before receiving a sentence, fueled calls to reform the Computer Fraud and Abuse Act (CFAA) (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

The following chapter covers developments in the United States until April 30, 2013. However, in June and July 2013, the British newspaper The Guardian *and the American* Washington Post *reported a series of leaks from a former contractor for the U.S. National Security Agency (NSA), which revealed that the extent of government surveillance of telephone records and internet activity is greater than had previously been acknowledged. Given that this surveillance has been ongoing for a number of years—including during the period covered by this report—Freedom House has decided to include it in this edition of Freedom on the Net (see Violations of User Rights).*

INTRODUCTION

Access to the internet in the United States remains relatively free compared with the rest of the world. Users face few restrictions on their ability to access and publish content online. The courts have consistently held that federal and state constitutional prohibitions against government regulation of speech apply to material published on the internet. The law also protects online service providers from liability for infractions committed by their users, a policy that fosters business models that permit open discourse and the free exchange of information.

Several recent developments, however, have placed the government and internet freedom advocates at odds over aspects of internet policy, especially with respect to online surveillance and privacy. In June and July 2013, a series of secret documents leaked to *The Guardian* and the *Washington Post* revealed that the National Security Agency (NSA) is conducting widespread surveillance on phone records and internet activities of American citizens and people around the world. In addition, in April 2013 the House of Representatives voted in favor of the Cyber Information Sharing and Protection Act (CISPA), which is intended to increase information sharing between companies and the government for the purpose of cybersecurity. Critics argued that the House bill was overly broad and could threaten user privacy if it were to become law;[1] the bill was subsequently shelved by the Senate.[2]

Prosecutions under the Computer Fraud and Abuse Act (CFAA) continued to raise concerns about the application of the law to prosecute crimes committed by online users, particularly in the case of Aaron Swartz, who was prosecuted under the CFAA for using the Massachusetts Institute of Technology's network to download nearly 5 million academic articles. This case reignited calls for amending the legislation, which critics argue is too broadly worded, particularly in regard to the meaning of the offense of accessing a computer "without authorization." In recent years, the CFAA has been used to prosecute crimes that fall outside of traditional concepts of cybercrime.

[1] "House Passes CISPA," Center for Democracy and Technology PolicyBeta Blog, April 18, 2013, https://www.cdt.org/pr_statement/house-passes-cispa.
[2] Jason Koebler, "ACLU: CISPA is Dead (For Now)," US News and World Report, April 25, 2013, http://www.usnews.com/news/articles/2013/04/25/aclu-cispa-is-dead-for-now.

Social networks and microblogging sites have been prominent targets for government demands to disclose data about users. The microblogging site Twitter received subpoenas requesting data identifying users, including individuals affiliated with the anti-secrecy organization WikiLeaks and the Occupy Wall Street movement. Twitter challenged a subpoena requesting records on an Occupy Wall Street protestor, but in September 2012 a court ruled that the company had to turn over the information, and Twitter complied.

OBSTACLES TO ACCESS

Access to the internet in the United States is largely unregulated. It is provided and controlled in practice by a small group of private cable television and telephone companies that own and manage the network infrastructure. This model has been questioned by observers who have warned that insufficient competition in the ISP market could lead to some increases in the cost of access, thus adversely affecting the economy and individuals' participation in civic life, which increasingly occurs online.[3] Observers have cautioned that if "network neutrality" regulations (discussed in greater detail below) prove too weak or are rejected by the courts, the dominant companies may decide not to continue to carry internet traffic in a content-neutral fashion.

Although the United States is one of the most connected countries in the world, it has fallen behind several other developed countries in terms of internet speed, cost, and broadband availability.[4] Approximately 81 percent of all Americans had access to the internet in 2012,[5] but only 65 percent of adults used high-speed broadband connections as of December 2012.[6] While the broadband penetration rate is considered high by global standards, it puts the United States significantly behind countries such as Switzerland, the Netherlands, Denmark, and South Korea. Lack of high-speed internet access is especially prevalent in rural areas, where low population densities make it difficult for private companies to justify large investments in network infrastructure. Wired broadband service is not yet available to 7 percent of U.S. residents, most of whom live in rural counties.[7] A June 2012 Federal Communications Commission (FCC) and National Telecommunications and Information Administration (NTIA) report indicated that 18 percent of rural residents in the

[3] Mark Cooper, "The Socio-Economics of Digital Exclusion in America, 2010," paper presented at 2010 TPRC: 38th Research Conference on Communications, Information, and Internet Policy, Arlington, Virginia, October 1–3, 2010.

[4] According to a study by the Organisation for Economic Cooperation and Development (OECD), as of June 2012 the United States was ranked 8th among the OECD member countries in terms of mobile wireless broadband subscriptions per 100 inhabitants, and was ranked even lower, at 15th, on fixed-line broadband penetration. See, OECD Broadband Statistics, "OECD Fixed (Wired) Broadband Subscriptions per 100 Inhabitants, by Technology, June 2012," and "OECD Terrestrial Mobile Wireless Broadband Subscriptions per 100 Inhabitants, by Technology, June 2012," accessed April 10, 2013, http://www.oecd.org/sti/broadband/1d-OECD-WiredWirelessBB-2012-6.xls.

[5] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2012, accessed June 26, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[6] "Pew Internet: Broadband," Pew Internet & American Life Project, accessed April 10, 2013. http://pewinternet.org/Commentary/2012/May/Pew-Internet-Broadband.aspx.

[7] Anne Neville, "Two Years and Five Updates for the National Broadband Map," National Broadband Map Blog, January 31, 2013, http://www.broadbandmap.gov/blog/2956/two-years-and-five-updates-for-the-national-broadband-map.

United States lack access to fixed broadband. However, mobile broadband is becoming an option for an increasing number of people.[8]

Senior citizens, Spanish-speakers, adults with less than a high school education, and those living in households earning less than $30,000 annually are the groups least likely to use the internet, though internet penetration has been growing at significantly higher rates among minorities than it has within the general population. In a survey conducted by the Pew Internet and American Life Project, when asked why they do not use the internet, many nonusers said they did not see the internet's relevance in their lives. They also cited factors such as usability and price as key deterrents. Approximately one in five nonusers said they know enough about technology that they could use the internet on their own.[9]

Mobile devices have become ubiquitous in the United States, with 98 mobile phone subscriptions per 100 residents.[10] As of mid-2012, about 63 percent of adult mobile phone users reported accessing the internet on their phones. Young adults, minorities, those with less than a college education, and those with lower household income are the most likely to say that a phone is their primary source of internet access.[11] A growing number of people use their phones to check e-mail, visit social-networking sites such as Facebook, and engage in online commerce. This has prompted many companies to develop special applications and versions of their websites that are designed for mobile phone viewing.

No single agency governs the internet in the United States. The Federal Communications Commission (FCC), an independent agency of the executive branch, is charged with regulating radio and television broadcasting, all interstate communications, and all international telecommunications that originate or terminate in the United States. Although the FCC is not specifically tasked with regulating the internet or ISPs, it has claimed jurisdiction over some internet-related issues. Other government agencies, such as the National Telecommunications and Information Administration (NTIA), also play advisory or executive roles with respect to telecommunications, economic, and technological policies and regulations. It is the role of the U.S. Congress to create laws that govern the internet and delegate regulatory authority. Government agencies such as the FCC and the NTIA must act within the bounds of congressional legislation.

Recognizing that internet penetration and connection speeds in the United States have been outpaced by those in several other developed countries, Congress devoted funding to improving the nation's broadband infrastructure and instructed the FCC to create a National Broadband Plan that promotes broadband availability for all U.S. residents. After issuing a notice of inquiry in April

[8] National Broadband Map, "Broadband Statistics Report: Broadband Availability in Urban vs. Rural Areas," Report published January 2013, http://www.broadbandmap.gov/download/Broadband%20Availability%20in%20Rural%20vs%20Urban%20Areas.pdf.
[9] Kathryn Zickuhr & Aaron Smith, "Digital Differences," Pew Internet and American Life Project, April 13, 2012, http://pewinternet.org/~/media//Files/Reports/2012/PIP_Digital_differences_041312.pdf.
[10] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2013, accessed June 26, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[11] Kathryn Zickuhr & Aaron Smith, "Digital Differences," Pew Internet and American Life Project, April 13, 2012, http://pewinternet.org/~/media//Files/Reports/2012/PIP_Digital_differences_041312.pdf.

2009 and weighing input from a wide variety of business, government, and civil society organizations,[12] the FCC issued its National Broadband Plan in March 2010. First among the goals was to provide at least 100 million U.S. homes with "affordable access to actual download speeds of at least 100 megabits per second and actual upload speeds of at least 50 megabits per second."[13] Three years after its implementation, the results of the National Broadband Plan are mixed. According to a 2013 report by the Congressional Research Office, the country is much closer to reaching its broadband availability goals than its broadband adoption goals. While it seems likely that 100 million U.S. homes will soon have access to the target download speeds, cost of service is still a major issue.[14]

Despite the economic recession, the United States is home to a thriving communications start-up community where innovators and entrepreneurs regularly offer new technological tools at no monetary cost to the public. Popular web applications such as Twitter, the video-sharing site YouTube, the social-networking site Facebook, and international blog-hosting services such as WordPress are all freely available.

Between 3,000 and 4,000 ISPs currently operate in the United States, although 15 of them control approximately 80 percent of the market, and four—AT&T, Comcast, Time Warner, and Verizon—control approximately 50 percent and own the majority of network cables and other infrastructure.[15] Until 2005, U.S. telephone companies were required to grant "nondiscriminatory" access to their wire networks to other ISPs to ensure open retail-level competition and optimal service for consumers. However, in 2005, the FCC embraced an aggressive deregulation agenda and freed the network owners from any obligation to lease their lines to competing ISPs. The proponents of deregulation claimed that this step would provide more incentive for large cable and telephone companies to further develop and upgrade their networks, while opponents claimed that it would lead to higher prices, fewer options for consumers, and worse service. Broadband speeds have increased, but a majority of Americans remain limited to three or fewer options when choosing a broadband provider offering at least 3 Mbps for downstream speeds and 768 Kbps for upstream speeds.[16]

Over the last decade, policymakers in the United States have engaged in deep debates over the concept of "network neutrality," according to which network providers must treat all content, websites, and platforms equally when managing data traffic.[17] Supporters of the principle argue that without it, ISPs would be able to block certain content and applications, or give preferential

[12] Stephanie Condon and Marguerite Reardon, "FCC Seeks Input on National Broadband Plan," CNet News, April 8, 2009, http://news.cnet.com/8301-13578_3-10214974-38.html.
[13] "National Broadband Plan: Connecting America," Federal Communications Commission (FCC), 2010, http://www.broadband.gov/download-plan/.
[14] Lennard G. Kruger, "The National Broadband Goals: Where Do We Stand?" Congressional Research Service, March 19, 2013, http://www.fas.org/sgp/crs/misc/R43016.pdf.
[15] "ISP Usage and Market Share: ISP Trends, Stats and Analysis," StatOwl.com, November 2012, http://www.statowl.com/network_isp_market_share.php.
[16] Federal Communications Commission (FCC), "Internet Access Services: Status as of December 31, 2011," http://www.fcc.gov/document/fcc-releases-new-data-internet-access-services-6.
[17] Tim Wu, "Network Neutrality FAQ," Timwu.org, accessed August 17, 2011, http://timwu.org/network_neutrality.html.

treatment to some content providers for a fee, a practice that could place limitations on citizen access to information and online services.

Although concerns about net neutrality began emerging in the early 2000s, the issue did not gain widespread attention until 2007 when FCC investigators found that Comcast, a cable-television company and major ISP, had begun slowing down and blocking certain types of peer-to-peer file-sharing traffic.[18] After a long court battle on the issue, a federal appeals court sided with Comcast in April 2010 and overturned the FCC's ruling against the company. The decision, which came shortly after the release of the National Broadband Plan, also found that the FCC did not have the authority to regulate ISPs under the legal framework the agency had cited, challenging its ability to protect consumers on the internet.[19]

In December 2010, the FCC issued a compromise ruling on net neutrality that instructs fixed-line service providers not to block access to, or unreasonably discriminate against, lawful websites, applications, devices, or services. The rules for wireless broadband providers are much more limited, however, restricting only some types of blocking and saying nothing about discrimination. Under separate FCC licensing rules covering the operation of a particular range of radio communication frequencies, some wireless carriers are barred from discriminating among devices and applications, but these rules are not universally applied.[20] In 2011, some advocates filed a complaint with the FCC alleging that Verizon had violated these licensing rules by demanding that certain applications (specifically, applications that enable a mobile device to create a wireless "hotspot," essentially sharing its connection with other devices) be removed from Google's application store. In 2012, Verizon settled this complaint with the FCC, agreeing that the company would not restrict the availability of such applications.[21]

Under the rules for fixed-line internet service, referred to sometimes as the "Open Internet Rules," ISPs are allowed to offer tiered services at different prices.[22] Some civil society organizations, though they agreed that the FCC adopted the rules in a free, fair, and independent manner,[23] expressed disappointment that the Commission did not take a stronger stance on net neutrality that would have applied the Communications Act's "common carrier" provisions. The FCC's rules officially took effect in November 2011.

---

[18] Peter Svensson, "Comcast Blocks Some Internet Traffic," MSNBC, October 19, 2007, http://www.msnbc.msn.com/id/21376597/ns/technology_and_science-internet/.

[19] *Comcast Corporation v. Federal Communications Commission, No. 08-1291, U.S. Court of Appeals for the District of Columbia Circuit (April 6, 2010),* http://www.cadc.uscourts.gov/internet/opinions.nsf/EA10373FA9C20DEA85257807005BD63F/$file/08-1291-1238302.pdf.

[20] U.S. Code of Federal Regulations, Title 47, sec. 27.16, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=82f1f40e3b6b119c316bbb90292bb254&rgn=div8&view=text&node=47:2.0.1.1.5.2.49.7&idno=47.

[21] Federal Communications Commission, Consent Decree In the Matter of Cellco Partnership d/b/a Verizon Wireless, DA 12-1228, July 31, 2012, http://fjallfoss.fcc.gov/edocs_public/attachmatch/DA-12-1228A1.pdf.

[22] "Report and Order: In the Matter of Preserving the Open Internet, Broadband Industry Practices," FCC 10-201, December 21, 2010, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf.

[23] "Network Neutrality," Public Knowledge, accessed April 28, 2012, http://www.publicknowledge.org/issues/network-neutrality.

Verizon v. FCC, a case challenging these rules, is pending before the Court of Appeals in Washington, D.C., the same appellate court that overturned the FCC's ruling in the Comcast case.[24] The telecommunications company Verizon argues that the FCC lacks the statutory authority to adopt the Open Internet Rules. The company further argues that it has a First Amendment right to exercise "editorial discretion" over the content it transmits, a right it argues renders unconstitutional the FCC's requirement that it not block or interfere with its customers' access to lawful internet content. Civil society groups filed a series of "friend of the court" briefs countering Verizon's claims, some of which focused specifically on critiquing the company's First Amendment arguments.[25] The court of appeals has scheduled the oral argument in the case for September 2013.

LIMITS ON CONTENT

Access to information on the internet is generally free from government interference in the United States. There is no government-run filtering mechanism affecting content passing over the internet or mobile phone networks. Users with opposing viewpoints engage in vibrant online political discourse and face almost no legal or technical restrictions on their expressive activities online.

Although the government does not restrict any political or social content, legal rules that apply to other spheres of life have been extended to the internet. For example, concerns over copyright violations, child pornography, protection of minors from harmful or indecent content, harassing or defamatory comments, publication of confidential information, gambling, and financial crime have presented a strong impetus for aggressive legislative and executive action.

Advertisement, production, distribution, and possession of child pornography—on the internet and in all other media—is prohibited under federal law and can carry a sentence of up to 30 years in prison. According to the Child Protection and Obscenity Enforcement Act of 1988, all producers of sexually explicit material must keep records proving that their models and actors are over 18 years old. In addition to prosecuting individual offenders, the Department of Justice, the Department of Homeland Security, and other law enforcement agencies have asserted their authority to seize the domain name of a website allegedly hosting child abuse images after obtaining a court order.[26]

Congress has passed several laws designed to restrict adult pornography and shield children from harmful or indecent content, such as the Child Online Protection Act of 1998 (COPA), but they have been overturned by courts due to their ambiguity and potential infringements on the First Amendment of the U.S. Constitution, which protects freedoms of speech and the press. One law

[24] Joint Brief for Verizon and MetroPCS, Verizon v. FCC, 11-1355, DC Circuit.
[25] Andrew McDiarmid, "CDT, Scholars, Technologists, and More Agree: ISPs Shouldn't Have the Right to Edit the Net," Center for Democracy and Technology PolicyBeta Blog, November 16, 2013, https://www.cdt.org/blogs/andrew-mcdiarmid/1611cdt-scholars-technologists-and-more-agree-isps-shouldn%E2%80%99t-have-right-edit-; Lucy Wolf, "Amicus Briefs Counter Verizon's First Amendment Argument in Verizon v. FCC," Public Knowledge Policy Blog, November 19, 2012, http://publicknowledge.org/blog/verizon-v-fcc-amicus-brief-roundup; Josh Levy, "Verizon vs. Humans," Free Press Blog, http://www.savetheinternet.com/blog/2012/11/21/verizon-vs-humans.
[26] Treating domain names as property subject to criminal forfeiture, 18 U.S.C. 2253.

currently in force is the Children's Internet Protection Act of 2000 (CIPA), which requires public libraries that receive certain federal government subsidies to install filtering software that prevents users from accessing child pornography or visual depictions that are obscene or harmful to minors. Libraries that do not receive the specified subsidies from the federal government are not obliged to comply with CIPA, but following the economic downturn, more public libraries have begun to seek federal aid in order to mitigate budget shortfalls.[27] Under the U.S. Supreme Court's interpretation of the law, adult users can request that the filtering be removed without having to provide a justification. However, not all libraries allow this option, arguing that the decisions about the use of filters should be left to the discretion of individual libraries.[28]

In addition to restricting access to universally illegal content such as child pornography, the government has in recent years started more aggressively pursuing alleged infringements of intellectual property rights on the internet. Since 2010, the Immigration and Customs Enforcement (ICE) division of the Department of Homeland Security has engaged in several rounds of domain-name seizures, with targets including blogs and file-sharing sites that allegedly link to illegal copies of music and films and sites that sell counterfeit goods.[29] These seizures have been criticized as extreme and overly secretive; for example, ICE seized the domain name of a legitimate hip-hop music site in November of 2010 and refused to return it for an entire year. The decision to withhold the domain was based on sealed court proceedings to which the owners of the domain were not allowed access.[30] In August 2012, three members of Congress wrote a letter to the U.S. Attorney General raising concerns about whether ICE procedures give websites meaningful due process.[31] However, ICE continues to pursue the project, which is known as "Operation in Our Sights." In January 2013, ICE launched a new "Operation in Our Sights" initiative called "Operation Red Zone," seizing 313 websites allegedly selling counterfeit goods that violate National Football League (NFL) copyrights.[32]

In 2011, the PROTECT IP Act (PIPA) and the Stop Online Piracy Act (SOPA), both of which sought to target websites outside of the United States that host material allegedly infringing on U.S. copyrights, were introduced with bipartisan support in the Senate and House of Representatives, respectively. These bills would have permitted the Attorney General, with little judicial review, to

[27] "Public Library Funding & Technology Access Landscape 2011-2012: Public Library Funding Landscape," American Library Association, p 15, accessed August 6, 2013, http://www.ala.org/research/sites/ala.org.research/files/content/initiatives/plftas/2011_2012/plftas12_funding landscape.pdf.

[28] Bob Bocher, "Children's Internet Protection Act, CIPA: A Brief FAQ on Public Library Compliance," Wisconsin Department of Public Instruction, February 2004, updated March 11, 2010, http://dpi.state.wi.us/pld/cipafaqlite.html. See, e.g., Bradburn v. North Central Regional Library District (Washington state Supreme Court) No. 82200-0 (May 6, 2010); Bradburn v. NCLR, No. CV-06-327-EFS (E.D. Wash. April 10, 2013).

[29] Corynne McSherry, "U.S. Government Seizes 82 Websites: A Glimpse at the Draconian Future of Copyright Enforcement?" Electronic Frontier Foundation, November 29, 2010, https://www.eff.org/deeplinks/2010/11/us-government-seizes-82-websites-draconian-future.

[30] Trevor Timm, "Blacklist Bills Ripe for Abuse Part II: Expansion of Government Powers," Deeplinks Blog, Electronic Frontier Foundation, December 9, 2011, https://www.eff.org/deeplinks/2011/12/blacklist-bills-ripe-abuse-part-ii-expansion-government-powers.

[31] Rep. Zoe Lofgren, Rep. Jason Chaffetz, Rep. Jared Polis, Letter to Attorney General Holder and Secretary Napolitano regarding ICE domain seizures, August 30, 2012, http://lofgren.house.gov/images/Letter_to_AG_Holder_083012.pdf.

[32] "ICE, CBP, USPIS seize more than $13.6 million in fake NFL merchandise during 'Operation Red Zone' *313 websites seized and 23 individuals arrested nationwide for selling counterfeit NFL merchandise," United States Immigration and Customs Enforcement News Release, January 31, 2013,* http://www.ice.gov/news/releases/1301/130131neworleans.htm.

seek orders directing ISPs to block access to domain names of sites allegedly dedicated to infringing activity, even if sites also contained lawful content.

The bills, if passed, would have suppressed legitimate, unquestionably legal speech and posed a threat to the infrastructure of the internet. In recognition of these concerns, technologists, digital rights advocates, companies such as Google and Mozilla, and the internet community at large voiced resounding opposition to the bills. Some estimates of user involvement in this effort include over 10 million signatures to petitions, four million e-mails to legislators, and 115,000 sites blacking out or going dim in protest.[33] In response to these efforts and internal concerns, members of Congress withdrew the bills from consideration. The bills remained shelved as of mid-2013.

The activities of WikiLeaks, which in 2010 published several tranches of U.S. government material that was leaked by U.S. Army intelligence analyst Bradley Manning, triggered a serious debate about the use of the internet to publicize sensitive or classified government documents.[34] WikiLeaks faced the cut-off of service by non-government entities, including Amazon's data storage service[35] and EveryDNS, Wikileaks' domain name service provider.[36] While these and other companies that severed ties with WikiLeaks claimed to be acting independently and without government influence, their decisions came amid fierce public criticism of WikiLeaks by executive branch officials and prominent members of Congress.[37] Bradley Manning pleaded guilty to some charges, was convicted of others and received a lengthy sentence. A federal grand jury investigation of Wikileaks is ongoing, but as of mid-2013, the U.S. government had not filed charges against WikiLeaks or any of the press outlets that republished the documents.[38]

The legality of online gambling is another topic of debate in the United States. Online gambling is governed by a patchwork of laws that have continued to shift over the last year. Currently, 37 states allow betting on games that require some degree of skill, but under U.S. law, certain popular online card games like poker and blackjack are not generally included under the "games of skill" designation.[39] In 2011, the Justice Department delivered a legal opinion clarifying the scope of the Wire Act of 1961 and opening the door for states to legalize many additional forms of gambling,

[33] Fight for the Future, http://sopastrike.com/numbers/.
[34] This information included video footage of a 2007 incident in which journalists and Iraqi civilians were killed by U.S. forces, documents on the wars in Afghanistan and Iraq, diplomatic cables from the U.S. State Department, and reports on prisoners held in Guantanamo Bay military prison, all of which number in the tens and (in the case of the Iraq war) hundreds of thousands.
[35] Geoffrey A. Fowler, "Amazon Says WikiLeaks Violated Terms of Service," Wall Street Journal, December 3, 2010, http://online.wsj.com/article/SB10001424052748703377504575651321402763304.html.
[36] Kevin Poulsen, "WikiLeaks Attacks Reveal Surprising, Avoidable Vulnerabilities," Wired, December 3, 2010, http://www.wired.com/threatlevel/2010/12/wikileaks-domain/.
[37] Ewen MacAskill, "WikiLeaks Website Pulled by Amazon After US Political Pressure," Guardian, December 2, 2010, http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon.
[38] Charlie Savage, "Soldier Admits Providing Files to WikiLeaks," The New York Times, February 28, 2013, http://www.nytimes.com/2013/03/01/us/bradley-manning-admits-giving-trove-of-military-data-to-wikileaks.html?pagewanted=all; Scott Shane, "Solider to Face More Serious Charges in Leak," The New York Times, March 1, 2013, http://www.nytimes.com/2013/03/02/us/manning-to-face-more-serious-charges-in-leak.html?ref=julianpassange.
[39] Julianne Pepitone, "Online Gambling Toes a Confusing Legal Line," CNN Money, June 10, 2013, http://money.cnn.com/2013/06/10/technology/innovation/online-gambling-poker/index.html.

including online poker and other "games of chance."[40] Following the opinion, Nevada, New Jersey, and Delaware legalized online gambling within their borders. Other states are considering similar legislation.[41] The first legal online poker website opened for business in June 2013, although the site is technically only legal for residents of Nevada.[42]

The internet plays a significant role in civic activism in the United States, and the growth of the blogosphere and citizen journalism has changed the ways in which many people receive news. Blogs and electronic media outlets reporting from various points on the political spectrum now have greater readership than most printed periodicals. Nearly all nongovernmental organizations and causes have a presence on the internet and use it for advocacy and social mobilization. E-mail campaigns, online petitions, and YouTube videos have been instrumental in organizing protests, lobbying government bodies, and putting a spotlight on issues ranging from environmental degradation to hate crimes.[43]

Political activity is increasingly moving online. According to a survey by the Pew Center's Internet and American Life Project, 66 percent of social media users have engaged in some form of political or civic activity using these tools. This represents nearly 40 percent of the adult American population. More than one third of social media users have used the tools to encourage others to vote.[44] In the 2012 presidential campaign, contributors increasingly turned to technology when donating money to candidates. Approximately half of the people who donated to a presidential candidate made at least one contribution online or via e-mail. One in ten donors made a contribution via text message or mobile phone app.[45] In addition, politicians at the local, state, and federal level increasingly use e-mail, mobile apps, and online content to garner support and keep their constituents engaged.

VIOLATIONS OF USER RIGHTS

The United States has a robust legal framework that supports free expression rights both online and offline, and the U.S. does not typically prosecute individuals for online speech. The broader picture of user rights in America, however, has become increasingly complex as a series of U.S.

[40] United States Department of Justice, Memorandum "Opinion for the Assistant Attorney General: Whether Proposals by Illinois and New York to Use the Internet and Out-of-State Transaction Processors to Sell Lottery Tickets to In-State Adults Violate the Wire Act," September 20, 2011, http://www.justice.gov/olc/2011/state-lotteries-opinion.pdf.
[41] Deena Beasley and Nichola Groom, "Analysis: U.S. States Race to Capture Online Gaming Bonanza," Reuters, February 28, 2013, http://www.reuters.com/article/2013/02/28/net-us-usa-gambling-idUSBRE91R1O120130228.
[42] Cyrus Farivar, "Ultimate Poker to Become First Legal, Real-Money Online Poker Site in the U.S.," Ars Technica, April 30, 2013, http://arstechnica.com/tech-policy/2013/04/ultimatepoker-to-become-first-legal-real-money-online-poker-site-in-us/.
[43] See for example the Credo "Stop the Tar Sands Pipeline" petition at http://www.credoaction.com/campaign/keystone_obama/index2.html. See also: Steve Williams, "President Obama Signs Hate Crimes Bill—Thank You to the 25,000 Care2 Members That Helped It Reach His Desk!" Care2, October 28, 2009, http://www.care2.com/causes/civil-rights/blog/25-000-care2-members-help-secure-presidents-signature-on-hate-crimes-bill/.
[44] Lee Rainey, Aaron Smith, Kay Lehman Schlozman, Henry Brady, and Sydney Verba, "Social Media and Political Engagement," Pew Internet and American Life Project, October 19, 2012, http://pewinternet.org/~/media//Files/Reports/2012/PIP_SocialMediaAndPoliticalEngagement_PDF.pdf.
[45] Aaron Smith & Maeve Duggan, "Presidential Campaign Donations in the Digital Age," Pew Internet and American Life Project, October 25, 2012, http://pewinternet.org/~/media//Files/Reports/2012/PIP_State_of_the_2012_race_donations.pdf.

government practices, policies, and laws touch on, and in some cases appear to violate, the rights of individuals both inside the U.S. and abroad. Government access to phone and internet records is a major concern, especially following newly revealed information about NSA surveillance practices. Aggressive prosecution under the Computer Fraud and Abuse Act (CFAA) has also been criticized. In addition, the privacy of NGOs, companies, and individual users is threatened by a growing number of cyberattacks initiated by both domestic and international actors.

The U.S. Constitution includes strong protections for free speech and freedom of the press. In 1997, the U.S. Supreme Court held that internet speech was entitled to the highest form of protection under the Constitution, and lower courts have consistently struck down attempts to regulate online content. Two federal laws also provide significant protections for online speech: Section 230 of the Communications Act of 1934 (as amended by the Telecommunications Act of 1996) provides immunity for ISPs and online platforms such as YouTube and Facebook that carry content created by third parties. The Digital Millennium Copyright Act (DMCA) of 1998 provides a safe harbor to intermediaries that take down allegedly infringing material after notice from the copyright owner. These statutes enable companies to develop internet applications and websites without fear that they will be held liable for content posted by users.[46]

The U.S. government generally does not prosecute individuals for posting information on the internet, with the notable exceptions of child pornography and content that infringes on copyright. As of mid-2013, the government had taken no decisive action against either WikiLeaks or site founder Julian Assange, but this may change in the wake of the Bradley Manning trial. Manning's own statements or other testimony may help prosecutors establish whether WikiLeaks played a conspiratorial role in the unauthorized downloading of classified documents from U.S. military computers or in the subsequent transmission of the material to WikiLeaks.[47]

In 2012, federal authorities issued a subpoena to the microblogging service Twitter, requesting information from the Twitter accounts of Manning, Assange, and others associated with WikiLeaks. With the subpoena came a gag order compelling Twitter not to disclose this information to anyone, including the users in question. Twitter attorneys successfully challenged the gag order in court and were able to notify users before disclosing their information to government officials.[48] A similar case arose in May 2012 when New York City's district attorney issued a subpoena to Twitter, requesting tweets and account information of an Occupy Wall Street protester. Twitter asked a state judge to throw out the request, arguing that the protester merited protection under the Fourth Amendment, given that prosecutors had failed to show probable cause necessary to obtain a warrant for the information.[49] Twitter's efforts in court were unsuccessful, and in September 2012

[46] "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," Center for Democracy and Technology, April 2010, http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_%282010%29.pdf.
[47] Scott Shane, "Solider to Face More Serious Charges in Leak," The New York Times, March 1, 2013, http://www.nytimes.com/2013/03/02/us/manning-to-face-more-serious-charges-in-leak.html?ref=julianpassange.
[48] Ryan Singel, "Twitter's Response to WikiLeaks Subpoena Should Be the Industry Standard," Wired, January 10, 2011, http://www.wired.com/threatlevel/2011/01/twitter/.
[49] Dan Goodin, "Twitter fights government subpoena demanding Occupy Wall Street protester info," Ars Technica, May 5, 2012, http://bit.ly/IZHFaO.

the company complied with a court order to produce the user's posts. The defendant pled guilty to disorderly conduct charges in late 2012.[50]

Aggressive prosecution under the Computer Fraud and Abuse Act (CFAA) has fueled growing criticism of that law's scope and application. Under CFAA, it is illegal to access a computer without authorization, but the law fails to define the term "without authorization," leaving the provision open to interpretation in the courts.[51] In one prominent case, programmer and internet activist Aaron Swartz secretly used Massachusetts Institute of Technology servers to download millions of files from a service providing academic articles. Prosecutors sought harsh penalties for Swartz under CFAA, which could have resulted in up to 35 years imprisonment.[52] Swartz committed suicide in early 2013. Shortly after his death, a bipartisan group of lawmakers introduced "Aaron's Law," draft legislation that would prevent the government from using CFAA to prosecute terms of service violations and stop prosecutors from bringing multiple redundant charges for a single crime.[53]

In another case of prosecution under CFAA, online activist Andrew Auernheimer was convicted and sentenced to three and a half years in prison in March 2013. In 2010, Auernheimer found a security breach in AT&T's website that allowed him to access thousands of customers' e-mail addresses, which he claims he then turned over to a journalist at Gawker in order to expose the company's security flaws.[54] Prosecutors used CFAA to convict Auernheimer of identity fraud and conspiracy to access a computer without authorization. In addition to the prison sentence, Auernheimer was ordered to pay over $73,000 in damages to AT&T.

In August 2011, public transit authorities in San Francisco suspended cell phone service in several underground stations of the Bay Area Rapid Transit (BART) system in an effort to impede planned demonstrations regarding the fatal shooting of a man by BART police the month prior. Numerous digital rights advocates and First Amendment scholars called the decision a violation of BART passengers' First Amendment rights and pointed to the international implications of BART's actions.[55] Following the incident, various civil liberties groups filed an emergency petition with the FCC requesting that the agency declare the BART shutdown a violation of the Communications

[50] Russ Buettner, "A Brooklyn Protestor Pleads Guilty After His Twitter Posts Sink His Case," The New York Times, December 12, 2012, http://www.nytimes.com/2012/12/13/nyregion/malcolm-harris-pleads-guilty-over-2011-march.html.
[51] "Computer Fraud and Abuse Act Reform," Electronic Frontier Foundation, accessed August 8, 2013, https://www.eff.org/issues/cfaa.
[52] "Deadly Silence: Aaron Swartz and MIT," The Economist, August 3, 2013, http://www.economist.com/news/international/21582578-campaigner-academic-openness-gains-partial-posthumous-vindication-deadly-silence.
[53] "Rep Zoe Lofgren Introduces Bipartisan Aaron's Law," website of Representative Zoe Lofgren, June 20, 2013, http://www.lofgren.house.gov/images/stories/pdf/aarons law - lofgren - 061913.pdf.
[54] Karen McVeigh, "US hacker Andrew Auernheimer given three-year jail term for AT&T breach," *The Guardian*, March 18, 2013, http://www.theguardian.com/technology/2013/mar/18/us-hacker-andrew-auernheimer-at-t.
[55] David Streitfeld, "Bay Area Officials Cut Cell Coverage to Thwart Protestors," Bits Blog, NYTimes.com, August 12, 2011, http://bits.blogs.nytimes.com/2011/08/12/bay-area-authorities-cut-cell-coverage-to-thwart-protestors/. See also, Cynthia Wong, "Welcome to San Francisco – Next Stop, Cairo?" Center for Democracy and Technology PolicyBeta Blog, August 23, 2011, http://cdt.org/blogs/cynthia-wong/238welcome-san-francisco-next-stop-cairo.

Act.[56] In early 2012, the FCC issued a call for public comment on the issue, but as of mid-2013 the agency had not yet taken further action on the subject.[57] In December 2011, BART adopted a policy outlining the circumstances under which it could shut down service; the policy did not require prior judicial approval but, had it been in place, it would not have allowed for the August 2011 shutdown.[58] In 2012, the California State Assembly and Senate approved a bill that would require a court order before allowing for cell network interruption. Governor Jerry Brown vetoed the bill in September 2012, citing concerns that requiring law enforcement to make certain decisions within six hours of interrupting service could divert attention away from resolving the emergency situation.[59]

Although some of the most popular social media platforms in the United States require users to register and create accounts using their real names through Terms of Service or other contracts,[60] there are no legal restrictions on user anonymity on the internet. Constitutional precedents protect the right to anonymous speech in many contexts. There are also state laws that stipulate journalists' right to withhold the identities of anonymous sources, and at least one such law has been found to apply to bloggers.[61] In April 2011, the Obama administration launched the National Strategy for Trusted Identities in Cyberspace (NSTIC). The stated goal of the effort is to ensure the creation of an "identity ecosystem" in which internet users and organizations can more completely trust one another's identities and systems when carrying out online transactions requiring assurance of identity.[62] The plan specifically endorses anonymous online speech.[63]

Laws that protect internet communications from government monitoring are complex. While in transit, the contents of internet communications are generally protected from government intrusion by constitutional rules against unreasonable searches and seizures,[64] although there is more legal ambiguity with data stored in "the cloud." The courts, however, have held that transactional data about communications—data showing who is communicating with whom and

[56] Mike Masnick, "FCC Asked For Declaratory Ruling That BART Shutting Off Mobile Phone Service Was Illegal," TechDirt (blog), August 31, 2011, http://www.techdirt.com/blog/wireless/articles/20110830/11591515740/fcc-asked-declaratory-ruling-that-bart-shutting-off-mobile-phone-service-was-illegal.shtml.
[57] "Commission Seeks Comment on Certain Wireless Interruptions," Federal Communications Commission, March 1, 2012, http://www.fcc.gov/document/commission-seeks-comment-certain-wireless-service-interruptions.
[58] Michael Cabanatuan, "BART Cellphone Shutdown Rules Adopted," SF Gate, December 2, 2011, http://www.sfgate.com/bayarea/article/BART-cell-phone-shutdown-rules-adopted-2344326.php. See also Gabe Rottman, "Shutting Down Cell Service During Protests: The Constitutional Dimension," ACLU of Northen California, May 1, 2012, http://bit.ly/16Am4bd.
[59] Brian Heaton, "California Governor Vetos Cell Service Shutdown Bill," Government Technology, October 1, 2012, http://www.govtech.com/policy-management/California-Governor-Vetoes-Cell-Service-Shutdown-Bill.html
[60] Erica Newland, Caroline Nolan, Cynthia Wong, and Jillian York, "Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users," Global Network Initiative, September 2011, http://cyber.law.harvard.edu/node/7080.
[61] "Apple v. Does," Electronic Frontier Foundation, accessed August 1, 2012, http://www.eff.org/cases/apple-v-does.
[62] "About NISTIC," National Strategy for Trusted Identities in Cyberspace, accessed April 23, 2013, http://www.nist.gov/nstic/about-nstic.html.
[63] Jay Stanley, "Don't Put Your Trust in 'Trusted Identities,'" Blog of Rights (blog), American Civil Liberties Union, January 7, 2011, http://www.aclu.org/blog/technology-and-liberty/dont-put-your-trust-trusted-identities. See also, Jim Dempsey, "New Urban Myth: The Internet ID Scare," Policy Beta (blog), Center for Democracy and Technology, January 11, 2011, http://www.cdt.org/blogs/jim-dempsey/new-urban-myth-internet-id-scare.
[64] Paul Ohm, "Court Rules Email Protected by Fourth Amendment," Freedom to Tinker, December 14, 2010, http://www.freedom-to-tinker.com/blog/paul/court-rules-email-protected-fourth-amendment.

when—is not protected by the Constitution.[65] Under a set of complex statutes, law enforcement and intelligence agencies can monitor communications and access stored information under varying degrees of oversight as part of criminal or national security investigations. In criminal probes, law enforcement authorities can monitor the content of internet communications in real time only if they have obtained an order, issued by a judge, under a standard that is actually a little higher than the one established by the Constitution for searches of physical places. The order must reflect a finding that there is probable cause to believe that a crime has been, is being, or is about to be committed.

The status of stored communications is more uncertain. One federal appeals court has ruled that the Constitution applies to stored communications, so that a judicial warrant is required for government access.[66] Currently, the Electronic Communications Privacy Act states that the government can obtain access to e-mail or other documents stored in the cloud with a mere subpoena issued by a prosecutor or investigator without judicial approval.[67] As of mid-2013, Congress was considering a proposed reform to ECPA that would require government officials to obtain a warrant before accessing any private communications through online service providers.[68] The requirement would cover e-mail and documents stored using cloud services.[69] The Securities and Exchange Commission (SEC), a civil regulatory agency, has complicated the issue by attempting to amend the bill to secure the authority to obtain stored e-mail and other documents directly from service providers.[70]

Following the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act, which expanded some of the government's surveillance and investigative powers in cases involving terrorism as well as in ordinary criminal investigations. Three expiring provisions of the PATRIOT Act—including the government's broad authority to conduct roving wiretaps of unidentified or "John Doe" targets, to wiretap "lone wolf" suspects who have no known connections to terrorist networks, and to secretly access a wide range of private business records with court orders issued on a broad standard (Section 215)—were renewed for an additional four years in May 2011.[71]

In mid-2013, *The Guardian* and the *Washington Post* revealed a series of secret documents[72] leaked by a former National Security Agency (NSA) contractor that provide new information (and raise many new questions) about surveillance activities conducted by the United States government.

---

[65] "A Brief History of Surveillance Law," Center for Democracy & Technology, accessed August 17, 2011, https://www.cdt.org/issue/wiretap-ecpa.
[66] United States v. Warshak, 09-3176, United States Court of Appeals for the Sixth Circuit.
[67] Ibid.
[68] Greg Nojeim, "Senate 'Dream Team' Introduced ECPA Reform Bill," Center for Democracy and Technology PolicyBeta Blog, March 19, 2013, https://www.cdt.org/blogs/greg-nojeim/1903senate-dream-team-introduces-ecpa-reform-bill.
[69] "ECPA: About the Issue," Digital Due Process, accessed April 23, 2013, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.
[70] Leslie Harris, "The SEC's Power Grab Threatens to Distort the US Justice System," Center for Democracy & Technology, July 31, 2013, https://www.cdt.org/commentary/sec's-power-grab-threatens-distort-us-justice-system.
[71] "Patriot Act Excesses," New York Times, October 7, 2009, http://www.nytimes.com/2009/10/08/opinion/08thu1.html.
[72] e.g. Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," The Guardian, June 5, 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Leaked documents indicate that the Foreign Intelligence Surveillance Court (FISA Court) has interpreted Section 215 of the PATRIOT Act to permit the FBI to obtain orders that compel the largest telephone carriers in the U.S. (Verizon, AT&T, Sprint, and presumably others) to provide the NSA with records of all phone calls made to, from, and within the U.S. on an ongoing basis. These billions of call records include numbers dialed, length of call, and other "metadata."[73] Data are gathered in bulk, without any particularized suspicion about an individual, phone number, or device. NSA analysts may conduct queries on this data without approval from the FISA Court or an independent magistrate.[74]

Leaks also reveal that under a program code-named "PRISM" the NSA has been compelling at least nine large U.S. companies, including Google, Facebook, Microsoft and Apple, to disclose content and metadata relating to e-mails, web chats, videos, images, and documents.[75] PRISM activities occur under Section 702 of the Foreign Intelligence Surveillance Act, which permits the NSA to target the communications of non-U.S. persons who are reasonably believed to be located outside the United States in order to collect "foreign intelligence information."[76] Although the program is targeted at persons abroad, the NSA is able to retain and use information "incidentally" collected about U.S. persons.

Critics have raised concern that the secret NSA programs may violate the 4th Amendment of the United States Constitution, which protects people inside the U.S. (citizens and non-citizens alike) from unreasonable search and seizure, as well as human rights enshrined in international agreements. In June 2013, a diverse coalition of prominent NGOs and companies submitted a letter to Congress urging lawmakers to explicitly prohibit the blanket collection of metadata, investigate actions of the NSA, and hold public officials accountable for unconstitutional surveillance.[77] Legislators have introduced proposals to narrow the scope of NSA activities.[78]

In another concerning case regarding government access to information, the Associated Press reported in May 2013 that, as part of a national security leak investigation, the U.S. Justice Department subpoenaed and gained access to two months of phone records for several reporters following AP coverage of a failed bomb plot in Yemen.[79] Justice Department guidelines specify that, in the course of an investigation, requests for journalists' records should be "as narrowly drawn as possible," and that investigators should attempt to obtain records directly from journalists

[73] For more information on privacy and metadata, see Aubra Anthony, "When Metadata Becomes Megadata: What Government Can Learn," Center for Democracy and Technology PolicyBeta Blog, June 17, 2013, https://www.cdt.org/blogs/1706when-metadata-becomes-megadata-what-government-can-learn-metadata.
[74] "Comparing Two Secret Surveillance Programs," The New York Times, June 7, 2013, http://www.nytimes.com/interactive/2013/06/07/us/comparing-two-secret-surveillance-programs.html.
[75] "NSA Slides Explain the PRISM Data Collection Program," Washington Post, June 6, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.
[76] H.R. 6304 Sec. 702.
[77] Coalition Letter to Congress on U.S. Spying, June 11, 2013, https://www.cdt.org/files/pdfs/CDT-Coalition-NSA-Spying.pdf.
[78] Spencer Ackerman and Paul Lewis, "Congress Eyes Renewed Push for Legislation to Rein in the NSA," The Guardian, August 2, 2013, http://www.theguardian.com/world/2013/aug/02/congress-nsa-legislation-surveillance.
[79] Carrie Johnson, "Justice Department Secretly Obtains AP Phone Records," National Public Radio, May 14, 2013, http://www.npr.org/2013/05/14/183810320/justice-department-secretly-obtains-ap-phone-records.

on a voluntary basis, when possible.[80] The Associated Press has since reported that the government's actions have had a chilling effect on sources, discouraging even long-standing informants from speaking with the AP.[81] In July 2013, the Attorney General tightened the rules on getting reporters' data, but did not prohibit the practice entirely.[82]

The Communications Assistance for Law Enforcement Act (CALEA) requires telephone companies, broadband carriers, and interconnected Voice over Internet Protocol (VoIP) providers to design their systems so that communications can be easily intercepted when government agencies have the legal authority to do so.[83] The FBI suggested in late 2010 that the law should be expanded to impose design requirements on online communications tools such as Gmail, Skype, and Facebook,[84] and while the FBI continued to push the issue,[85] no legislation has yet been proposed in Congress.

In April 2013, the House of Representatives voted in favor of the Cyber Intelligence Sharing and Protection Act (CISPA), a proposed law that would allow ISPs and other corporations to share cyber threat information with one another and the government.[86] Civil liberties advocates warn that the bill, in its current form, would allow companies to share citizens' private information with the government, including internet records and e-mail content, without first taking reasonable steps to remove material not related to the threat.[87] The Senate has since shelved the bill and President Obama has pledged to veto the legislation if it reaches his desk as written, citing concerns about privacy and civil liberties of internet users.[88]

Law enforcement agencies have also begun to use open, public websites and social media to monitor different groups for suspected criminal activity. One notable example that stoked controversy in February 2012 was an initiative by the New York Police Department (NYPD) to monitor Muslim student groups at various universities in the northeastern United States. The Associated Press reported that, from 2006 onward, the NYPD Cyber Intelligence unit had monitored blogs, websites, and online forums of Muslim student groups and produced a series of secret "Muslim Student Association" reports describing group activities, religious instruction, and

[80] "Look Who's Talking: The Administration Seems to Have Trampled on Press Freedom,"The Economist, May 18, 2013, http://econ.st/YN4N8n.
[81] Lindy Royce-Bartlett, "Leak Probe Has Chilled Sources, AP Exec Says," The Associated Press, June 19, 2013, http://www.cnn.com/2013/06/19/politics/ap-leak-probe.
[82] Charlie Savage, "Holder Tightens Rules on Getting Reporters' Data." The New York Times, July 12, 2013, http://www.nytimes.com/2013/07/13/us/holder-to-tighten-rules-for-obtaining-reporters-data.html?pagewanted=all&_r=0.
[83] The FCC does not classify Skype as an "interconnected VoIP" service.
[84] Charlie Savage, "U.S. Tries to Make it Easier to Wiretap the Internet." The New York Times, September 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=all.
[85] Declan McCullagh, "FBI: We Need Wiretap-Ready Websites – Now," CNET, May 4, 2012, http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now.
[86] "Rogers-Ruppersberger Cyber Bill (CISPA) Passes House," U.S. House of Representatives Permanent Select Committee on Intelligence, Press Release, April 18, 2013, http://1.usa.gov/18Aoi6v.
[87] "House Passes CISPA," Center for Democracy and Technology PolicyBeta Blog, April 18. 2013, https://www.cdt.org/pr_statement/house-passes-cispa; Michelle Richardson "CISPA Explainer #1: What Information Can Be Shared?" ACLU Blog, April 2, 2013, http://www.aclu.org/blog/national-security-technology-and-liberty/cispa-explainer-1-what-information-can-be-shared.
[88] "Statement of Administration Policy: H.R. 624 – Cyber Intelligence Sharing and Protection Act," Executive Office of the President, Office of Management and Budget, April 16, 2013, http://1.usa.gov/110RWxH.

the frequency of prayer by the groups.[89] The New York City mayor defended the practice by stating that the NYPD did not break any laws by monitoring websites and online activity that was already publicly available, although others pointed to the religious-profiling nature of the activity. Muslim students from across the nation have expressed concern about this type of surveillance and in late 2012 told Freedom House that they often self-censor when conducting online activities.

Like most other countries, the United States faces the growing challenge of addressing cyberattacks conducted by both international and domestic actors. China is one focal point of the cybersecurity discussion, especially following a report by computer security firm Mandiant which stated that many attacks against U.S. organizations, companies, and government agencies appear to have originated in an office of the Chinese People's Liberation Army in Beijing.[90] The purpose of these attacks is presumably to gain information, but the United States faces other types of cybersecurity threats as well. For example, the Department of Homeland Security reported a wave of attacks in mid-2013 that sought to reveal vulnerabilities in infrastructure managed by private energy companies. The attacks seem to have originated in the Middle East, but the exact source is unknown.[91] In response to growing concern about cybersecurity threats, President Obama produced an executive order in February 2013 recognizing the need for improved cybersecurity measures and calling for a new "Cybersecurity Framework" to address security threats.[92] At the same time the U.S. military admitted that it is developing the ability to carry out offensive cyberattacks.[93] The documents leaked by Edward Snowden included a Presidential Policy Directive describing U.S. "Offensive Cyber Effects Operations (OCEO)."[94]

[89] Al Baker and Kate Taylor, "Bloomberg Defends Police's Monitoring of Muslim Student Web Sites," New York Times, February 22, 2012, http://www.nytimes.com/2012/02/22/nyregion/bloomberg-defends-polices-monitoring-of-muslim-student-web-sites.html.

[90] David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit is Seen as Tied to Hacking Against the U.S." The New York Times, February 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&gwh=24BE5E3C317441D6CAB213658308303F&_r=0.

[91] David E. Sanger and Nicole Perlroth, "Cyberattacks Against U.S. Corporations Are on the Rise," The New York Times, May 12, 2013, http://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html?pagewanted=all.

[92] "Executive Order – Improving Critical Infrastructure Cybersecurity," February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[93] Mark Mazzetti and David E. Sanger, "Security Leader Says U.S. Would Retaliate Against Cyberattacks," The New York Times, March 12, 2013, http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?pagewanted=all.

[94] Glenn Greenwald and Ewen MacAskill, "Obama Orders U.S. to Draw Up Overseas Target List for Cyberattacks," The Guardian, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

UZBEKISTAN

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	19	20
Limits on Content (0-35)	28	28
Violations of User Rights (0-40)	30	30
Total (0-100)	**77**	**78**

* 0=most free, 100=least free

POPULATION: 29.8 million
INTERNET PENETRATION 2012: 37 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The government established a new telecommunications regulator with consolidated powers to control the internet and other information and communications technologies (ICTs) (see **OBSTACLES TO ACCESS**).
- Judges declared the leading mobile phone operator, Uzdunrobita (partially owned by Russian telecoms company MTS), bankrupt, in a case involving potential bribes from the ruling family and confirming the hostility of the environment for foreign investment in the telecommunications sector (see **LIMITS ON CONTENT**).
- Criminal investigations using trumped-up charges were opened against a popular news site, Olam.uz, which had been reporting on the corruption allegations surrounding the Uzdunrobita case (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

In the period of May 2012 to April 2013, internet regulation in Uzbekistan did not improve and the country remains one of the most restrictive in Central Asia. The Uzbek government has adopted several programs aimed at stimulating the development of the telecommunications infrastructure and raising awareness about computer technologies, especially among rural populations. However, as reported by the International Telecommunications Union (ITU) in 2011, Uzbekistan is on the verge of being excluded from the global information society due to the still prohibitively high prices for broadband internet access.[1]

In the fall of 2012, the government consolidated regulatory authority over the ICT industry in Uzbekistan through the establishment of a new telecommunications regulator. The action was taken after the former telecom regulator, UzACI, was involved in the unlawful termination of the leading GSM operator, Uzdunrobita (MTS-Uzbekistan) beginning in July 2012. All media regulatory bodies were integrated into the structure of the new telecommunications regulator.

In 2012–2013, the state-owned telecommunications carrier Uztelecom retained centralized control over the country's connection to the international internet, facilitating nationwide censorship and surveillance. The Uzbek authorities block access to a wide range of international news websites, human rights groups, and exile publications, while at educational and cultural institutions, access is strictly limited to the national intranet system, or ZiyoNet. A popular online news site, Olam.uz, which reported extensively about the Uzdunrobita case, was shut down in January 2013 due to the politically motivated charges against its owner and editor-in-chief. Additionally, two journalists reporting for online media are serving long sentences on trumped-up charges.

OBSTACLES TO ACCESS

Direct access to the internet backbone via the Trans Asia Europe fiber-optic cable became operational in Uzbekistan in 1998.[2] Despite extensive state investments in telecommunications infrastructure and internet connectivity since 1999, internet penetration reached a mere 9 percent of the population by 2009.[3] In January 2013, according to the government, the number of internet users reached 9.8 million, comprising 33 percent of the population—a small increase from 31

[1] International Telecommunication Union (ITU), "Measuring the Information Society: 2012," accessed July 30, 2013, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf.
[2] Trans Asia Europe, "Historical reference 2005," accessed July 30, 2013, http://taeint.net/en/about/company_history/.
[3] United Nations Development Program (UNDP), "Review of Information and Communication Technologies Development in Uzbekistan: 2005," Tashkent 2006, http://www.undp.uz/en/publications/publication.php?id=19. Also see ITU, "Key 2000 – 2011 country data: Percentage of individuals using the Internet," http://www.itu.int/ITU-D/ict/statistics/.

percent in April 2012.[4] Estimates by the International Telecommunication Union calculated the internet penetration rate slightly higher at 37 percent for 2012.[5]

Digital divides are found across urban, rural, and remote areas of the country, where factors such as computer literacy and income affect the likelihood that individuals have access to the internet. Problems with the electrical grid limit the usefulness of the telecommunications infrastructure, especially in rural and remote areas.[6] A digital divide also exists between the capital, Tashkent, and the country's 12 regions (*viloyati*), with the lowest internet penetration rate registered in the semi-autonomous republic of Karakalpakstan—a home to the Karakalpak, Kazakh, and Uzbek ethnic groups.[7]

Only 8 percent of households were connected to the internet in Uzbekistan by the end of 2011, the second lowest estimate in the region of the Commonwealth of Independent States (CIS) after Turkmenistan.[8] Though work seems to be a primary place to access the internet, "collective" or public access points such as internet cafes remain popular as well. Since December 2010, minors are officially prohibited from visiting internet cafes without parents or adults between 10:00 p.m. and 6:00 a.m.[9] Reportedly, since 2011, students are also not allowed to visit internet cafes between 8:30 a.m. and 7:00 p.m.[10]

Public libraries, museums, nearly all of the country's educational, scientific and cultural institutions, and youth organizations connect to the internet exclusively via the "unified information network ZiyoNet," or intranet, initiated by the government in September 2005.[11] ZiyoNet requires user identification and employs software protecting against "aggressive internet content."[12] Given the role of those institutions in Uzbek society,[13] online resources on the intranet consist mainly of government sources of information, including state educational but also ideological materials.[14] As

[4] State Committee for Communications, Information and Telecommunications Technologies (SC for CITT), "Показатели развития отрасли: Актуальные статистические данные о состоянии внедрения и развития ИКТ в Республике Узбекистан,"accessed April 25, 2013, http://ccitt.uz/ru/indicators/.
[5] International Telecommunication Union (ITU), "Percentage of Individuals Using the Internet," 2012, accessed July 30, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[6] International Telecommunication Union, "Sustainable electricity supply of telecommunications objects in rural and remote areas," accessed September 21, 2012, http://www.itu.int/ITU-D/projects/display.asp?ProjectNo=2UZB11003.
[7] UzACI and UNDP Uzbekistan, "Анализ состояния и перспектив развития Интернет в Республике Узбекистан" [Analysis of the Internet Development and its Prospects in Uzbekistan], 2009, accessed July 30, 2013, http://infocom.uz/wp-content/files/otchet.pdf.
[8] ITU, "Measuring the Information Society: 2012," accessed July 30, 2013, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf.
[9] "O poriadke predostavlenia dostupa k seti Internet v obschestvennikh punktakh pol'zovania" [On Adoption of the Terms of Provision of Access to the Internet Network in Public Points of Use], promulgated by Order of the Communications and Information Agency of Uzbekistan No. 216, July 23, 2004, *SZ RU* (2004) No. 30, item 350, at Art. 17 (e).
[10] "Lyceum students banned from e-cafes," Uznews.net, May 31, 2012, http://www.uznews.net/news_single.php?lng=en&sub=top&cid=4&nid=19973.
[11] Resolution of the President RU "О создании общественной образовательной информационной сети Республики Узбекистан" [On the Establishment of the Public, Educational, and Information Network of the Republic of Uzbekistan], No. ПП-191, 28 September 2005, SZRU (No. 40), item. 305, at Art. 4.
[12] Ibid., at Art. 5.
[13] Resolution of the President RU "О государственной программе "Год гармонично развитого поколения"" [On the State Program "The Year of Harmoniously Developed Generation"], No. ПП-1271, January 27, 2010, SZRU (2010) No. 5, item 37.
[14] "Библиотека" [Library], ZiyoNet.uz, accessed July 30, 2013, http://www.ziyonet.uz/ru/library/.

of January 2013, there were 41,541 of these "approved" online information resources, some of which are knock-offs of popular social media platforms such as Utube.uz.

Internet connectivity is available via dial-up, ADSL broadband, and WiMax, but no longer via satellite. Dial-up connections are more common in rural areas than urban areas.[15] In 2011, the government made a commitment to expand the number of users with a dial-up connection from 3 million to 3.5 million.[16] By 2012, 147,760 users had a fixed-broadband subscription in the country,[17] which is significantly higher than the national target of 100,000 set by President Karimov to be achieved by the end of 2011.[18] Given this target, Uztelecom and the Chinese telecommunications equipment supplier ZTE launched the mass production of ADSL modems and DSLAM network devices in August 2011.[19] As of February 2013, Uztelecom offered FTTB broadband internet to 837 buildings in Tashkent. WiMAX broadband is available only in Tashkent and six regions since it was first introduced on the Uzbek market by a private operator in 2008.[20] As described below, the ban on private ISPs to access the internet via satellite has been in force since February 2011.

The state-owned JSC Uzbektelecom, established in 2000 and re-branded as "national operator Uztelecom" in 2011, operates Uzbekistan's telecommunications infrastructure under a state license renewable every 15 years. In August 2005, Uztelecom took over the internet connectivity functions from the state data transfer network company, "UzPAK," which later became its subsidiary.[21] The latter is claimed to have been only partially successful in maintaining a monopoly and centralized state control over international internet connectivity since its establishment in 1999.[22] By contrast, due to a favorable regulatory environment, Uztelecom has succeeded in becoming a pure monopoly over the country's connection to the internet and an upstream ISP, with private ISPs required to have their international internet traffic routed and transmitted through a single Uztelecom network gateway (the International Centre for Packet Switching, abbreviated as MZPK in Russian).

---

[15] Sarkor Telekom, Press Release, December 16, 2011, http://www.sarkor.com/ru/press/news/.

[16] Uztelecom, "Рассмотрены перспективы развития телекоммуникационных сетей" [The Prospective for the Development of Telecommunications Networks Has Been Analyzed], February 21, 2011, http://www.uztelecom.uz/ru/press/media/2011/141/.

[17] ITU, "Key 2000 – 2011 country data: Fixed (wired)-broadband subscriptions," http://www.itu.int/ITU-D/ict/statistics/.

[18] Report of the President RU to the Government, "Все наши устремления и программы – Во имя дальнейшего развития родины и повышения благосостояния народа" [All our aspirations and programs – in the name of the further development of the motherland and improvement of the welfare of the people], February 21, 2011, http://www.press-service.uz/ru/news/archive/dokladi/#ru/news/show/dokladi/vse_nashi_ustremleniya_i_programmyi__1/.

[19] Uztelecom, "Запущена в эксплуатацию технологическая линия по производству DSLAM оборудования и ADSL модемов" [A Technological Production of DSLAM Equipment and ADSL modems Has Been Launched], August 31, 2011, http://www.uztelecom.uz/ru/press/news/2011/187/.

[20] See UzACI and UNDP Uzbekistan, note 9 above.

[21] Decree of the President RU "On measures for development of data transfer services and preparation for privatization of JSC "Uzbektelecom", No. PP-149, August 8, 2005.

[22] Josh Machleder, "Struggle over Internet Access Developing in Uzbekistan," December 3, 2002, www.eurasianet.org/departments/rights/articles/eav031202.shtml.

In March 2011, the former telecommunications regulator, UzACI, amended its 2004 regulatory provisions in ways that further established Uztelecom's control over the traffic of other ISPs.[23] Firstly, the amendments specified that ISPs have "the right to access international telecommunications networks solely through technical means of JSC Uzbektelecom." Consequently, on December 30, 2011, the Uzbek parliament amended the 1999 Law on Communications to impose more general legal obligation upon ISPs to "provide interconnections of their networks according to technical specifications of the operator of the connecting telecommunications networks."[24] Secondly, UzACI revoked the norm guaranteeing the right of private ISPs to install and maintain their own satellite stations in order to enable internet connectivity.

As a government-sanctioned monopoly, Uztelecom sets the price for use of its internet gateway by downstream ISPs. In February 2013, this price reached approximately $384 per 1 Mbps per month for private ISPs—a reduction from $495 in February 2012.[25] There are no statistics demonstrating whether private ISPs systematically pass down Uztelecom's price reductions to their subscribers. In April 2013, private ISPs offered household internet access at a minimum download speed of 256 Kbps for a monthly subscription of $30 (with free traffic up to 2,000 Mb) and a maximum download speed of 2,048 Kbps for $44 per month (with free traffic up to 12,000 Mb).[26] Similar prices were reported for ADSL broadband packages offered by Uztelecom in January 2012. As reported by the ITU, such prices are prohibitively high and exceed the monthly GNI per capita level at the rate of approximately 188 percent.[27] As of May 2012, neither Uztelecom nor other ISPs offer a monthly internet access package with unlimited usage.

While prices for international internet access remain prohibitively high for most citizens in Uzbekistan, by contrast, Uzbek ISPs offer low cost access without traffic limitations to websites domestically hosted in Uzbekistan within the TAS-IX network. Registered in February 2004 by the five largest domestic ISPs at the time, TAS-IX is a nongovernmental organization with ISPs regulating their relationship by an agreement and annually selecting a network administrator among its members.[28] By March 2013, the TAS-IX peering center had a membership of 37 ISPs interconnecting their networks in order to enable traffic conveyance and exchange at no mutual charge and without the need to establish international internet connections via Uztelecom.[29] Membership of Uztelecom may, however, complicate the presumably self-regulating structure of

[23] Приказ генерального директора Узбекского агенства связи и информатизации "О внесении изменений в Положение о порядке регулирования межсетевого взаимодействия Интернет-провайдеров на сетях передачи данных" [Order of the General Director of UzACI 'On Amendements to the Rules on the Procedure Regulating Network Interconnection Among Internet Providers on Data Networks'], No. 4-Yu, March 15, 2011, *SZRU* (2011) No. 10-11 (458-459), item 108, at Annex.
[24] Law RU, "O telekommunikatsiiakh" [On Telecommunications], No. 822-I, 20 August 1999, *VOM RU* (1999) No. 9, 219, as amended by Law No. 3РУ-314 on December 30, 2011, at Art. 17, para. 3.
[25] Uztelecom, "О снижении тарифов на интернет-услуги для провайдеров" [Tariff Reduction for Internet Service Providers], March 6, 2012, http://www.uztelecom.uz/ru/press/news/2013/962/.
[26] See, e.g., a tariff list from the leading ISP provider TPS, at http://www.tps.uz/tariffs/section/jet (last accessed on April 26, 2013).
[27] ITU, "Measuring the Information Society: 2012."
[28] InfoCom.uz, "Самое нужное ННО для Узнета – Соглашение TAS-IX," February 18, 2004, http://infocom.uz/2004/02/18/samoe-nuzhnoe-nno-dlya-uznetasoglashenie-tas-ix/.
[29] TAS-IX, List of Members, http://tas-ix.uz/index.php?option=com_content&view=article&id=63:listofmembers.

TAS-IX. Presently, the relationship between Uztelecom and all other TAS-IX participating ISPs is not clear and is at the stage of negotiations.[30] TAS-IX has evolved to become a conduit for domestically hosted content. TAS-IX also filters and blocks content or applications to the same extent as Uztelecom.[31] At the same time, as some have pointed out, TAS-IX ISPs are challenged to find the income streams for the investments needed to meet the capacity requirements of their customers.[32]

According to the latest ITU data, over 20 million Uzbeks had a mobile phone subscription by the end of 2012, with a mobile phone penetration rate of approximately 72 percent.[33] Mobile phone connectivity via 3G technology is widely available, though as of October 2011, only 23 percent of mobile phone subscribers were using mobile broadband services.[34] As of December 2011, mobile broadband based on 4G/LTE technology was limited only to some parts of the capital Tashkent.[35] WiMax mobile broadband is said to be available only in Tashkent and the other five major cities of the country.[36] Still, there are general complaints about the poor quality of mobile phone connections and broadband internet access, which are related, among other things, to such regulatory obstacles as intricate customs procedures for the import of ICT equipment, unduly complicated tender conditions, and various bureaucratic obstacles at the local level.[37]

As of May 2013, four out of five operators were left to share the Uzbek market for mobile phone services. The smallest numbers of subscribers reportedly belonged to two CDMA operators—Uzmobile (a brand of the state-owned Uztelecom) and Perfectum Mobile (owned by the Uzbek company Rubicon Wireless Communication).[38] Two GSM operators—Beeline (owned by the Russian VimpelCom Ltd) and Ucell (owned by the Swedish-Finnish company TeliaSonera)—shared the largest portions of the market.[39] Recently, the Uzbek antitrust authorities accused and fined the

[30] InfoCom.uz, "Итоги работз в 2010 году" (Information on a meeting between TAX-IS and Uztelecom in January 2013 on the matter of network interconnectivity), March 4, 2013, http://tas-ix.uz/index.php?option=com_content&view=article&id=62:-2012-.

[31] TAX-IS participating ISP maintain a service to find out whether a website is in the TAS-IX network. See, e.g., ISP TPS, http://www.tps.uz/tasix/.

[32] Eugeniy Sklyarevskiy, 'Узбекистан: Кто платит за бесплатный TAS-IX?', October 24, 2012, http://www.12news.uz/news/2012/10/24/узбекистан-кто-платит-за-бесплатный-tas-ix/.

[33] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2012, accessed July 13, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[34] However, it is not clear whether this official data also includes statistics of internet access provided by private mobile phone companies. See, UzACI, "Коллегия УзАСИ подвела итоги деятельности 9 месяцев" [The UzACI Board Summed up 9 Months of its Activity], October 25, 2011, http://www.aci.uz/ru/news/uzaci/article/1407.

[35] UzDaily, "МТС-Узбекистан начал продавать 4G модемы" [MTS-Uzbekistan Started to Sell 4G Modems], December 22, 2011, http://www.uzdaily.uz/articles-id-9334.htm.

[36] EVO Premium Operator, "About us", http://evo.uz/ru/company/about.

[37] "Узбекистан: Beeline и Ucell плохо справляются с обслуживанием абонентов в отсутствии Uzdunrobita," Fergananews.com, May 6, 2013, http://www.fergananews.com/articles/7714.

[38] "UZMOBILE subscribers' number exceeds 200,000 users," UzDaily, January 31, 2013, http://www.uzdaily.com/articles-id-21856.htm#sthash.eB7gIe9p.dpbs. Perfectum Mobile does not make public its customer base. Reportedly, the numbers reached an average of 500,000 subscribers in 2012. See Mobinfo.Uz, "Сколько же абонентов было у МТС- Узбекистан на самом деле?" November 10, 2012, http://mobinfo.uz/print:page,1,10830-skolko-zhe-abonentov-bylo-u-mts-uzbekistan-na.html.

[39] By the end of December 2012, Beeline reported having 9.2 million subscribers. See Beeline, "Билайн в Узбекистане," http://about.beeline.uz/ru/about/index.wbp (last accessed on April 20, 2013). By the end of September 2012, Ucell had 9.5 million subscribers. See http://mobinfo.uz/print:page,1,10830-skolko-zhe-abonentov-bylo-u-mts-uzbekistan-na.html.

latter two companies for price fixing that allegedly took place in 2012 and 2013. Still, Beeline and Ucell have been able to increase their customer base after the Uzbek government terminated the operations of a leading competitor and GSM operator, Uzdunrobita (a wholly owned subsidiary of the Russian company MTS).

On July 17, 2012, Uzdunrobita's mobile phone services and internet broadband access became permanently inaccessible to more than 9.5 million subscribers.[40] From August 2012 to April 2013, the company struggled to challenge official charges of violations of tax, antimonopoly, and consumer protection laws, including the award of $587 million worth of compensatory damages for the state by domestic courts.[41] After Uzdunrobita's petition for voluntary bankruptcy, the company was declared bankrupt by order of the Tashkent Commercial Court on April 22, 2013. The Uzdunrobita case is the first case of unlawful expropriation of foreign businesses providing access to digital technologies in Uzbekistan.

The reported period was characterized by disclosures of vast bribery in the domestic telecommunications business from as far back as 2007. According to allegations, the president's daughter, Gulnara Karimova, had systematically solicited bribes from MTS (Uzdunrobita) and TeliaSonera (Ucell). Karimova is believed to have sold outstanding shares of Uzdunrobita to MTS for $250 million in cash in June 2007.[42] Her middleman, Uzdunrobita's general director, fled the country in June 2012 and, as of May 2013, remains one of the suspects in pending investigations into money-laundering and aggravated bribery in Switzerland and Sweden. Reportedly, the Sweden-based TeliaSonera allegedly paid bribes worth millions of dollars to Karimova over a five-year span between 2007 and 2012, starting with the acquisition of a 3G telecom license for $314.6 million.[43] As of May 2013, Gulnara Karimova held the post of Ambassador, Permanent Representative of the Republic of Uzbekistan to the United Nations and other international organizations in Geneva; however, Karimova lost her post in July 2013.[44]

The government's control over the internet infrastructure and its influence on mobile phone operators enables it to limit or block connectivity to Web 2.0 applications at will, which it appears to have done on several occasions in recent years. In August 2011, individual users and independent news websites reported that the Google search engine and its Russian equivalent, Rambler, were blocked for several days amidst a broader increase in blocked websites.[45] Government officials and service providers denied that the disruptions were intentional, but observers suspected that the restrictions were related to the upcoming 20th anniversary of the end of the Soviet era in September

[40] RFE/ RL, "Millions of Uzbek Customers Left Without Mobile-Phone Service," July 18, 2012, http://www.rferl.org/content/uzbekistan-mobile-phone-provider-suspended-uzdunrobita/24649344.html.
[41] MTS, "Annual Report: 2012," http://www.mtsgsm.com/upload/contents/294/MTS_Clean.pdf.
[42] Saveliy Vezhin, "Узбекское молчание МТС. Инвестиции мобильного оператора "Уздунробита" в развитие сотовой связи республики – под угрозой" [Uzbek Silence of MTS: The Investments of the Mobile Operator Uzdunrobita in the Development of Mobile Services in the Republic are Under Threat], June 24, 2012, http://www.ng.ru/ideas/2012-07-24/5_mts.html.
[43] RFE/RL, "New Documents Suggest Fresh Evidence of TeliaSonera Ties to Karimova," May 22, 2013, http://www.rferl.org/content/sweden-teliasonera-uzbekistan-karimova/24993135.html.
[44] Murat Sadykov, "Uzbekistan: Gulnara's Future Uncertain After Exiting UN Post," Eurasianet.org, July 14, 2013, http://www.eurasianet.org/node/67246.
[45] Reporters Without Borders, "Uzbekistan," *Enemies of the Internet 2012*, March 12, 2012, http://en.rsf.org/uzbekistan-uzbekistan-12-03-2012,42079.html.

2011 and the government's fear that it might trigger social media-inspired protests in Uzbekistan.[46]

On May 21, 2012, the government adopted a resolution establishing unified rules for the use of mobile phones in all educational institutions of the country.[47] The resolution completely bans the use of mobile phones in the buildings of educational institutions, not only for students but also for teachers and other personnel. According to the resolution, the aim of such measures is to prevent "negative aspects" of the use of mobile phones in educational settings, such as cheating; digital gaming; and the dissemination of materials undermining morals and ethics, promoting a culture of violence, cruelty and pornography, or promoting "reactionary sectarian, pseudo-religious ideology." Another stated aim, however, is to enable the "education of the youth in the spirit of love to its motherland, respect for national values and those of the humanity, [and] ideas of national independence." In the past, the government has sporadically ordered the shutdown of text messaging and internet services by mobile operators, particularly during examinations.[48]

Apart from these sporadic restrictions, YouTube, Facebook, Twitter, and LiveJournal remained generally available in 2012–2013, though some individual pages were blocked. In March 2012, however, reports emerged that the Uzbek authorities had blocked LiveJournal out of concern that potential protests could erupt over the results of the Russian presidential elections.[49] The blog-hosting platform Wordpress remained blocked in its entirety during the reported period.[50]

Service providers are required to have a license to operate, and in 2005, the Cabinet of Ministers adopted Resolution No. 155, which stipulates that telecommunications providers must first register as a legal entity before being issued a license. Thereafter, the licensing procedure is fairly straightforward but in practice is often encumbered by political interests, with applicants from outside the government's inner circle regularly denied licenses for unjustifiable reasons.[51]

The Uzbek Agency for Communications and Information (UzACI) ceased to exist in October 2012, when President Karimov issued a decree[52] establishing a new telecommunications regulator, the State Committee for Communications, Information and Telecommunications Technologies (State

[46] Institute for War & Peace Reporting, "Tashkent Spooked by Web Interest in Arab Protests," February 24, 2011, http://iwpr.net/report-news/tashkent-spooked-web-interest-arab-protests; "В Узбекистане блокируют Живой Журнал и поисковые системы" [LiveJournal and Search Engines are Blocked in Uzbekistan], Ferghana News, August 10, 2011, http://www.fergananews.com/news.php?id=17125; Catherine A. Fitzpatrick, "Uzbekistan: Internet Sites Blocked," Eurasianet.org, August 10, 2011, http://www.eurasianet.org/node/64026.

[47] Resolution of the Cabinet of Ministers RU, "О мерах по упорядочению пользования мобильными телефонами в образовательных учреждениях Республики Узбекистан," No. 139, May 21, 2012, *SZ RU* (2013 No. 21 (521), item. 229.

[48] "Uzbekistan 'halts mobile Internet, SMS' for exam day," AFP, August 2, 2011, http://www.google.com/hostednews/afp/article/ALeqM5iAt_J3V1eR_Homvu0Osp2K3mqMdQ.

[49] "LiveJournal website blocked in Uzbekistan," Uznews.net, March 20, 2012, http://www.uznews.net/news_single.php?nid=19380.

[50] IREX, "Europe & Eurasia Media Sustainability Index 2013," http://www.irex.org/sites/default/files/u105/EE_MSI_2013_Uzbekistan.pdf

[51] IREX, "Uzbekistan."

[52] Decree of the President RU "О создании Государственного комитета связи, информатизации и телекоммуникационных технологий Республики Узбекистан" [On the Establishment of the State Committee for Communications, Information and Telecommunications Technologies], УП-4475.

Committee for CITT).[53] Similarly to its predecessor, the new governmental body lacks independence and is accountable to the Cabinet of Ministers in the executive branch.[54] The president appoints and dismisses the committee chairman and first deputy, who are also members of the Executive Board of the national operator Uztelecom, where the committee has the right to manage 51 percent of state shareholdings.[55] Moreover, the Cabinet of Ministers approves members of a committee's collegium selected from the committee's top bureaucrats. The collegium coordinates the planning and implementation of the committee's main activities and appoints the committee's *nomenklatura*.[56] These appointment processes lack transparency. In addition, the composition of the committee is not representative of different stakeholders' interests. With the establishment of the State Committee for CITT, the government has consolidated its regulatory authority over the ICT industry.

The government maintains direct control over the administration, registration, and use of domain names with the ".uz" top-level domain, which was established in April 1995 and re-delegated to the government in April 2003.[57] Current rules for the assignment, registration, and use of the country's top-level domain create an obstacle to internet access.[58] The Computerization and Information Technologies Developing Center (Uzinfocom) manages the ".uz" top-level domain. There are seven private ISPs officially authorized to provide registry services in the ".uz" domain zone.[59] Uzinfocom is also the largest provider of web hosting services, including for the e-government project, government-backed intranet, national search engine, and social-networking sites.[60]

LIMITS ON CONTENT

The Uzbek government engages in pervasive and systematic blocking of independent news and any content expressing critical opinions and views about Uzbekistan's government, the country's foreign and domestic affairs—including the human rights situation—and other issues of general public interest in Uzbekistan.[61] Access to online information was relatively open until 2001 when the authorities began filtering politically sensitive websites and reportedly intercepting e-mail

[53] State Committee for Communications, Information and Telecommunications Technologies official website, http://www.ccitt.uz/ru/.
[54] Resolution of the Cabinet of Ministers RU "Об утверждении положений о Государственном комитете связи, информатизации и телекоммуникационных технологий Республики Узбекистан и о Государственной инспекции по надзору в сфере связи, информатизации и телекоммуникационных технологий" [On the Adoption of Rules on the State Committee for Communications, Information and Telecommunications Technologies of the Republic of Uzbekistan and on the State Inspection in the Fields of Communications, Information and Telecommunications Technologies], No. 355, 19 December 2012, *SZRU* (2012) No. 52 (552), item 589, at Art. 2.
[55] Postanovlenie at Art. 13.
[56] Ibid., at Art. 16.
[57] IANA, "Report on Redelegation of the uz Top-Level Domain," April 10, 2003, http://www.iana.org/reports/2003/uz-report-10apr03.html.
[58] Law RU "On Telecommunications," at Arts. 8, 11.
[59] ccTLD.uz, "Администраторы" [Administrators], http://cctld.uz/reg/.
[60] Uzinfocom Data Centre, "Услуги веб-хостинга" [Web Hostimg Services], http://dc.uz/rus/hosting/.
[61] Reporters Without Borders, "Internet Enemies: Uzbekistan," http://en.rsf.org/internet-enemie-uzbekistan,39765.html; Alexei Volosevich, "Journalism in Uzbekistan is not history. It has but moved to the Net," February 26, 2007, http://enews.fergananews.com/article.php?id=1855.

communication.[62] However, state internet censorship and surveillance have significantly intensified since May 2005, following the government's violent crackdown on peaceful antigovernment protests in Andijan and the subsequent news blackout on this event in the traditional media.[63] In 2012–2013, the Uzbek government continued to apply pressure on online content providers in order to force the removal of political content from certain sites.

Since the government officially banned the operation of such international broadcasters as the BBC and the U.S. government-funded Radio Free Europe/Radio Liberty (RFE/FL) in Uzbekistan in 2005, their websites (Bbc.co.uk/uzbek, Ozodlik.org) have remained permanently inaccessible.[64] The websites of two international broadcasters, Deutsche Welle (Dw.de) and Voice of America (Voanews.com/uzbek), are also blocked. Permanent blocking also applies to independent online news media, such as Uznews.net, Ferghananews.com, Harakat.net, Mediauz.ucoz.ru, and Uzmetronom.com, as well as the websites of Uzbek opposition groups in exile.[65] In addition to being blocked, none of these websites appear in the results of the national search engine www.uz, which is regulated by the government and primarily catalogues sites with ".uz" domain names.[66]

In February 2013, assumedly under pressure of the Uzbek government, administrators of the Russian social-networking site Odnoklassniki.ru removed a web page of the National Movement of Uzbekistan "without the possibility of being restored."[67] At the time of removal, the Uzbek dissident group that had been established in 2011 had 26,000 "friends" on Odnoklassniki. In January 2013, the official website of the movement, Uzxalqharakati.com, had already come under a distributed denial-of-service (DDoS) attack, the third since its registration in May 2011.[68] The attack paralyzed the website for several days.

The Uzbek authorities appear to have fairly sophisticated censorship technology at their disposal that enables them to not only block entire domains, but also restrict access to individual pages that contain politically sensitive content while retaining access to other parts of a particular site. For example, in February 2011, after people started discussing the protests that were erupting in the Middle East, including expressing solidarity with demonstrators and sharing news links about what was happening, users began reporting that certain pages and discussions on Facebook, LiveJournal,

[62] "Country Profile: Uzbekistan," OpenNet Initiative, December 21, 2010, http://opennet.net/research/profiles/uzbekistan.
[63] OSCE, "Coverage of the Events and Governmental Handling of the Press During the Andijan Crisis in Uzbekistan: Observations and recommendations," June 15, 2005, http://www.osce.org/fom/15617; Alo Khodjayev, "The Internet Media in Uzbekistan", in OSCE Representative on Freedom of the Media (ed.), Pluralism in the Media and the Internet (OSCE Representative on Freedom of the Media, Vienna, 2006), 143-148, at 144.
[64] Committee to Protect Journalists, "Attacks on the Press 2010: Uzbekistan," February 15, 2011, http://www.cpj.org/2011/02/attacks-on-the-press-2010-uzbekistan.php.
[65] See, e.g., website of the Uzbekistan "Erk" Democratic Party, http://uzbekistanerk.com/.
[66] Resolution of the President RU "О дополнительных мерах по дальнейшему развитию информационных технологий" [Program on the Establishment and Development of a National Information Search System], No.ПП-117, signed July 8, 2005, Annex 3, *SZRU* (2005) No.27, 189.
[67] Uznews.net, "НДУ изгнали из одноклассников," February 18, 2013, http://www.uznews.net/news_single.php?lng=ru&cid=30&nid=22104.
[68] Ozodlik.org, "Атака на сайт Народного Движения Узбекистана," January 27, 2013, http://www.ozodlik.org/content/article/24884770.html.

and Twitter were being blocked, though the social media tools as a whole remained available.[69] Similarly, in February 2012, the media reported that the Uzbek-language pages of Wikipedia were blocked, while their Russian counterparts remained available, although the latter typically contain more information on often-censored topics like human rights abuses. Analysts speculated that the block was more related to the government's nationalistic wish to monopolize Uzbek-language content than because of concerns that users would access politically sensitive information.[70]

Most censorship takes place at the country's international internet connection, operated by Uztelecom, which aggregates the private ISPs' traffic at a single node within its infrastructure. There is a widespread suspicion of involvement of foreign firms providing networking equipment to Uztelecom for the purpose of state censorship over the internet. The architecture of Uztelecom's network UzNet, which provides internet transit for private ISPs and internet access in governmental institutions, is based on network routers and switches produced by Cisco Systems, Inc.[71] Moreover, in its daily operations, Uztelecom widely employs the equipment of the Chinese company ZTE. ZTE opened its Uzbek office in 2003 and became a leading supplier of USB modems, mobile phones, and routers to all mobile phone operators and Uztelecom.[72] Furthermore, the government grants ISPs and mobile phone operators import duty and sales tax exemptions on surveillance equipment, which they are then required to install on their networks at their own expense.[73] Reportedly, the government has abolished some of its import tax exemptions on telecommunications equipment in 2013.

Under the 1999 Law on Telecommunications and several other government resolutions, the license of lower tier ISPs may be withheld or denied if the company fails to take measures to prevent their computer networks from being used for exchanging information deemed to violate national laws, including ones that restrict political speech. Under Order No. 216 passed in 2004, ISPs and operators "cannot disseminate information that, inter alia, calls for the violent overthrow of the constitutional order of Uzbekistan, instigates war and violence, contains pornography, or degrades and defames human dignity."[74] Given these broad restrictions, many individuals and organizations prefer to host their websites outside the country.[75]

---

[69] Institute for War & Peace Reporting, "Tashkent Spooked by Web Interest in Arab Protests," News briefing, February 24, 2011, http://iwpr.net/report-news/tashkent-spooked-web-interest-arab-protests.

[70] Jillian C. York, "This Week in Censorship: Syrian, Moroccan Bloggers Under Fire; New Censorship in Uzbekistan," Electronic Frontier Foundation, March 1, 2012, https://www.eff.org/deeplinks/2012/02/week-censorship-blogger-threats-syria-morocco-uzbek-censorship; Sarah Kendzior, "Censorship as Performance Art: Uzbekistan's Bizarre Wikipedia Ban," The Atlantic, February 23, 2012, http://bit.ly/zpyytP.

[71] Uztelecom, "Бизнесни ривожлантириш Маркази," accessed July 30, 2013, http://bit.ly/15CvbSH.

[72] UzDaily, "ZTE Corporation Expands Cooperation with Uzbekistan," November 1, 2011, http://www.uzdaily.com/articles-id-16308.htm. But ZTE is often accused of facilitating internet censorship and surveillance worldwide. See Madeline Earp, "China not most censored, but may be most ambitious," May 2, 2012, http://bit.ly/IUL7Yj.

[73] See the "Violations of Users Rights" below. See Tax Code of RU, SZRU (2007) No. 52(II), at Arts. 208 (§33), 211 (§7), 211 (§9), 230 (part 2, §5), 269 (§§15-16), and 355 (§ 13).

[74] Regulation "О порядке предоставления доступа к сети Интернет в общественных пунктах пользования" [On Adoption of the Terms of Provision of Access to the Internet Network in Public Points of Use], promulgated by Order of the Communications and Information Agency of Uzbekistan No. 216, July 23, 2004, *SZRU* (2004) No. 30, item 350.

[75] According to government figures, only about 30 percent of websites with ".uz" domain names were hosted on servers based in Uzbekistan as of December 2011. See Uzinfocom, "Только цифры" [Only Numbers], January 5, 2012, http://bit.ly/1hbO2sN.

The government has also placed political pressure on mobile phone operators. In March 2011, amid growing unrest in the Middle East, regulators demanded that operators notify the government of any attempts to circulate mass text messages with "suspicious content" and reportedly warned that the providers would be required to shut down internet connections provided to mobile users at the authorities' request.[76]

Several government-linked entities monitor and control online communications, though the opaque system offers few details on how decisions are made or what websites are blocked at any given time. The Center for the Monitoring of the Mass Communications Sphere, which is integrated into the structure of the State Committee on CITT, takes various measures to maintain compliance with national legislation that restricts free expression.[77] Its key objectives are "to analyze the content of information disseminated online and ensure its consistency with existing laws and regulations."[78] Based on its systematic monitoring of online content, the center has contributed to the takedown of independent websites.[79]

In August 2011, the government created a new secretive body—the Expert Commission on Information and Mass Communications—to oversee online controls, including the work of the Monitoring Center.[80] The commission is not independent and must submit quarterly reports to the Cabinet of Ministers.[81] Furthermore, its membership is not made public,[82] although the body is reportedly comprised exclusively of government employees.[83] The new commission is mandated to evaluate online publications and determine if they (1) have a "destructive and negative informational-psychological influence on the public consciousness of citizens;" (2) fail to "maintain and ensure continuity of national and cultural traditions and heritage;" or (3) aim to "destabilize the public and political situation," or commit other potential content violations.[84]

The commission also assesses publications referred to it by the Monitoring Center or other state bodies, including the courts and law enforcement, drawing on a designated pool of government-

[76] Murat Sadykov, "Uzbekistan Tightens Control over Mobile Internet," Eurasianet.org, March 15, 2011, http://www.eurasianet.org/node/63076.
[77] Zhanna Hördegen, "The Future of Internet Media in Uzbekistan: Transformation from State Censorship to Monitoring of Information Space since Independence," in Eric Freedman and Richard Schafer (eds.), *After the Czars and Commissars: Journalism in Authoritarian Post-Soviet Central Asia* (The Eurasian Political Economy and Public Policy Studies Series, Michigan State University Press, April 2011), 99-121.
[78] Paragraph 1, Regulation No. 555, On the Measures of Improving the Organizational Structures in the Sphere of Mass Telecommunications, adopted by the Cabinet of Ministers of Uzbekistan on November 24, 2004, via OpenNet Intiative, "Uzbekistan," December 2010, http://opennet.net/research/profiles/uzbekistan#footnote37_1d627h4.
[79] A news website Informator.uz was shut down in 2007. See, "Pochemu zakrito nezavisimoe SMI Uzbekistana—Informator.Uz?" [Why the independent mass media of Uzbekistan, Informator.Uz, is closed?], September 20, 2007, www.uforum.uz/showthread.php?t=2565. See also Freedom on the Net 2013: Uzbekistan, regarding the case of www.eDoctor.uz.
[80] Resolution of the Cabinet of Ministers RU, "О дополнительных мерах по совершенствованию системы мониторинга в сфере массовых коммуникаций" [On Supplementary Measures for the Improvement of the Monitoring System for the Sphere of Mass Communications], No. 228, 5 August 2011, *SZ RU* (2011) No. 32-33, item 336.
[81] Ibid., at Annex II, Art. 31.
[82] Ibid., Annex I, containing a list of the Commission's members, is not made public.
[83] Reporters Without Borders, "Uzbekistan," *Enemies of the Internet 2012*.
[84] Resolution of the Cabinet of Ministers RU, No. 228, at Art. 1 and Annex II, Art. 5. See note 50 above.

approved experts.[85] The experts submit reports to the commission, whose members then vote on whether or not a violation has been committed. If a violation is found, the decision becomes the basis for action to be taken by state bodies, including courts, and by "other organizations," presumably private ISPs.[86] There are no procedures in place that require notification of those whose content is affected by the decision or that grant them an opportunity to defend the speech in question, nor is there a clear avenue to appeal the decision after it is made. As of April 2013, the Commission appeared to be functioning but little information on its activities is available. The broadly defined violations and wide discretion granted to the commission raised concerns of how it could be used to suppress or punish free speech—including ordering ISPs to delete content or encouraging the arbitrary imprisonment of bloggers—particularly given the Uzbek government's track record of politically motivated censorship.[87]

Self-censorship is pervasive, given the government's tight controls over the media and harsh punishment of those who report on topics deemed "taboo," including criticism of the president, revelations about corruption, or health education.[88] Given the government's history of harassing traditional journalists, as well as their families, many online writers are cautious about what they post.

The editorial direction of the online versions of state-run news outlets is often determined by unofficial guidelines from the government. In an apparent effort to develop the country's media and information society, President Karimov signed a decree in December 2011 that extends tax preferences to media outlets. Taking effect on January 1, 2012, the decree exempts media services from the value added tax (VAT) and decreases the single tax payment required of media organizations from six to five percent, among other changes.[89] While the decree purportedly aims to strengthen "public control over the activities of state power and control,"[90] observers have noted that without an overall change in the regime's attitude to independent media, the new benefits will unlikely have a meaningful effect on freedom of speech in the country.[91]

According to the website rating firm Alexa, international social media websites like Facebook, YouTube, and Twitter, as well their Russian equivalents, are among the most visited websites in Uzbekistan. The most popular social-networking site in Uzbekistan is the Russian Odnoklassniki.ru, which became available in the Uzbek language in December 2012.[92] Facebook is

[85] Ibid., at Art. 1 and Annex II, Art. 14.
[86] Ibid., at Annex II, Arts. 26 and 29.
[87] For the detailed discussion of the governmental regulation of speech on ideological grounds, see: Zhanna Kozhamberdiyeva, "Freedom of Expression on the Internet: A Case Study of Uzbekistan," *Review of Central and East European Law* Vol. 33 (1) 2008, 95-134.
[88] Uznews.net, "В Узбекистане закрывается лучший медицинский сайт" [The Best Medical Website is Going to be Shut Down in Uzbekistan], March 25, 2010, http://www.uznews.net/news_single.php?lng=ru&cid=30&sub=&nid=13072; Catherine A. Fitzpatrick, "Uzbekistan: AIDS Activist Released, But Other Human Rights Defenders Harassed," September 6, 2011, http://www.eurasianet.org/node/64131.
[89] Alastair Carthew and Simon Winkelmann, "Uzbekistan – Overview," Konrad-Adenauer-Stiftung - Media Programme Asia, last updated May 24, 2012, http://www.kas.de/medien-asien/en/pages/10117/.
[90] "President of Uzbekistan Provides Tax Preferences to Media," The Journal of Turkish Weekly, December 31, 2011, http://www.turkishweekly.net/news/129114/president-of-uzbekistan-provides-tax-preferences-to-media.html.
[91] IREX, "Uzbekistan."
[92] "Top Sites in Uzbekistan," Alexa.com, accessed May 1, 2012, http://www.alexa.com/topsites/countries/UZ.

ranked second with over 120,000 members from Uzbekistan by April 2012, a notable increase from the year before.[93]

As social-networking sites and blogging platforms have grown in popularity, the government has adopted a new approach to influence the information circulated on them by creating and promoting Uzbek alternatives to popular global or regional brands. In 2010, the state-run Uzinfocom Center began creating a "social media zone" specifically geared toward users of the ZiyoNet intranet in Uzbekistan. The zone includes a range of Web 2.0 applications, including Id.uz (a social-networking site), Fikr.uz (a blog-hosting platform), Utube.uz (a video-sharing platform), Smsg.uz (an instant messenger service), and Desk.uz (a site for personal widgets). Access to these applications requires users to register either as an anonymous user or with their passport details. Although for the moment the zone's applications remain less popular than international brands, as of April 2013, 35,792 people had registered at Id.uz.[94] Uzinfocom Center's close relationship to the government has also raised concerns over the pressure the applications may receive from the authorities to censor and monitor users.

Besides the social media zone aimed at ZiyoNet users, two other social-networking websites were created in recent years with government support.[95] The more popular of the two, Muloqot.uz (meaning "dialogue"), was launched in September 2011 in an apparent effort to offset the growing influence of Facebook.[96] It is open only to Uzbek citizens residing in Uzbekistan, and at least one incident of censorship has been reported.[97] On the first day the social network was launched, staff of the Uzbek service of RFE/RL reportedly registered accounts and posted RFE/RL content, which is usually blocked, to a general "wall." According to their reports, within 15 minutes, their profiles were deleted.[98]

The blogosphere in Uzbekistan is weak, largely of entertainment character, and, due to the repressive environment, unable to significantly facilitate public discourse on political and social issues.[99] A handful of blogs critical of the regime are run by Uzbek dissidents (for example: Jahonnoma.com, Turonzamin.org, Fromuz.com) or are affiliated with independent online news sites like Uznews.net or Fergananews.com. Since its establishment in January 2012, a forum at Choyxona.com has become somewhat popular, with around 1,400 threads, 55,000 posts, and 620 members as of May 2013. It is run by the former editors of Arbuz.com, a forum site that was suspended in 2011 after Uzbek authorities arrested several of its users.

---

[93] "Uzbekistan Facebook Statistics," SocialBakers, accessed May 1, 2012, http://www.socialbakers.com.
[94] Uzinfocom, "Только цифры" [Only Numbers], April 2013, http://www.uzinfocom.uz/ru/news/406.
[95] UzACI, "Развиваются национальные информационные ресурсы. - УзА" [National information Resources are Developing - UzA], which reports on the creation of http://my.olam.uz/ with support of Uztelecom, http://www.aci.uz/ru/news/about_ict/article/1079/.
[96] "Manifest of the Community Muloqot.Uz," Muloqot, accessed May 1, 2012, http://muloqot.uz/help/about.
[97] Freedom House, "Uzbekistan Launches Government-Run Social Networking Site on Anniversary of Independence," Freedom Alert, August 31, 2011, http://bit.ly/KgeA1F.
[98] Luke Allnutt, "Uzbekistan Launches Its Own Facebook, Except It's Not For Everyone."
[99] Sarah Kendzior, "Digital Freedom of Expression in Uzbekistan: An Example of Social Control and Censorship in the 21st Century," New America Foundation, July 18, 2012, http://newamerica.net/publications/policy/digital_freedom_of_expression_in_uzbekistan.

Although there were no significant cases of political mobilization via social media, these tools have been important for exposing and disseminating information related to human rights abuses. In May 2005, for example, videos documenting Uzbek security forces opening fire on unarmed protesters in Andijan were uploaded to YouTube and regular updates were posted on Arbuz.com, contributing to international condemnation of the incident.

VIOLATIONS OF USER RIGHTS

The environment for internet users' rights in Uzbekistan is already one of the most restrictive in the region, with the government employing extensive surveillance measures to monitor online activity, as well as frequently using trumped-up charges to target individuals who publish material online that is deemed counter to the government's interests. In September 2012, Uztelecom began systematically blocking access to proxy servers. In January 2013, the editors of Olam.uz, a popular news website, chose to take the site offline after Uzbek authorizes charged them with various crimes, reflecting the degree to which the government continues to exert control over outlets that report on sensitive topics.

The constitution of Uzbekistan guarantees the right to freedom of expression (Article 29) and freedom of the mass media (Article 62). It also prohibits censorship (Article 62). In practice, however, these constitutional rights are not fulfilled and severely restricted by laws and governmental regulations. Judges lack the independence and impartiality needed to ensure the constitutional protection of speech.[100]

The 1997 law "On Mass Media" was amended in 2007 with the purpose of altering the definition of "the press" to include "websites in generally accessible telecommunication networks."[101] This law neither defines nor establishes clear criteria for what is a news-oriented website; a website is described as an electronic means of disseminating information to the general public not less frequently than once a period of six months.[102] In order to be regarded as part of news media, websites are required to obtain an official registration certificate in a procedure similar to that required for traditional news media outlets.[103] This procedure is generally known to be content-based, arbitrary, and inhibits editors and readers from exercising their freedom of expression.[104] Applications for press certificates are supposed to include details such as the website's digital media title, founder(s), language, aims and purposes, content specialization, domain name, sources of

[100] Joint Resolution of the Plenums of the Supreme Court and Higher Economic Court RU "О судебной власти" [On the Judicial Branch of Power] No. 1, 20 Dec. 1996, as amended on December 22, 2006 (No. 14/151), at para. 3 (justifying the rule that all judges are appointed by the President of Uzbekistan).

[101] Law RU "О средствах массовой информации" ["On the Mass Media"] No. 541-I, adopted December 26, 1997, as amended on January 15, 2007, *SZRU* (2007) No. 3, item 20, at Art. 4.

[102] Ibid.

[103] Resolution of the Cabinet of Ministers RU "О дальнейшем совершенствовании порядка государствен ной регистрации средств массовой информации в Республике Узбекистан" [On the Further Development of the Procedure for State Registration of the Mass Media in the Republic of Uzbekistan] No. 214, October 11, 2006, in *SP RU* (2007) No. 14, item 141, at Art. 8.

[104] UN Human Rights Committee, *Mavlonov and Sa'di v. the Republic of Uzbekistan*, Communication No. 1334/2004, Views adopted on April 29, 2009, UN Doc. CCPR/C/95/D/1334/2004, at paras. 2.6, 2.11 and 8.3.

financing, editor(s), address of an editorial office, as well as affiliation of the founder(s) or editor(s) with other mass media outlets.[105] Journalists or non-media professionals affiliated with registered online news media outlets are awarded certain rights and must abide by statutory conditions that are applicable to professional journalists, arguably creating, in practice, an environment where journalists' key responsibility is "loyalty to the regime."[106] As of December 2011, there were about 160 private websites registered as mass media in Uzbekistan.[107]

The legislation regulating the exercise of freedom of expression applies equally to traditional news media outlets and the internet. Due to the 2007 amendments, the law "On the Mass Media" is applicable to overseas news media outlets whose content is accessible from within the territory of Uzbekistan.[108] No cases of this law being invoked by Uzbek courts against foreign websites have been reported so far. In addition, some laws have been used to punish individuals for posting or accessing content deemed to violate vague information security rules.[109] Under the criminal code, slander (Article 139) and insult (Article 140)—including of the president (Article 158)—are criminal offenses that also apply to online content, as do provisions that punish activities such as "dissemination of materials posing a threat to public safety." Both slander and insult are punishable with fines ranging from 50 to 100 times the minimum monthly wage, correctional labor of two to three years, arrest of up to six months, or detention for up to six years.[110]

Beginning in 2010, online journalists have been prosecuted under charges of libel, defamation, and insult,[111] as well as for the production, storage, and propagation of materials inciting national, racial, or religious animosity.[112] However, no such incidents took place in the reported period.

On January 19, 2013, Olam.uz, which at the time was Uzbekistan's second most-visited news site, chose to go offline for "technical reasons," according to its Facebook page. However, as independent sources report, the Uzbek authorities had opened up proceedings against its editor-in-chief and the website owner, the Tashkent-based LLC Mobile Mass Media.[113] Charges included such offences as the infringement of copyright and patent law, high treason, encroachment upon the constitutional order, espionage, subversive act, loss of documents containing state or military secrets, and robbery. At the time of its disconnection, Olam.uz was reporting extensively about the Uzdunrobita (MTS-Uzbekistan) case and was allowing readers to leave comments on every article published.

---

[105] Resolution of the Cabinet of Ministers RU No. 214, note 109 above, at Annex II.
[106] Olivia Allison, "Loyalty in the New Authoritarian Model: Journalistic Rights and Duties in Central Asian Media Law," in Eric Freedman and Richard Schafer (eds.), After the Czars and Commissars: Journalism in Authoritarian Post-Soviet Central Asia (The Eurasian Political Economy and Public Policy Studies Series, Michigan State University Press, April 2011), 143-160, at 154-155.
[107] Parliament RU, "Меры поддержки негосударственных СМИ" [Measures Supporting Independent Mass Media], December 28, 2011, http://www.parliament.gov.uz/ru/analytics/5051?sphrase_id=12000.
[108] Law RU "On the Mass Media," at Art. 2.
[109] Zhanna Kozhamberdiyeva, "Freedom of Expression on the Internet: A Case Study of Uzbekistan."
[110] Article 139 and Article 140, Criminal Code of the Republic of Uzbekistan, http://bit.ly/1aA516n.
[111] For the cases of Vladimir Berezovsky, Abdumalik Boboyev, and Viktor Krymzalov, see Freedom of the Net 2012: Uzbekistan.
[112] For the case of Elena Bondar, see Freedom of the Net 2012: Uzbekistan. Elena Bondar was given refugee status in Kyrgyzstan in May 2013.
[113] Uznews.net, "Uzbek olam.uz news site shut down, staff accused of high treason," January 29, 2013, http://bit.ly/19KDiic; Id., "Is olam.uz trying to hide its criminal charges?", February 1, 2013, http://bit.ly/18eYayZ.

As of April 2013, two Uzbek online journalists remained in jail, ostensibly on fabricated criminal charges. Solidzhon Abdurakhmanov, a reporter for the independent news website Uznews.net, continues to serve a 10-year sentence imposed in October 2008 for allegedly selling drugs. Prior to his arrest, he had reported on human rights and economic and social issues, including corruption in the Nukus traffic police office, which fueled suspicions that the drug charges were trumped-up and in retaliation for his reporting.[114] Dilmurod Saiid, a freelance journalist and human rights activist, is serving a 12.5 year sentence imposed in July 2009 on extortion charges. Before his detention, he had reported on government corruption in Uzbekistan's agricultural sector for local media and independent news websites.[115] No new cases of prison sentences were documented between January 2011 and April 2013.

The authorities have also used various forms of arbitrary detention and intimidation to silence online critics. In November 2011, the government released Jamshid Karimov, an independent journalist and nephew of the president, from a psychiatric hospital where he had been kept against his will since September 2006. Prior to his detention, he regularly published articles on online websites, including about human rights abuses in Uzbekistan. He is widely believed to have been detained in retaliation for his journalistic activity. In January 2012, he suddenly disappeared again and his whereabouts remain unknown as of April 2013.[116]

While there have been no reports of government agents physically attacking bloggers or online activists, the National Security Service (NSS) has been known to employ various intimidation tactics to restrict freedom of expression online. For example, in June 2011, there were reports of NSS officers confiscating electronic media devices at the airport, checking browsing histories on travelers' laptops, and interrogating individuals with a record of visiting websites critical of the government.[117]

The use of proxy servers and anonymizers remains a very important tool and the only way to access content blocked in Uzbekistan. However, in September 2012, Uztelecom started a centralized and permanent blocking of proxy servers and websites enlisting free proxies without a web interface.[118] At the same time, the use of both proxies and anonymizers require computer skills beyond the capacity of many ordinary users in Uzbekistan.

---

[114] "Government increases pressure on Uzbek journalists," Committee to Protect Journalists, February 17, 2010, http://cpj.org/2010/02/government-increases-pressure-on-uzbek-journalists.php.

[115] "Uzbek appeals court should overturn harsh sentence," Committee to Protect Journalists, September 3, 2009, http://cpj.org/2009/09/uzbek-appeals-court-should-overturn-harsh-sentence.php; See also, "Дождется ли Дильмурад Сайид справедливости?" [Will Dilmurad Saiid receive justice?], Uznews.net, April 2, 2010, http://www.uznews.net/news_single.php?lng=ru&cid=3&nid=13210.

[116] "Jamshid has the rights to live freely!" Human Rights Society of Uzbekistan, January 20, 2012, http://en.hrsu.org/archives/1367; "Uzbekistan: UPDATE – Human rights defender released from forcible detention in psychiatric hospital," Front Line Defenders, November 30, 2011, http://www.frontlinedefenders.org/node/16704.

[117] "Farg'ona aeroportida yo'lovchilar noutbuki tekshirilmoqda" [At the Ferghana Airport, the Laptop Computers of Passengers Are Being Checked], Ozodlik.org, June 2, 2011, http://www.ozodlik.org/content/fargona_aeroportida_yolovchilar_noutbuki_tekshirilmoqda/24212860.html.

[118] Uznews.net, "Интернет-цензура Узбекистана стала еще жестче," 10 October 2013, http://www.uznews.net/news_single.php?lng=ru&cid=30&nid=20962.

The space for anonymous online communication in Uzbekistan is steadily shrinking. As mentioned above, the year 2011 saw the closure of Arbuz.com, one of the country's most important online forums for anonymous discussion, after the arrest of several users. The site's founder told media that several people who had been active contributors to a forum about Kyrgyz-Uzbek ethnic clashes in 2010 had been detained.[119] According to some reports, the NSS had tracked them through their internet protocol (IP) addresses.[120] Increasingly, few options remain for posting anonymous comments on other online forums—such as Uforum.uz,[121] which is administered by the state-run Uzinfocom Center—as individuals are increasingly encouraged to register with their real names to participate in such discussions.[122] Individuals must also provide a passport to buy a SIM card.[123] There are no explicit limitations on encryption, though in practice, the government strictly regulates the use of such technologies.[124]

Although Article 27 of the constitution guarantees the secrecy of "written communications and telephone conversations," there is no data protection legislation in Uzbekistan. The government employs systematic surveillance of internet and ICT activities, including the e-mail correspondence of Uzbek political activists and comments in online forums. A 2006 Resolution of the President authorizes the NSS to conduct electronic surveillance of the national telecommunications network by employing a "system for operational investigative measures" (SORM), including for the purposes of preventing terrorism and extremism.[125] The state-owned telecommunications carrier Uztelecom, private ISPs, and mobile phone companies are required to aid the NSS in intercepting citizens' communications and accessing user data. This includes a requirement to install SORM equipment in order to obtain an ISP license.[126] ISPs face possible financial sanctions or license revocation if they fail to design their networks to accommodate electronic interception.

The scope of violations against digital media users' privacy is difficult to evaluate amid government secrecy and a provision in the Law on Telecommunications that prohibits service providers from disclosing details on surveillance methods.[127] Moreover, there is no independent oversight to guard against abusive surveillance, leaving the NSS wide discretion in its activities.[128] Adopted on

---

[119] "Uzbek chat room closes political topics after government pressure," Uznews.net, February 9, 2011, http://www.uznews.net/news_single.php?lng=en&cid=3&sub=&nid=16297.
[120] IWPR "Web Use Spirals in Uzbekistan Despite Curbs," news briefing, January 3, 2012, http://bit.ly/sqYKRF.
[121] UForum.uz, "Правила форума" [Terms of Use], at http://uforum.uz/misc.php?do=cfrules.
[122] U.S. Department of State, "Uzbekistan," Counter Reports on Human Righst Practices for 2011, p 16, http://www.state.gov/documents/organization/186693.pdf.
[123] MTC Uzbekistan, "How to subscribe," http://www.mts.uz/en/join/.
[124] Resolution of the President RU "О мерах по организации криптографической защиты информации в Республике Узбекистан" [On Organizational Measures for Cryptographic Protection of Information in the Republic of Uzbekistan] No. ПП-614, April 3, 2007, *SZ RU* (2007) No 14, item 140, at Art. 1.
[125] Resolution of the President RU "О мерах по повышению эффективности организации оперативно-розыскных мероприятий на сетях телекоммуникаций Республики Узбекистан" [On Measures for Increasing the Effectiveness of Operational and Investigative Actions on the Telecommunications Networks of the Republic of Uzbekistan] No. ПП-513, November 21, 2006, at Preamble and Arts. 2-3.
[126] Ibid., at Art. 5.8. Infra., note 110. Also, tax and custom exemptions apply for import of the SORM equipment by domestic ISPs, see Tax Code of RU, at Arts. 208, 211, 230 part 2, and 269.
[127] Law RU, "On Telecommunications," at Art. 18.
[128] Resolution of the President RU, note 108 above. See, Criminal Procedural Code of RU, *Vedomosti Oliy Mazhlisa RU* (1995) No. 12, item 12, at Art. 339 part 2, "Tasks of Investigation," and Art. 382, "Competences of the Prosecutor." Resolution of the President RU No. ПП-513, note 87 above, at Art. 4.

December 26, 2012, a long-awaited law on "Operational and Investigative Activity" failed to give more guarantees against abusive state surveillance of telecommunications networks.[129] According to Articles 16 and 19 of this law, content intercepted via surveillance of telecommunications networks is admissible as evidence in court.

Since July 2004, cybercafes and other providers of public internet access have been required to monitor their users and cooperate with state bodies, an obligation that is generally enforced. Uzbek security agents stepped up surveillance of cybercafes after violent clashes between ethnic Kyrgyz and Uzbeks took place in Kyrgyzstan during the summer of 2010.[130]

In March 2012, the president signed a resolution "On measures for the further implementation and development of modern information-communication technologies," which outlines a stage-by-stage plan for the establishment of a national information system integrating the information systems of state bodies as well as individuals between 2012 and 2014.[131] The announcement raised concerns that the integrated system might enable greater state surveillance of user activities.

A few distributed denial-of-service (DDoS) attacks were reported in January 2013. First, the official website of the National Movement of Uzbekistan, Uzxalqharakati.com, was attacked for the third time since its registration in May 2011.[132] The attack paralyzed the website for several days. Second, there were two DDoS attacks against the website of the Uzbek national radio and television company, Mtrk.uz. The hacker group Clone-Security claimed to be behind the DDoS attacks for politically motivated reasons, and launched the attacks from within Uzbekistan.[133]

In 2005, the government established the Computer Emergency Readiness Team (UZ-CERT) as an operational arm of the State Committee on the CITT dealing with cybercrime.[134] UZ-CERT cooperates with law enforcement bodies to prosecute cybercriminals, and the criminal code contains several provisions addressing these issues in a section dedicated to information technology crimes.[135]

---

[129] Law RU "Об оперативно-розыскной деятельсности" [On Operational and Investigative Activity] No. ЗРУ – 344, December 26, 2012, SZ RU (2012) No. 52 (552), item 585, at Arts. 16, 19.
[130] "Attacks on the Press 2010: Uzbekistan," Committee to Protect Journalists, February 15, 2011, http://www.cpj.org/2011/02/attacks-on-the-press-2010-uzbekistan.php.
[131] Resolution of the President RU "О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий" [On Measures on the Further Impelmentation and Development of Modern Information and Communication Technologies], No. ПП-1730, 21 March 2010, SZRU (2012), 13 (513), item 139, at Annex II.
[132] Ozodlik.org, "Атака на сайт Народного Движения Узбекистана," January 27, 2013, http://www.ozodlik.org/content/article/24884770.html.
[133] Ozodlik.org, "В Узбекистане сайт МТПК подвергся хакерской атаке," January 31, 2013, http://www.ozodlik.org/content/article/24888716.html.
[134] Resolution of the President RU "О дополнительных мерах по обеспечению компьютерной безопасности национальных информационно-коммуникационных систем" [On Further Measures Supporting the Maintenance of Information Security of the National Information and Communication Systems], No. 167, September 5, 2005, at Preamble and Arts. 2 and 7.
[135] Ibid., at Annex II, Art. 8. See, Criminal Code Article 278-1 "Violation of the Rules of Informatization"; Article 278-2 "Illegal (Unsanctioned) Access to Computer Information"; Article 278-3 "Production and Dissemination of Special Tools for Illegal (Unsanctioned) Access to Computer Information"; Article 278-4 "Modification of Computer Information"; and Article 278-5 "Computer Sabotage."

VENEZUELA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	15	16
Limits on Content (0-35)	14	16
Violations of User Rights (0-40)	19	21
Total (0-100)	**48**	**53**

* 0=most free, 100=least free

POPULATION: 29.7 million
INTERNET PENETRATION 2012: 44 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Disruptions of internet service occurred at crucial times in Venezuela during 2012 and 2013, most notably during the April 14th presidential election and the subsequent count of electoral votes (see **LIMITS ON CONTENT**).
- The websites of key opposition candidate Henrique Capriles Radonsky and independent news sites were blocked during the October 7th presidential election (see **LIMITS ON CONTENT**).
- In 2012 and 2013, the Venezuelan government increased its efforts to identify social media users who had posted objectionable information online, especially concerning social and political issues (see **VIOLATIONS OF USER RIGHTS**).
- Bloggers and journalists writing about President Chavez's health—or subsequent death—were subject to increasing harassment and intimidation by government supporters in 2012 and 2013 (see **VIOLATIONS OF USER RIGHTS**).
- Politically-motivated cyberattacks and hijackings of social media accounts increased in 2012 and 2013 (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

In a country where all government branches act in compliance with the interests of the ruling party, ensuring a hegemonic ICT system characterized by informational opacity,[1] the Venezuelan people widely use the internet to participate in social networks.[2] Recent tensions regarding the death of President Hugo Chávez and the opposition's contestation of newly elected President Nicolas Maduro have resulted in increased use of digital media in Venezuela.[3] In response to the popularity of such technology among the general population as well as the political opposition, the government has begun to expand its control of the internet.[4]

As government opponents have made their opinions known via global platforms, Chávez's ruling United Socialist Party of Venezuela (PSUV) has increased its efforts to influence online discussions and to restrict online content. In 2012 and early 2013, harassment increased, targeting those critical of government. Sporadic blocking of opposition and independent news websites, as well as cyberattacks and hackings that temporarily disabled such sites, became a problematic trend. Such actions witnessed a surge at times of heightened political sensitivity and were particularly pronounced surrounding presidential elections and speculation over the health of President Chavez.

Among the most disturbing developments of 2012 and 2013 were incidents of cyberattacks focused on critical media, the usurpation of the Twitter profiles of political activists, and the rise of anonymous Twitter accounts. Such accounts have emerged as a new tool by which to pursue legal action against government critics. Although there is often no evidence that members of the opposition are, in fact, the authors of such sites, objectionable content posted online is attributed to them and used to justify their arbitrary detention.[5]

The internet arrived in Venezuela in 1992. The first commercial internet service providers (ISPs) were granted licenses by the National Telecommunications Committee (CONATEL) in 1996.[6] While the 1999 constitution obligates the State to provide the public with access to new information and communication technologies (ICTs),[7] the Organic Law of Telecommunications

[1] Information regarding President Chávez's health has been sporadic and has come only from Vice President Maduro and Minister of Communication Ernesto Villegas rather than from an independent team of physicians. See: *Access to Health Information from the Heads of State* (Regional Alliance for Free Expression and Information), http://transparencia.org.ve/wp-content/uploads/2013/01/Salud-y-Presidentes-Alianza-Regional-LDE.pdf. In the days between his return to Venezuela and his death, the only evidence that President Chavez was alive consisted of an official report and three tweets allegedly sent by Chavez on the day he returned to his country. See: Ultimas Noticias, "Chávez Tuitea," [Chávez Tweets], *Últimas Noticias* online, Feb 18, 2013, http://www.ultimasnoticias.com.ve/noticias/actualidad/politica/chavez-ya-tuitea.aspx.

[2] Tendencias Digitales, "Internet Statistics in Venezuela 2012," presented in the framework of the event 'State of the Internet in Venezuela and its Impact on Business,' Caracas, May 2012.

[3] Laura Vidal, "Venezuela Tuits y Etiquetas Electorales," [Venezuela Election Tweets and Tags] *Global Voices* online, October 8, 2012, http://es.globalvoicesonline.org/2012/10/07/venezuela-tuits-y-etiquetas-electorales/.

[4] Espacio Público, "Ataques Informáticos Sacuden las Redes Sociales en el País," [Hacking Shakes Social Networks in the Country] October 16, 2012, http://bit.ly/15Az8pL.

[5] "Investigan Presunta Instigación al Terrorismo en Twitter," [Investigation into Alleged Incitement to Terrorism on Twitter] *Últimas Noticias* online, January 8, 2013, http://bit.ly/WtJ3IH.

[6] UNDP, Las Tecnologías de Información y Comunicación al Servicio del Desarrollo [Information and Communication Technologies for Development] (Caracas: UNDP, 2002), 249.

[7] See: Article 108 and Article 110 of the Venezuelan Constitution: http://www.tsj.gov.ve/legislacion/constitucion1999.htm.

(reformed in December 2010) declares ICT an area of state interest.[8] Although privately owned companies do exist, the state dominates the internet market through the National Telephone Company of Venezuela (CANTV). Investment in and expansion of the private ICT sector are complicated by disadvantageous competition with CANTV, foreign currency exchange control, and the difficulty private companies face when they attempt to repatriate their earnings.[9]

OBSTACLES TO ACCESS

By the end of 2012, internet penetration in Venezuela had reached 44 percent.[10] This figure excludes internet connections mediated by mobile phones, for which there are no official numbers, indicating that penetration may be even higher.[11] Over 95 percent of the approximately 3.7 million internet subscriptions in Venezuela were broadband, evidence of a substantial shift from dial-up to broadband technology.[12] According to data provided by the consultancy firm Tendencias Digitales (Digital Tendencies), more than 50 percent of internet users in Venezuela are under 25 years old. The majority of internet connections come from households (71 percent), followed by internet cafes (30 percent) and mobile phones (21 percent).[13] Venezuelans use the internet primarily to visit social networks—there are nearly 10 million Venezuelan Facebook users and over 3 million Twitter users[14]—to read the news, and to search for information. Key topics disseminated and debated through this medium include politics and news.[15] There are no special restrictions on the opening of cybercafés in Venezuela.

The most substantial obstacles to internet access in Venezuela are lack of service availability, slow connection speed, geographic isolation in rural areas, low computer literacy, and the expense of necessary equipment. The cost of access itself is likely a less significant obstacle, however service remains poor. The regional divide in internet access in Venezuela is noteworthy. Penetration exceeds 90 percent in the Capital District and Miranda State, while in poorer states such as

[8] In July 2008, a plan to reform the law was met with great opposition. As a result, the measure was not introduced or approved in the National Assembly until December 2010.

[9] The repatriation of capital is subject to authorization by the Currency Administration Commission (Cadivi), which in most cases either does not process it or does so with significant delay.

[10] ITU, Time Series by Country (2000-2012) "Percentage of Individuals Using the Internet," ITU World Data – Statistics, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[11] Vicepresidencia de la Republica Bolivariana Venezuela, "Estadistica de Telecommunicaciones al Cierre del IV Trimestre de 2012" [Telecommunication Sector Statistics at the End of 2012], Accessed February 27, 2013, http://conatel.gob.ve/#http://conatel.gob.ve/index.php/principal/presentacionresultados. In some areas traders also resell individual connections through routers, indicating that the percentage of the population accessing the internet may be even higher than official figures suggest, although the incidence of resold connections would be impossible to measure. See also: *La Nación*, "Venezuela: ¿Medalla de Oro en Uso de Internet?" [Venezuela: Gold Medal in Internet Use?], *La Nación* online, August 7, 2012, http://www.lanacion.com.ve/tecnologia/venezuela-medalla-de-oro-en-uso-de-internet/.

[12] Vicepresidencia de la Republica Bolivariana Venezuela, "Estadistica de Telecommunicaciones al Cierre del IV Trimestre de 2012" [Telecommunication Sector Statistics at the end of 2012], Accessed February 27, 2013, http://bit.ly/1azPe7A.

[13] Tendencias Digitales, "Internet Statistics in Venezuela 2012," Presented in the framework of "State of the Internet in Venezuela and Its Impact on Business," Caracas, May 2012.

[14] Social Bakers, "Facebook Statistics by Country," Accessed January 13, 2013, http://www.socialbakers.com/facebook-statistics/; See also: Twven, "Facebook y Twitter en Venezuela," *Twven* (blog), http://twven.com/twitter-venezuela/facebook-y-twitter-en-venezuela/.

[15] *El Universal*, "Facebook y Twitter en Venezuela," *El Universal* online, June 25, 2012, http://bit.ly/Q2TOBj.

Amazonas, Yaracuy, and Apure, penetration hovers around 15 percent.[16] Connectivity in rural areas has been further compromised by a severe electricity crisis that has led to rationing in every city but the capital, Caracas. Regional disparities are also evident in the expansion plans of telecommunications companies, which typically focus new investments on the capital and surrounding areas.[17]

By the end of 2012, mobile phone penetration in Venezuela had exceeded 100 percent.[18] This figure does not necessarily reflect a population saturated with mobile technology, however. Some Venezuelans have as many as three phones, each associated with a different mobile provider, in order to ensure countrywide coverage. Over one third of Venezuela's mobile subscribers use CDMA technology. Although the number of users with smart phones and data plans is growing, currency exchange control and the devaluation of the Venezuelan bolivar have resulted in high prices and a limited supply of advanced mobile phones.[19] Those who do have smartphones typically live in urban areas and have higher than average income levels.

Following its 2007 re-nationalization, a move that benefited CANTV significantly in regard to currency controls, the company increased the country's fiber-optic backbone infrastructure by 48 percent.[20] While this figure reflects significant growth in broadband internet access, quality of service remains poor. Venezuela's fixed broadband penetration and speed are lower than the regional average and less than would be expected based on GDP per capita, which is higher in Venezuela than in Latin America as a whole.[21]

Despite growth in internet and mobile phone use in recent years, development in the ICT sector has slowed overall, and in some respects has slid backward since CANTV's re-nationalization. Instead of being reinvested to improve ICT services, the earnings obtained by CANTV are reserved for social programs in the health and education sectors.[22] With 51.92 percent of internet subscribers and a monopoly on ADSL service, CANTV dominates the fixed, mobile, and broadband markets.[23] The company's dominant position stifles competition, some of which comes from cable

---

[16] Vicepresidencia de la Republica Bolivariana Venezuela, "Estadistica de Telecommunicaciones al Cierre del IV Trimestre de 2012" [Telecommunication Sector Statistics at the end of 2012], Accessed February 27, 2013, http://bit.ly/18zRVXl.

[17] Inside Telecom, Vol. III No. 95, December 19, 2012 (Excerpted from company newsletter; not available online).

[18] Vicepresidencia de la Republica Bolivariana Venezuela, "Estadistica de Telecommunicaciones al Cierre del IV Trimestre de 2012" [Telecommunication Sector Statistics at the end of 2012], p.6, Accessed February 27, 2013, http://bit.ly/18zRVXl.

[19] Heberto Alvarado Vallejo, "Mercado Móvil Venezolano Tendrá Sabor Agridulce en 2013" [2013 Mobile Market in Venezuela Will be Bittersweet], Hormiga Analítica, Accessed May 13, 2013, http://bit.ly/1azPe7A.

[20] As a state company, CANTV enjoys preference for Cadivi's currency approvals. See: Casetel Chamber of Business Telecommunications Services, "Oswaldo Cisneros Sigue Apostandole a Venezuela: Digitel Busca Vías para Consolidarse en 3G," [Oswaldo Cisneros Keeps Betting on Venezuela: Digitel Seeks Ways to Consolidate in 3G] June 23, 2010, http://www.casetel.org/detalle_noticia.php?id_noticia=509.

[21] Budde.com, "Venezuela - Telecoms, Mobile, Broadband and Forecasts," Budde.com, July 2012 Publication, http://www.budde.com.au/Research/Venezuela-Telecoms-Mobile-Broadband-and-Forecasts.html.

[22] Ministerio de Ciencia y Tecnología, "Gobierno Nacional Honra Pagos de Prestaciones con Dividendos de CANTV" [National Government Honors Benefit Payments with Dividends from CANTV], April 4, 2012, http://www.mcti.gob.ve/Noticias/14031; See also: Luigino Braci, "¿Las Peores Velocidades de Internet Están en Venezuela? Sí, pero..." [Venezuela has the Worst Internet Speeds? Yes, but…], May 31, 2013, http://lubrio.blogspot.com/2012/05/las-peores-velocidades-de-internet.html.

[23] According to a Google Analytics study, in South America, only Paraguay and Bolivia have slower connection speeds than Venezuela. See: Google Analytics, Global Site Speed Overview, April 2012, http://analytics.blogspot.com.es/2012/04/global-site-speed-overview-how-fast-are.html; See also: (1) International Telecommunications Union (ITU), *Measuring the Internet*

modems, mobile broadband, and satellite connections.[24] Inter, the company that places a distant second in the market, offers a triple pack that includes cable television, cable modem, and telephony.[25]

Although CANTV's connections are slow, its relatively low prices have given the company an edge in the market. Private providers have had difficulty competing with CANTV's rates, a reality that accounts in large part for the decline of the ICT sector's contribution to GDP.[26] The lack of competition has also reduced incentives for providers to retain high quality service or to expand their offerings.[27] In several recent cross-country studies assessing ICT trends over the past five years, Venezuela is among the countries that have fallen farthest in the rankings relative to its peers.[28]

While more people are now connected to the internet, the majority of the population has access only to narrowband service.[29] Nationally, CANTV offers a prepaid plan with a minimum connection speed of 512 Kbps at a cost of about $10.50 per month, compared to a minimum wage of about $324.[30] The most popular plan, called "ABA Para Todos" (broadband for everyone) offers a connection speed of 1.5 Mbps at a cost of $22.81 per month.[31] In April, the president of CANTV announced a new 4 Mbps plan at a cost of $79.20 per month, which represents nearly a quarter of the minimum wage. In a May 2013 announcement, President Maduro announced that connection speed would increase to 6Mbps, but this advancement has not yet come to fruition.[32]

The policies developed by CANTV to massively increase subscription rates have been detrimental to quality of service, a development that has generated online campaigns from users.[33] In early May

---

Society 2011, March 2012, http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf; (2) Inside Telecom, "Los Tres Potentes Liderazgos de Cantv" [The Three Powerful Leaders of CANTV], November 1, 2012, http://bit.ly/U4OSRO.

[24] Hernan Galperin, "Precios y Calidad de la Banda Ancha en America Latina: Benchmarking y Tendencias" [Prices and Quality of Broadband in America: Benchmarking and Trends], Universidad de San Andrés (Argentina), 2012, http://bit.ly/PsBDoY.

[25] Budde.com, Venezuela - Telecoms, Mobile, Broadband and Forecasts, Accessed January 7, 2013, http://bit.ly/1dPLzoe.

[26] Inside Telecom, Volume 7 No. 86 (2011): In late 2012, after 14 months of request, Movistar was given the authority to increase its rates from 9%-17% for annual inflation. Movilnet, for its part, increased 32.6% (excerpt from newsletter; not available online).

[27] Jorge Espinoza, *Argumentos in Situ de Las Operadoras Móviles Privadas: Smartphones e Internet Móvil Suplen Carencias Fijas* [Arguments in Situ of Private Mobile Phone Operators: Smartphones and Mobile Internet Fized Unfilled Gaps], Inside Telecom, May 25, 2012.

[28] Kai Bucher, "Las Economias Latinoamericanas Todavia Estan Atrasadas en el Aprovechamiento de las Tecnologias de la Informacion..." [The Latin American Economies are Still Behind in the Use of Information Technologies], World Economic Forum, 2010-2011 Report, http://bit.ly/gnrzob; Venezuela dropped from #74 to #77 on ITU's 2012 Index. See: ITU, Measuring the Information Society 2012 (Geneva: ITU, 2012), http://bit.ly/1fyOEgO.

[29] Raisa Urribarrí: "La Comunicación Alternativa es Antihegemónica" [Alternative Communication is Hegemonic], *Diario Tal Cual*, August 11, 2012, Reproduced online at: http://bit.ly/1bRqJXb.

[30] *El Universal*, "Cantv Mejora Velocidad de Conexión a Internet" [Cantv Improves Internet Speed], *El Universal* online, September 3, 2012, http://bit.ly/REHRjy; CANTV, Planes y Servicios del Servicio de Banda Ancha (ABA) [Service Plans and Broadband Services], January 2013, http://bit.ly/qlCVIQ; See also: *El Universal*, "A partir de hoy el salario mínimo es de 2047,48 Bs" [Starting Today, the Minimum Wage is 2047.48 Bs] S *El Universal* online, September 1, 2012, http://bit.ly/TIwBEy.

[31] See: CANTV´s Connection Plans, Accessed May 27, 2013, http://bit.ly/f42m4R.

[32] Radio Mundial, "Gobierno Nacional Anuncia Nueva Conexión ABA de 6 Megas" [Government Announces New ABA Connection of 6 Mbps], Radio Mundial online, May 21, 2013, http://bit.ly/13J2pRW.

[33] Activism, "CANTV: Solicitamos Formalmente Mejorar Significativamente las Velocidades de Download y Upload del ABA en Venezuela" [CANTV: Formal Requests Significantly Improve the Download and Upload Speeds of ABA in Venezuela], Activism online, Accessed January 11, 2013, http://bit.ly/1biXwVW; Netindex.com reports that internet connection in Venezuela is one

2013, on Internet Day, a group of activists launched a petition entitled "For a Better Internet for Everyone in Venezuela" through Change.org. To date the document has been signed by approximately 1,200 people.[34]

Substantial interruptions of telecommunication services, such as the fall of the entire .ve internet domain, have begun to occur, however, Venezuelan authorities have not been forthcoming regarding the root of the problem.[35] CANTV's slow progress increasing Mbps (and consequently internet speed) for fixed lines has elevated mobile internet to the point that it is now poised to take half the market,[36] yet while there are approximately 30 telecommunications operators in the country, only three provide mobile phone services. Movistar, the Venezuelan unit of Spain's Telefónica, has nearly 10 million subscribers; Digitel, a locally owned private company, has approximately 4 million subscribers; and CANTV's Movilnet, which leads the market, has 15.5 million subscribers out of a total of 29 million.[37] A recent CANTV initiative, "Buy Made in Venezuela," which aims to give preference to locally produced cell phones manufactured by Vtelca and Orinoquia in partnership with the Chinese firms ZTE and Huawei, has resulted in decreased availability.[38] Local manufacturers cannot satisfy national demand, and the state's blocking of foreign currency has made it difficult to import mobile phones from foreign manufacturers.[39] Local manufacturers cannot satisfy national demand, and the state's blocking of foreign currency has made it difficult to import mobile phones from foreign manufacturers.[40] These two factors have resulted in price speculation as well as a shortage of cell phones within the country.[41]

The networks run by private mobile phone service providers suffer from severe congestion and require further development. Discriminatory currency controls, however, have forced these providers to ration their services and to decrease investment in infrastructure.[42] Digitel, Movistar, and MovilMax (a WiMAX provider only available in the nation's capital city) plan to deploy 4G/LTE networks in 2013 and 2014.[43] Public universities, such as the Universidad de Los Andes, which were once leaders in the telecommunications field, have witnessed the deterioration of their

---

of the most expensive and slowest in the world. See: *BBC Mundo* online, "Como un Pais Desaparece de Internet," [How a Country's Internet Disappears] May 2012, http://bbc.in/KEy5NO.

[34] Espacio Público A.C., "Por un Internet de Calidad Para Todos en Venezuela" [For a Better Internet For Everyone in Venezuela], Change.org, May 17, 2013, https://www.change.org/es-LA/peticiones/internet-de-calidad-para-todos-en-venezuela.

[35] Notitarde, "Falla en el Sistema 'nic.ve' Mantiene Sin Servicio a Todos los Dominios '.ve'" [System Failure nic.ve Remains Without Service] May 28 2012, http://bit.ly/19ehDgg.

[36] Víctor Suárez, "La Vergüenza de Estar Siempre en el Mismo Lugar, o Más Atrás: Estado de Internet en Venezuela" [The Shame of Being Always in The Same Place, or Further Back: State of the Internet in Venezuela], Inside Telecom, August 15, 2012, http://m.insidetele.com/index.php?article_id=-6637399748013051426.

[37] Inside Telecom, "Los Tres Potentes Liderazgos de Cantv" [The Three Powerfu l Leaders of Cantv], Inside Teleocm online, November 1, 2012, http://m.insidetele.com/index.php?article_id=-5703104260882784216.

[38] Gobierno Bolivariano de Venezuela, "Menéndez: Distribuidos 328 Mil Equipos Celulares de Fabricación Nacional" [Menendez: Distributed 328,000 Domestically Manufactured Cell Phones], MCTI, August 2011, http://bit.ly/16TO4AL.

[39] Rojas, Ingrid, "Falta de Divisas Limitó Importación de Celulares en el Año 2012," [Lack of Cellular Import of Limited Currency in 2012], *El Mundo, Economía y Negocios* online, January 2, 2013, http://bit.ly/12Wos6J.

[40] Rojas, Ingrid, "Falta de Divisas Limitó Importación de Celulares en el Año 2012."

[41] Inside Telecom, Vol. XIII No. 41, November 10, 2012 (newsletter; not available online).

[42] In 2013, most Internet plans were not available for new activations. Inter, which offers a 10MB navigation plan, is also closed for new activations at high speed and currently offers only 1MB. Websites of the three companies, accessed January 10, 2013: http://bit.ly/19NJUeJ; http://bit.ly/qlCVIQ; http://www.digitel.com.ve/Personas/Internet/Prepago.aspx#1.

[43] Budde.com, Venezuela - Telecoms, Mobile, Broadband and Forecasts, Accessed January 7, 2013, http://bit.ly/1dPLzoe.

service platforms due to lack of state resources.[44] In May 2013, the Ministry of Higher Education announced it would reduce broadband service provided to universities due to alleged underutilization.[45]

In addition to acting as the dominant service provider through CANTV, the state also administers ICT regulation and licensing through the state regulatory body CONATEL. Although incidents of CANTV engaging in censorship and monitoring have been isolated and have not suggested more systematic controls, the lack of independent oversight has raised concerns about the ease with which systematic content filtering and surveillance could be implemented in the future.[46] Article 35 of the Organic Law of Telecommunications provides for CONATEL's operational and administrative autonomy, however, the president has the power to appoint and remove the agency's director and the four members of its Directive Council. A series of presidential decrees over the past decade has shifted oversight of the commission to various ministries and finally to the vice president,[47] a progression to centralized control that has increased the agency's politicization.[48] In 2012, CONATEL continued to demonstrate progovernment bias in decisions related to broadcast media, although it has not yet made comparable judgments affecting internet or mobile phone service.

LIMITS ON CONTENT

Although Venezuelan authorities do not engage in systematic filtering of online content, they have sporadically used blocking, service disruptions, and other censorship tactics to restrict information at sensitive times. In 2012 and 2013, this was particularly evident in advance of presidential elections and as Chavez's health worsened, when several independent websites were either blocked or experienced disabling cyberattacks. During the April 2013 Presidential election, CANTV shut down broadband service for approximately 30 minutes, leaving 95 percent of Venezuelans disconnected from the internet at a crucial time. Pro-opposition and independent news websites were also temporarily blocked or disabled in Venezuela, and the website of the country's National Electoral Council was temporarily unavailable from both inside and outside of the country. Such restriction of information during pivotal times is a concerning development.

The sites of international news sources and human rights organizations such as Freedom House, Reporters Without Borders, and Amnesty International are freely available in Venezuela. Social media applications such as Facebook, Twitter, and YouTube are also freely accessible and are

[44] Nelson Espinoza, "Solventada Falla de la Red Teleinformática de la ULA" [ULA Solved Its Network Failure], Prensa ULA, January 10, 2013, http://uvero.adm.ula.ve/prensa/index.php/solventada-falla-de-la-red-teleinformatica-de-la-ula/.
[45] Urribarrí, Raisa, "El Cenit Reducirá el Ancho de Banda a las Universidades Venezolanas" [Government will reduce bandwidth toVenezuelan universities], Periodismo en Línea online, May 10, 2013, http://bit.ly/179du1z.
[46] Ryan Gallager, "Report: Silicon Valley Internet Surveillance Gear Use by Authoritarian Regimes," *Slate*, Jan 16, 2013.
[47] Andrés Cañizález, "Conatel, La Joya de la Corona," [Conatel: The Jewel in the Crown], *Tal Cual* Digital, August 9, 2010, http://www.talcualdigital.com/nota/visor.aspx?id=39046.
[48] Jesús Urbina, "Las Mordazas Invisibles: Nuevas y Viejas Barreras a la Diversidad en la Radiodifusion" [Invisible Jaws: New and Old Barriers to Diversity in Broadcasting], http://legislaciones.amarc.org/mordazas/VEN_pais.htm.

growing in popularity.[49] Despite the availability of human rights websites and social media networks, however, Venezuela's history of blocking key sites and interrupting internet service during times of heightened political sensitivity has continued over the past year. During the 2012 presidential campaign, for example, CANTV blocked the official website of the main opposition candidate, Henrique Capriles Radonsky.[50] On the day of the election, weekly newspaper *6to poder* (Sixth Power) also reported the blocking of its website during the final count of votes.

Continuous cyberattacks and hackings, which rendered websites temporarily inaccessible, also plagued a number of independent news sites during both the 2012 and 2013 elections. Problems accessing the website of *Noticiero Digital* (Digital News) were reported during the 2012 election. In the same period, the news channel Globovisión registered a general failure of its servers without explanation and the informational website *La Patilla* (The Watermelon), the thirteenth most visited site in the country, suffered continuous cyberattacks, which made it difficult, if not impossible, to access.[51]

The government has not offered any explanation for these attacks, blockings, and site disruptions, a problem compounded by the political situation in Venezuela in which there are no established checks and balances between the different branches of the state. Although the judiciary lacks independence, there have been no reports of judicially imposed censorship; instead, suppression comes from sporadic blocking and disruptions. In this context, there is no transparent process or independent institution through which website owners and content producers can pursue complaints.

Despite such continuing opacity regarding the availability of independent websites, the government has recently been forthcoming about two particular disruptions. During the highly contested presidential election of April 2013 (which would mark the country's first new leader in 14 years), broadband service offered by the national telephone company CANTV, the largest operator in the country, was shut down for approximately 30 minutes. Access to the webpage of the National Electoral Council was likewise unavailable to all CANTV subscribers, leaving 95 percent of those with internet access unable to track election results. Vice President Jorge Arreaza, who also held the post of Minister of Science and Technology until April 2013, informed the public that the service disruption was orchestrated by the government as part of an operation to identify those responsible for hacking into the Twitter accounts of interim and current president, Nicolas Maduro, as well as Chief of Press of the Government Palace, Teresa Maniglia.[52] Arreaza also announced that the website of the National Electoral Council would remain inaccessible from outside the country to prevent further attack.[53] Such a move also prevented the international

[49] Alexa, "Top Sites in Venezuela," Accessed January 10, 2013, http://www.alexa.com/topsites/countries/VE.
[50] *El Universal*, "Denuncian que CANTV Bloqueó Acceso a la Página Web Hay un Camino," [Complaints that CANTV Blocked Access to Website 'There is a Way'] *El Universal* online, August 14, 2012, http://bit.ly/O8im8N.
[51] Ratings from Alexa, Accessed January 4, 2013, http://www.alexa.com/topsites/countries/VE.
[52] Editor DJ el Dom, "Jorge Arreaza Pide Calma por Caída del Internet: Fue para Evitar Hackeos." [Jorge Arreaza Calls for Calm: It Was to Prevent Hacking], *Informe 21* online, April 14, 2013, http://bit.ly/ZjyI83.
[53] Alba Ciudad Radio, "Jorge Arreaza: Suspensión Momentánea de Internet se Hizo para Proteger a la Página Web del CNE de Ataques" [Jorge Arreaza: Momentary Internet Suspension was Made to Protect CNE Website Attacks], in video format, April 14, 2013, http://bit.ly/ZUXcjK.

community from attaining a real-time perspective on the election, which was of great international interest.

In December 2010, the National Assembly adopted a reform of the 2004 Law of Social Responsibility in Radio and Television (The Resorte Law), extending regulation to online and electronic media,[54] a move that has laid the groundwork for censorship of transmitted content by websites and service providers. According to the Committee to Protect Journalists, under the amended law, online media outlets are expected to establish mechanisms to restrict content that violates the law. Websites found in violation may be fined up to VEF 13,000 ($3,000). Service providers who do not respond to government inquiries risk high fines and temporary suspension of operations.[55] Despite these increasing restrictions, authorities have not vigorously enforced the law, and online content providers do not appear to be engaging in politically motivated deletions of user comments.

Venezuelans are avid users of digital media, which has emerged as an important platform for circulating information and expressing opinions at a time when independent television and radio stations have come under increased pressure.[56] Venezuela has approximately three million registered Twitter users, occupying the thirteenth place in the world and the fourth place in Latin America.[57] Rather than engaging in significant censorship, the government is making substantial use of social media platforms to propagate its point of view and counter political opposition. The Socialist Party proactively disseminates its views and counters opponents through pro-Chávez platforms, such as the website Apporrea.org, launched in 2002, and the Twitter feed "@RedVergataria," launched in 2011 with the support of CANTV's Movilnet and the Ministry of Popular Power for Science and Technology.[58]

This trend has intensified over the past year as a consequence of the president's prolonged illness and absence from the country, and his subsequent death.[59] During the first weeks of 2013, in the absence of independent medical reports on the president's health, use of Twitter was particularly intense. Although there have not yet been notable instances of the opposition utilizing social media for mobilization—even during the January 2013 swearing in of President Hugo Chavez in absentia,

---

[54] República Bolivariana de Venezuela, "Ley de Responsabilidad Social en Radio, Television y Medios Electronicos," [The Law of Social Responsibility in Radio, Television and Electronic Media] *Scribd*, accessed January 19, 2013, http://bit.ly/ek6v7E.
[55] ifex, "CPJ Condemns Two Media Laws," December 22, 2010, http://bit.ly/15CluUe.
[56] "Globovisión Supera los 2 Millones de Seguidores en Twitter, Líder entre los Medios Venezolanos en la Red, [Globovision Exceeds 2 Million Followers on Twitter], *Globovision*, January 15, 2013, http://bit.ly/Uoj6Nh.
[57] Marjuli Matheus, "Venezuela es el 13º País Más Activo en Twitter," [Venezuela is the 13th Most Active Country on Twitter] *Últimas Noticias* online, January 7, 2013, http://www.ultimasnoticias.com.ve/movil/noticia.aspx?idnota=119935.
[58] Government of Hugo Chávez, *Red Vergataria* (blog), accessed January 14, 2013, http://www.redvergataria.com/; See also: (1) Rachel Glickhouse, Explainer: Twitter in Latin America, Americas Society/Council of the Americas, January 18, 2013. http://bit.ly/YdKylj; (2) Americas Society/Council of the Americas, Digital Policy Council's World Leaders on Twitter Ranking Report, December 2012, http://bit.ly/TFkEBS; (3) Anais Lucena, "Lanzamiento de Red Social "Vergataria" en Twitter se Efectuó desde el Zulia" [Launch of Social Networking 'Vergataria' on Twitter was Made from Zulia State], *Radio Mundial*, October, 27, 2011, http://bit.ly/uJFZ1J; (4) *Patria Grande*, "Colectivos de Telecomunicaciones Lanzan @redvergataria para Organizacion Politica" [Collective @redvergataria Telecommunications to Throw Political Organization] October 10, 2011, http://bit.ly/mRxFXN.
[59] Comment on the Twitter page of a political journalist: "Until recently in the social networks *majunchismo* had certain hegemony," https://twitter.com/nerdysinperro/status/196247112772616194; See also: Diario ABC, "Chávez, Un Año de Enfermedad," [Chávez, A Year of Illness] Madrid, May 31, 2012, http://bit.ly/IR8OPJ.

an occurrence which the opposition described as a coup[60]—*Voluntad Popular* and other emerging political parties have begun to use social media to disseminate party news and to mobilize their supporters. Online campaigning by the opposition appears to be effective: in presidential elections, states with high internet penetration rates showed a higher proportion of votes in favor of the opposition, while in areas with low internet penetration, there was a higher proportion of votes in favor of the government candidate.

Chávez and his supporters have sought to gain the upper hand in a variety of ways, sometimes acting openly and fairly, but at times also resorting to opaque, manipulative tactics. Vice President Nicolás Maduro has clearly stated the government's assertive position, saying: "If lies come through Twitter we are going to strike back through Twitter."[61] The most recent Twitter controversy occurred after the disputed April 2013 presidential election. National Assembly deputy Pedro Carreño blamed ensuing violence on posts published to Twitter, and subsequently announced a bill to regulate social networking.[62] It remains to be seen exactly what sort of regulations would be contained in such a bill, and whether it would, indeed, be passed.

In April 2010, President Chávez opened his own Twitter account, @Chavezcandanga, which allowed him to connect to the Venezuelan people (and according to one opposition candidate, to make a mockery of the nation by ruling via Twitter[63]) after beginning treatment for cancer in Cuba in mid-2011.[64] By November 2012, Chávez had nearly four million followers, the largest number for any Venezuelan;[65] his popularity places him at the top of the list of most influential politicians on Twitter, second only to Barack Obama.[66] Following the creation of a presidential Twitter page, the government began an official campaign to increase Chavez's following, rewarding the 4 millionth follower with a house.[67]

In order to counter rumors about Chávez's health, which gained momentum in the absence of an independent medical report, progovernment digital communications specialists created an information vacuum that was filled with official updates from a single source. Real-name and anonymous tweeters with high numbers of followers then propagated rumors to contrast official updates.[68]

---

[60] "Ledezma: El oficialismo Dio un Golpe al Presidente Chávez" [Ledezma: The Ruling Gave a Blow to President Chávez], *El Universal* online, January 13, 2012, http://bit.ly/18ezy9K.
[61] Daniel Pabón, "El Vacío Informativo Entrampa a Twitter en Estridentes Rumores" [The Information Vacuum Filled by Rumors from Twitter], *El Carabobeño*, January 9, 2012, http://bit.ly/Xk2pmz.
[62] Últimas Noticias, May 8, 2013, "Pedro Carreño Anuncia que Hablará con Twitter por Violencia Postelectoral" [Pedro Carreño Announced that Twitter had Spoken of Post-Election Violence], http://bit.ly/11iwwBo.
[63] EFE, "Capriles Critica a Chávez y Dice que 'Gobernar por Twitter' es una 'Burla,'" [Capriles Criticizes Chávez and Says that 'Rule by Twitter' is a 'Mockery'] *Univision Noticias* online, April 22, 2012, http://bit.ly/19ehpWv.
[64] Ezequiel Minyaya, "When Chávez Tweets, Venezuelans Listen," *Wall Street Journal*, April 25, 2012, http://on.wsj.com/KbY2RI
[65] A. Leff, "Does Chávez Govern by Twitter?" Globalpost, May 4, 2012, http://bit.ly/IR4NhO.
[66] El Mundo, "Chávez es el Segundo Político del Mundo Más Influyente en Twitter," [Chávez is the World's Second Most Influential Politician in Twitter] January 3, 2013, http://bit.ly/ZfCh0d.
[67] *Diario El Siglo*, "Una Casa a Para La Seguidora Cuatro Millones de @chavezcandanga," [A Home for Four Millionth Follower @chavezcandanga],*Diario El Siglo* online, February 18, 2013, http://bit.ly/17dcAjI.
[68] Daniel Pabón, "El Vacío Informativo Entrampa a Twitter en Estridentes Rumores" [The Information Vacuum Filled by Rumors from Twitter], *El Carabobeño*, January 9, 2012, http://bit.ly/Xk2pmz.

In light of the government's increased use of social media, members of the public have occasionally complained of the ruling party using state resources and programs to promote a partisan ideology via ICTs. On Christmas Eve 2011, a text message in Chávez's name was sent to more than 27 million mobile phone subscribers, encouraging people to celebrate "our unstoppable march towards a Good and Pretty Country." Although there are no laws restricting such communications, critics complained that forcing mobile phone companies to disseminate partisan propaganda was an abuse of power.[69] In another case, the Canaima Education project, under which the government agreed to supply over two million laptops to elementary school children, came under criticism with allegations that the computers contained content for parents that blatantly promoted Chávez's political ideology.[70]

Manipulation of online content by the ruling party and its supporters has compromised the atmosphere of free online debate of sociopolitical issues. Such careful management of content has included steering conversations along progovernment lines, hacking, discrediting opposition voices via Twitter impersonations, and encouraging self-censorship. In addition to suspicions that paid government commentators have been directing the trajectory of online discussions, allegations have surfaced of the government attempting to influence online news coverage by manipulating the allocation of advertising. Progovernment media have also reported that the government allocates advertising to digital outlets run by figures of the opposition in order to influence the editorial line of critical media.[71]

VIOLATIONS OF USER RIGHTS

In Venezuela, there are many avenues by which bloggers, journalists, and private citizens can be punished for content posted online. The Venezuelan Constitution prohibits anonymity, and vague language in the penal code encourages self-censorship. Despite these provisions, however, government opposition and independent bloggers are active on social media platforms. In 2012 and 2013, such expression was met with increased physical and technical violence extending to harassment, intimidation, detentions, and cyberattacks. Digital impersonations are also on the rise, and have compromised the integrity of a number of websites and digital identities.

Freedom of speech and freedom of the press are constitutionally guaranteed in Venezuela, and a 1999 provision requires the State to provide public access to ICTs.[72] Despite these positive commitments, however, various laws and decrees have been used to undermine online freedom

[69] *Noticiero Digital*, "Telefonicas Asumieron Costo del Mensajito Navideno Presidencial" [Telephone Companies Assume Cost of Presidential Christmas Message], *Noticiero Digital* online, December 28, 2011, http://bit.ly/uGGQQ3; *Devils Excrement* (blog), "Hugo Chávez' Christmas Spam to all Venezuelans," December 27, 2011, http://bit.ly/uAvEkr.
[70] Canaima Educativo, "Venezuela Ensamblará 500 Mil Computadoras Para Proyecto Educativo" [Venezuela Assembles 500,000 Computers for Educational Project], October 4, 2011, http://bit.ly/1azJWck; See also: Ariana Guevara Gomez, "Ideologización: Las "Canaimitas" Fomentan el Culto a la Figura del Líder" [Ideology: The "Canaimitas" Promote the Cult Figure of the Leader], Reportero 24, September 23, 2011, http://bit.ly/nLwDgp.
[71] Aporrea.org, "Miguel Henrique Otero Forrado de Billete Proveniente del Estado, Como Copropietario de Noticias 24" [Miguel Henrique Otero Padded By Ticket of the State, As Part Owner of News 24], November 19 2012, http://bit.ly/S9z6RE.
[72] Asamblea Nacional Constituyente, Constitution [in Spanish], March 24, 2000, 108:110 http://bit.ly/tXiOk.

and to restrict media. When coupled with CANTV's market dominance, the lack of institutional checks and balances in Venezuela makes it possible for the government to monitor and harass political opponents with impunity. Since 2001, the Supreme Court of Justice has passed down no fewer than 10 judgments curbing freedom of expression,[73] evidence of the Court's susceptibility to influence from the executive branch, particularly in regard to cases of political importance. A 2005 reform included significant restrictions on expression, especially in cases involving contempt or disrespect.

The 2001 Special Law against Information Crimes[74] and the 1991 Communications Privacy Protection Law[75] safeguard the privacy, confidentiality, inviolability and secrecy of communications and impose prison terms of up to six years on those who illegally intercept others' communications.[76] In 2012 and early 2013, however, there were numerous incidents of government opponents' communications being hacked, recorded, and manipulated with little response from the authorities on the part of the victims. Information obtained via such privacy breaches has been published in state-run media, indicating possible government involvement.[77]

During its tenure, the Chavez government was highly proactive in its pursuit of greater media control. In December 2010, the National Assembly was due to be replaced with a newly elected chamber containing a substantial opposition presence.[78] In its final days, the outgoing Assembly passed 16 legal decrees that increased regulation of media. The Resorte Law was extended from print to online and electronic media; and the Law of Telecommunications that deemed ICTs to be of public rather than general interest, was amended, rendering ICTs subject to greater state control.[79] The Assembly also delegated its powers to the president for 18 months, granting him the authority to legislate by decree in multiple areas, including ICTs.[80] When freedom of expression advocates demanded to participate in the lawmakers' deliberations, they were harassed and assaulted by government supporters at the doors of the chamber.[81]

The vague language used in the penal code also lays the groundwork for self-censorship both online and offline, criminalizing the dissemination of "false information," with punishments of two to five

[73] Juan Francisco Alonso, "Jueces Buscan Limitar Libre Expresión" [Judges Seek to Limit Free Speech], *El Universal* online, August 21, 2010, http://politica.eluniversal.com/2010/08/21/pol_art_jueces-buscan-limit_2012844.shtml.
[74] The National Assembly, Special Law Against Cybercrime [in Spanish], accessed January 7, 2013, http://bit.ly/gmLBCi.
[75] For the full law on Protection of Communications Privacy, see Biblioteca Susuerte: http://bit.ly/15Ck5Nv.
[76] "Ley sobre Protección a la Privacidad de las Comunicaciones" [Law on Protection of Communications Privacy], see Biblioteca Susuerte: http://bit.ly/15Ck5Nv.
[77] Gregorio Salazar, "Under Chávez: Media Harassed with Online Hacking, Phone Tapping and Censorship," *Sampsonia Way* online, January 23, 2012, http://bit.ly/xZWdVq.
[78] Sara Carolina Díaz, "En 15 Días Asamblea Aprobó 16 Leyes" [In 15 Days, Assembly Passes 16 Laws], *El Universal* online, December 19, 2010, http://www.eluniversal.com/2010/12/19/pol_art_en-15-dias-asamblea_2141341.shtml.
[79] "Ley Organica de Telecomunicaciones," [Organic Law of Telecommunications] Scribd, accessed January 13, 2013, http://www.scribd.com/doc/45293016/Nueva-Ley-Organica-de-Telecomunicaciones.
[80] "Texto de la Ley Habilitante Entregada al la AN" [Text of the Enabling Act Submitted to the National Assembly], *El Universal* online, December 14, 2010, http://www.eluniversal.com/2010/12/14/pol_esp_texto-de-la-ley-habi_14A4853573.shtml.
[81] Juan Francisco Alonso, "Reclaman procesar a agresores de activista de DDHH" [Prosecution Demanded for Aggresors of Human Rights Activist], *El Universal*, December 18, 2010, http://bit.ly/etbhad; See also:*Todos en Red* (blog) "Esperamos Respuesta Oportuna de AN a Documento Por una Internet de Contenido Libre" [Hopes For a Timely Response by AN to a Document for Free Internet Content] December 17, 2010, http://bit.ly/i59ymL.

years in prison.[82] Article 147 of the penal code stipulates that defamation of the president is punishable by 6 to 30 months in prison, while Article 148 stipulates that offenses against lower-ranking officials carry lighter punishments.[83] Given that the internet is classified as a channel of mass distribution of information, some violations of the penal code (such as defamation or incitement of hatred or rebellion) may be considered more severe online than in other media forms.[84]

Detentions of Twitter users and citizen journalists have not been uncommon in past years, however, one particularly notable case made headlines in late 2012 and early 2013. In response to the emergence of anonymous Twitter profiles with supposedly confidential information regarding President Chávez's health, Mario Silva (@LaHojillaTV), a popular pro-government newscaster from state-run VTV, began a campaign to uncover the identities of those responsible for the posts. Silva's investigation resulted in a raid on the house of Federico Medina Ravell, cousin of Alberto Federico Ravell (of pro-opposition news site *La Patilla*).[85] In response to allegations that he had authored posts questioning the president's health (@LucioQuincioC), Venezuelan intelligence officers confiscated several of Federico Medina Ravell's computers and reportedly detained, interrogated, beat, and threatened his family.[86] Following the public prosecutor's allegations that he had "instigated terrorism through social networks,"[87] Ravell was fired by his employer, Mercedes Benz, reportedly under intense pressure from the Chávez regime.[88] Activist groups have interpreted these actions as a clear attempt to curb freedom of expression.[89] Ravell is now seeking political asylum in the United States.[90]

The Venezuelan constitution explicitly prohibits anonymity, a rule that applies to all media.[91] While there are few safeguards in place to limit security agencies' access to user data and private communications, National Assembly deputies from the ruling party have reported complaints from law enforcement agencies that only state-owned Movilnet provides information with immediacy.[92] Despite the provision against anonymity, customers at cybercafes are not required to present

[82] Gaceta Official, "Summary of the National Assembly" [in Spanish], Gaceta Oficial No. 5.763 (March 16, 2005) http://www.tsj.gov.ve/gaceta_ext/marzo/160305/160305-5763-01.html.
[83] *Sumate*, "Respeto a la Libertad de Expresión: ¿Limita el Código Penal la Libertad de Expresión?" [Respect for Freedom of Expression: Does the Penal Code Limit Freedom of Expression?], *Sumate* online, accessed August 22, 2012, http://infovenezuela.org/democracy/cap4_es_2.htm.
[84] Rafael Martínez, "Twitter: Esos Malditos 140 Caracteres" [Twitter: Those Damned 140 Characters], *SoyRafael.com* (blog), February 22, 1010, http://www.analitica.com/va/sociedad/articulos/9309847.asp; See also: Article 285 of the Penal Code.
[85] *La Verdad*, "Sebin Busca a Tuitero que Habla Sobre la Salud del Presidente" [Sebin Searches for Twitterers Talking about the Health of the President], *La Verdad* online, January 7, 2013, http://bit.ly/TGAUUC.
[86] LucioQuincoC, Twitter post, January 8, 2013, https://twitter.com/LucioQuincioC/status/288668104987406337/photo/1.
[87] *La Patilla*, "Fiscalía Investiga Supuesta Instigación al Terrorismo a Través de Twitter" [Prosecutor Investigates Alleged Incitement to Terrorism through Twitter], *La Patilla* online, January 8, 2013, http://bit.ly/ZlPnV8.
[88] "Why Did Mercedes-Benz Fire an Anti-Chávez Political Activist?" *The Commentator*, April 21, 2012, http://bit.ly/IdeVwM.
[89] Care2 Petition Site, "Venezuela, Stop Censorship!" Accessed February 26, 2013, http://bit.ly/13EDHDi.
[90] Raheem Kassam, "Interview: The Man who Chávez Wants Dead," *The Commentator* online, January 9, 2013, http://bit.ly/13gTma7; See also: Chris Miles, "Blogger Federico Medina Ravell has His Home Raided by Intelligence Officials for Spreading Rumors about Chávez," PolicyMic, Januray 2013, http://bit.ly/19eh5qI.
[91] Article 57 establishes freedom of expression and freedom from censorship, but also forbids anonymity. Official site of The Supreme Court: http://www.tsj.gov.ve/legislacion/constitucion1999.htm.
[92] "Presionan a Brindar Información Personal" [Pressed to Provide Personal Information], Blackberry Vzla.com, June 24, 2010, http://www.blackberryvzla.com/2010/06/presionan-brindar-informacion-personal.html.

identification to gain internet access, nor are there any known cases in which cybercafe users' activities have been tracked.

The full scale of surveillance of users' communications applications in Venezuela remains unclear. According to one report, however, Venezuelan security agencies tapped more than one hundred phones over the course of one year, including those of opposition figures Maria Corina Machado, Henrique Capriles, Alberto Ravell, Aixa Lopez, Guillermo Zuloaga and Julio Borges.[93] Given that extralegal wiretapping of phones is common, many Venezuelans suspect that such surveillance extends to the online sphere as well. State representatives have also suggested that the government is capable of tracking down users of Twitter and other social media. In February 2011, when official news agencies were slow to release information about a fire on the premises of the Compania Anonima Venezolana Military Industries (Cavim), details of the incident began to appear on Twitter and other social networks. A military commander subsequently warned that it was "technologically feasible" for the state to track down the origin of those messages and take action against those who had committed the crime of generating public anxiety; no arrests were made at the time, however.[94]

In February 2013, Venezuela's social media tracking campaign experienced renewed vigor after Nestor Reverol, Minister of Interior and Justice, reported that intelligence services would "follow" instigators of an alleged "destabilization plan" seeking to cause panic and chaos among users of social media.[95] Following this announcement, two suspected hackers were arrested for "attempting to undermine the institutional order of Venezuela." The suspects, who were arrested after illegally accessing government webpages and revealing vulnerabilities in the security of state governmental systems, were members of the group Venezuelan Hackers (@ VenezuelanH).[96] In April and May 2013, Venezuelan Hackers published accounts of its recent activities—including infiltrating the websites of Venezuelan State Airline Conviasa, state-owned CANTV, and additional government sites, such as the National Institute of Hygiene—on its Twitter account.[97] The arrests, which were highly publicized, underscored the media tracking campaign and served as a warning to others who might be considering subversive activities online.

In early march, after Chávez's death, Lourdes Alicia Ortega Perez was arrested for "spreading false information" via Twitter. She was released one week later, but is required to make monthly court

[93] Analisis24, "Venezuela: El Ultra Secreto 'CASO 1' que Genero Zozobra en el Gobierno de Hugo Chávez" [The Top Secret "CASE 1" which Generated Anxiety in the Government of Hugo Chávez], Analisis24.com, January 20, 2013, http://bit.ly/WiNbxq.
[94] "Sebin y DIM Investigarán Mensajes de Twitter sobre Caso Cavim," [DIM Investigates Sebin and Twitter Messages about Cavim Case], *Espacio Publico* online, February 2, 2011, http://bit.ly/fcRg6p.
[95] "Reverol: El Cicpc Investiga Mensajes Desestabilizadores en Redes Sociales," [Reverol: The Cicpc Investigates Destabilizing Messages on Social Networks], *El Nacional* online, February 20, 2012, http://bit.ly/13zL8r5; Sebastiana Barraez, "Plan para El Control de La Prensa y La Oposición," [Plan to control the press and opposition], *Código Venezuela*.com, February 15, 2013, http://bit.ly/11LcJdl.
[96] "Sebin Combate Los 'Hackers' que Intentan Vulnerar El Orden Institucional en Venezuela," [Sebin Battles "Hackers" who Try to Undermine The Constitutional Order in Venezuela], *Noticias24* online, February 9, 2013, http://bit.ly/TZwKIS.
[97] "Hackearon la Página Web de Cantv.net" [Website of Cantv.net Hacked], *El Universal* online, April 21, 2013, http://bit.ly/16A8B3a; See also: Apertura Venzuela, "Hackean Página Web de Conviasa" [Conviasa Hacked Website], *El Universal* online, May 12, 2013, http://bit.ly/ZB2xkB.

appearances until further notice.[98] Perez's arrest echoes a spate of cases in 2010, when a number of Twitter users with few followers were arrested for "spreading false information" and "plotting to destabilize the government" under a measure that seems designed to generate self-censorship and fear.[99]

Since 2005, CONATEL has required mobile phone operators to collect copies of their subscribers' identity documents, addresses, fingerprints, and signatures.[100] According to the Computer Crimes Act, this information must be delivered to state security agencies upon presentation of a judicial warrant. Service providers are also obligated to keep detailed logs of all calls, including the phone number and location of both the caller and the recipient. The Law Against Kidnapping and Extortion also necessitates that ICT providers and financial institutions supply data to prosecutors upon presentation of a judicial warrant.

Journalists and online activists have been subject to physical intimidation and attacks in recent years. The offices of civil society group Espacio Publico, which advocates for freedom of expression online, were burglarized twice in November 2011.[101] Although there was no evidence of government responsibility, the authorities' slow investigation, despite the availability of security camera footage, raised suspicions that these were not random acts of violence.[102]

Espacio Publico has repeatedly been the target of defamation campaigns in state-run media. Several days after the second attack, Luis Carlos Díaz, a respected journalist known for teaching cyberactivism workshops throughout the country, began receiving anonymous threats by phone and Twitter.[103] Leonardo León, journalist and press coordinator of Universidad de Los Andes' radio station, and Alonso Moleiro, journalist and Unión Radio announcer, have also been victim to intimidation and threats via Twitter.[104] Moleiro received death threats from another Twitter user after mentioning the severity of President Chávez's illness.[105] In May 2012, the headquarters of *Qué*

---

[98] "Detienen a Tuitera por Generar Rumores Desestabilizadores" [Twitter User Was Arrested for Generating Destabilizing Rumors], *La Patilla* online, March 13, 2013, http://bit.ly/WnBZBY.
[99] Urribarrí, Raisa, "El Año en que Tuiteamos en Peligro" [The Year We Tweeted in Danger], *Periodismo en Línea* online, November 15, 2010. http://periodistasandinos.blogspot.com/2010/11/el-ano-en-que-tuiteamos-en-peligro.html.
[100] Gaceta Oficial No. 38.157, April 1, 2005, http://www.tsj.gov.ve/gaceta/abril/010405/010405-38157-20.html.
[101] Natalia Mazotte, "Back-to-Back Robberies, Slow State Response Suspicious, Says Venezuelan Freedom of Expression NGO," Knight Center for Journalism in the Americas, *Journalism in the Americas* (blog), November 30, 2011, http://bit.ly/JMn5Ln; "Freedom of Expression NGO Robbed," ifex.com, November 23, 2011, http://bit.ly/spu1tb.
[102] Letter from Bernardo Alvarez Herrera, "Venezuela Debe Terminar con la Campana Contra Prestigioso Defensor de Derechos Humanos," [Venezuela Must End the Campaign Against Prestigious Human Rights Defender] Human Rights Watch, August 19, 2010, http://bit.ly/16A7Dnr; Reporters Without Borders, "Authorities Drag Heels in Investigation of Two Burglaries at Offices of Free Speech NGO," IFEX, December 5, 2011 http://www.ifex.org/venezuela/2011/12/05/second_robbery/; "Roban por Segunda Vez Sede de Espacio Publico," [Stolen for a Second Time at the Headquarters of Espacio Publico] *El Universal* online, November 26, 2011, http://bit.ly/rKifHn.
[103] Natalia Mazotte, "Twitter Becoming a Common Way to Threaten Journalists in Venezuela," Knight Center for Journalism in the Americas, *Journalism in the Americas* (blog), November 28, 2011, http://knightcenter.utexas.edu/en/blog/twitter-becoming-common-way-threaten-journalists-venezuela; Natalia Mazotte, "Online Attacks Against Reporters in Venezuela become latest form of censorship (Interview)," Knight Center for Journalism in the Americas, *Journalism in the Americas* (blog), January 18, 2012, http://bit.ly/HTT5gr.
[104] Instituto Prensa y Socieded (Ipys), "Amenazan a Periodista a Través de Twitter" [Journalists Threatened via Twitter], Ipys.com, October 1, 2012, http://www.ipys.org.ve/alerta?id=3005.
[105] Instituto Prensa y Socieded (Ipys), "Venezuelan Journalist Gets Death Threats after Tweeting about Chávez," ifex, December 2012, http://www.ifex.org/venezuela/2012/12/17/moleiro_threats/.

Pasa (What's Up), a digital newspaper critical of the Chávez regime, was attacked with a grenade.[106] The perpetrators are still unknown.

In March 2013, a group of renowned journalists, writers, and humorists, such as Milagros Socorro, Rayma Supriani, Leonardo Padrón, and Laureano Márquez—all of whom had recently been attacked on social networks—began experiencing harassment and threats over their cell phones, via press publications, and on national television programs.[107] Naibet Soto and Luis Carlos Díaz, two bloggers who are well known in the cybersphere for their creation of Google pages dedicated to discussing the political situation in Venezuela, have also suffered harassment by government supporters following Chavez's death.[108]

In recent years, journalists and opposition figures have been subject to periodic waves of hacking and impersonation attacks. In August 2011, the blogs and Twitter accounts of at least two-dozen government critics and other prominent figures were hacked, hijacked, and used to disseminate progovernment messages. Among those targeted in the waves of cyberattacks occurring in late 2011 and 2012 were journalists, artists, economists, activists, and opposition politicians, including the Miranda State governor and presidential candidate Henrique Capriles Radonsky.[109] In some cases, the pro-government nature of the messages was palpable and immediately raised suspicions that a particular account had been compromised. But in other instances, the hackers' approach was more cunning.

Examples included a statement by the usually critical economist Jose Guerra suddenly praising the president's price control policy; supposed criticism by the opposition-linked pollster Luis Vicente Leon regarding one of the opposition's own presidential candidates; and threatening comments towards other users wrongfully attributed to political activist Luis Trincado and journalist Marianela Balbi, Executive Director of the Press and Society Institute of Venezuela. Email accounts associated with activists' Twitter feeds or blogs have also been compromised, and the contents of several blogs have been erased.[110] In February 2013, the Twitter account @radaremergencia and the blog "Radar de los Barrios," both of which belong to Venezuelan journalist Jesús Torrealba, were hacked for the second time. The accounts were commandeered to issue tweets with a strong political bent and to insult Torrealba.[111]

---

[106] Natalia Mazzote, "Periódico Digital Venezolano es Atacado con una Granada," [Digital Venezuelan Newspaper is Attacked with a Grenade], Knight Center, *Journalism in the Americas* (blog), June 6, 2012, http://bit.ly/LjmTJi.

[107] "Continuan las Agresiones a Periodistas" [Attacks on Journalists Continue], *Espacio Público* online, March 19, 2013, http://bit.ly/WJpXnV.

[108] Naibet Parra, "Estado General de Sospecha" [General state of suspicion], *Zaperoqueando* (blog), March 26, 2013. http://zaperoqueando.blogspot.com/2013/03/estado-general-de-sospecha.html.

[109] Adriana Prado, "Pro-Chávez Hackers Steal Twitter Passwords from Venezuelan Journalists," Knight Center for Journalism in the Americas, *Journalism in the Americas* (blog) September 13, 2011, http://bit.ly/qi7g8J; Natalia Mazotte, "More Venezuelan Opposition Journalists' Twitter Accounts Hacked," Knight Center for Journalism in the Americas, *Journalism in the Americas* (blog) February 1, 2011, http://bit.ly/xoOTNS; "Hackean la Página Web de la Gobernación de Miranda" [Web Page of the Government of Miranda Hacked], *La Patilla* online, February 12, 2012, http://bit.ly/yGiaIZ.

[110] "Continuan los Ataques Informaticos en Twitter y Gmail," [Cyber Attacks Continue on Twitter and Gmail], *Espacio Público* online, November 25, 2011, http://bit.ly/uLN8JL.

[111] *Espacio Público* "Hackean La Cuenta @radaremergencia y El Blog Radar de Los Barrios,"[@ radaremergencia Twitter Account and Radar de Los Barrios Blogs Hacked], *Espacio Público* online, February 21, 2013, http://bit.ly/1bRpwiO.

In February 2012, online activists took matters into their own hands in response to the Twitter hackings, launching what they called Operation BAS (short for Operation Block and Spam).[112] Complaints to Twitter resulted in the suspension of several dozen allegedly compromised accounts. Observers noted, however, that accounts belonging to genuine Chávez supporters, not paid commentators, were among those targeted, and that the campaign thus posed a restriction to freedom of expression.[113]

It remains unclear whether the government is directly behind Twitter usurpations and other forms of cyberattack. Although a group of hackers calling itself N33 has taken responsibility for the attacks, some also suspect government involvement.[114] N33, which has been given air time on state-run TV, claims that it supports the president but does not act at the behest of the government. Editor of opposition news site Codigo Venezuela (and recent victim of hacking) Milagros Socorros, however, received an e-mail from an anonymous sympathizer who claimed otherwise. The informant, who claimed to work at the Ministry of Science and Technology, reported that an entire floor of the ministry is devoted to following and hacking opposition activists' online communications. To date, the allegation remains unconfirmed and prosecutors have ignored requests from victims to launch an investigation.[115]

Several web pages of governmental organizations also suffered cyberattacks in 2012 and 2013.[116] Ernesto Villegas, Minister of Communication and Information, denounced the creation of fake accounts on the social network Twitter, one allegedly belonging to him and others created by hackers impersonating president Chávez's daughter, President of the Central Bank Nelson Merentes, and popular progovernment TV star Winston Vallenilla.[117] Villegas called on his followers to block the accounts and report them as spam.[118]

In May 2012, the N33 hacking group named Alberto Federico Ravell, editor of popular news portal La Patilla, as an important future target.[119] A few weeks later, *La Patilla* reported that it had

[112] *6toPoder*, "Operación BAS ha Suspendido un Centenar de Usuarios que Violan las Normas de Twitter" [Operation BAS Has Suspended a Hundred Users who Violate the Rules of Twitter], *6toPoder* online, March 11, 2012, http://bit.ly/AtIKYy.
[113] Luis Carlos Díaz, "El Descubrimiento de la Multitud," [The Discovery of the Crowd] *Periodismo de Paz* (blog), April 3, 2012, http://www.periodismodepaz.org/index.php/2012/03/04/el-descubrimiento-de-la-multitud/.
[114] Laura Vidal, "Venezuela: Government opponents' twitter accounts hacked" *Global Voices Online* (blog), December 5, 2011, http://globalvoicesonline.org/2011/12/06/venezuela-government-opponents-twitter-accounts-hacked/.
[115] Francisco Toro, "Hack a Mole," *International Herald Tribune*, Latitude (blog), November 28, 2011, http://nyti.ms/tUajph.
[116] "Páginas Web de Diversos Organismos Gubernamentales Sufren Ataque Informático" [Websites of Various Government Agencies Suffer Hacking Attacks], *Espacio Público* online, August 28, 2012, http://bit.ly/OtNDb0.
[117] "Villegas Denuncia Cuenta Falsa de Nelson Merentes" [Villegas Denounces False Twitter Account of Nelson Merentes], *Últimas Noticias* online, February 10, 2013, http://bit.ly/15BPtko; "Hackean Cuenta Twitter de Winston Vallenilla con Mensaje Falso Sobre la Salud del Presidente Chávez" [Winston Vallenilla Twitter Account Hacked with False Message about the Health of President Chavez], *Globovisión*, February 13, 2013, http://bit.ly/WnPi4l.
[118] "Ministro Villegas Denuncia Falsa Cuenta suya en Twitter" [Minister Villegas Denounces False Report on his Twitter Account], *Últimas Noticias* online, January 9, 2013, http://bit.ly/1bhtYo8.
[119] Adriana Prado, "Pro-Chávez Hackers Steal Twitter Passwords from Venezuelan Journalists," Knight Center for Journalism in the Americas, September 13, 2011, http://bit.ly/qi7g8J; Juan Carlos Figueroa, "Hacker del n33 Advierte: La Joya de la Corona es Alberto Ravell" [Hacker warns of N33: The jewel in the Crown is Alberto Ravell], *El Tiempo*, September 7, 2011, http://bit.ly/oZIKxe.

successfully fended off an intense cyberattack,[120] however during the October 2012 electoral weekend the site suffered continuous DDoS attacks.[121]

Cyberattacks, impersonations, and blocking all intensified on the day of the presidential election. The Twitter accounts of political activists Ricardo Ríos and Carlos Valero, as well as that of Humberto Prado (director of NGO Observatorio Venezolano de Prisiones), were all compromised on election day, as was the account of Ricardo Koesling, general secretary of political opposition party *Piedra*. The account of well-known singer Oscar De León was also appropriated and used to comment on voting abstention.[122] Problems accessing news sites such as *Noticiero Digital* (Digital News) and Globovisión (which registered a general failure of its servers) were also reported on the day of the election. Weekly newspaper *6to poder* (Sixth Power) reported the blocking of its website by CANTV during the count of electoral votes; Ismael García, a well-known opposition deputy who runs a political show, also noted the disabling of his personal website.[123]

Cyberattacks and blockings also gained vigor surrounding questions of President Chavez's health. After his return to the country in February 2013, a group identifying itself as "Anonymous Venezuela" and demanding to know the truth about the president´s health attacked the websites of several military branches.[124] In early 2013, Venezuelans accused state telecom CANTV of blocking access to *Cuba Diary* and *Apporea* in order to maintain secrecy surrounding the president's health.[125]

Several victims of cyberattacks and digital identity theft have filed complaints with the authorities, yet as of May 2013 state bodies have neither launched an official investigation nor condemned the attacks. The lack of response has led prominent civil society figures to take matters into their own hands, holding a press conference and publishing an open letter denouncing the attacks as part of a government-endorsed policy of "computer terrorism."[126] Among the group's complaints is that although the Committee for Scientific, Penal and Criminal Investigations (CICPC) had successfully identified several perpetrators, the investigation was halted and the lead investigator was relieved of his duties.[127]

Illegal intrusion into computer systems is classified as a criminal offense according to the Special Law Against Cybercrime, which condemns the access, interception, destruction, sabotage, modification, alteration, espionage and disclosure of any private information found in information

---

[120] "La Patilla Informa a Sus Lectores sobre Ataque a Su Plataforma" [La Patilla Informs its Readers about Attack on its Platform], *La Patilla* online, October 1, 2011, http://bit.ly/o8Gd88.
[121] Reference was collected by personal interview with a La Patilla source on condition of anonymity.
[122] "Ataques Informáticos Sacuden las Redes Sociales en el País" [Hacking Shakes Social Networks in the Country], *Espacio Público* online, October 16, 2012, http://bit.ly/15Az8pL.
[123] "Ataques Informáticos Sacuden las Redes Sociales en el País" [Hacking Attacks Shake Social Networks in the Country].
[124] "Hackean Páginas Militares Venezolanas y Exigen Saber qué Pasa con la Salud de Chávez," [Venezuelan Military Websites Hacked; Demands To Know What is Happening with Chavez's Health], *La Patilla* online, February 23, 2013, http://bit.ly/XvxAKr.
[125] *Journalism in the Americas* (blog), "Venezuela's State Telecom Accused of Blocking Access to Site Reporting on Chávez's Health," Accessed February 5, 2013, http://bit.ly/11nCLUb; See also: *Espacio Publico* (blog), http://bit.ly/18zL9kl, and *Harioff* (blog): http://twitter.com/harioff/statuses/303668574671745024.
[126] Liderazgo y Vision Asociacion Civil, "Hackeados e Indiganados Denunciaron el Terrorismo Informatico" [Hackers and Outraged Citizens Denounced Computer Terrorism], December 2, 2011, http://bit.ly/164lnod.
[127] "Denuncian 'Terrorismo Informatico' Impulsado por el Gobierno de Chávez" [Denouncing Computer Terrorism Driven by Chávez Government] *Globovision* online, December 2, 2011, http://www.globovision.com/news.php?nid=210517.

technology systems. Although the law specifies severe punishment for such crimes, extending to imprisonment and fines, no penalties have yet been imposed.[128] Taken together, these circumstances have led many observers to believe that the president or other top officials are either directly or implicitly supporting the attackers.[129]

[128] "Espacio Público Exige al Estado Venezolano que Investigue y Sancione a los Responsables de los Ataques a Cuentas de Correo y Usurpación de Identidad en Redes Sociales," [Espacio Público Demands that the Venezuelan State Investigate and Punish those Responsible for Attacks on Email Accounts and Identity Theft on Social Networks], *Espacio Público* online, February 1, 2012, http://bit.ly/1bRp5F2.

[129] Natalia Mazzote, "Ataques Digitales Contra Periodistas se Convierten en una Nueva Forma de Censura en Venezuela" (Entrevista a Luis Carlos Díaz)" [Digital attacks against journalists become a new form of censorship in Venezuela (Interview with Luis Carlos Díaz)] Knight Center for Journalism in the Americas, January 2012.

VIETNAM

	2012	2013
INTERNET FREEDOM STATUS	NOT FREE	NOT FREE
Obstacles to Access (0-25)	16	14
Limits on Content (0-35)	26	28
Violations of User Rights (0-40)	31	33
Total (0-100)	**73**	**75**

* 0=most free, 100=least free

POPULATION: 89 million
INTERNET PENETRATION 2012: 39 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Vietnam overtook Iran as the world's second worst jailer of netizens after China in 2013, with more than 30 behind bars, according to Reporters Without Borders (see **VIOLATIONS OF USER RIGHTS**).
- A court sentenced blogger Nguyen Van Hai—already jailed since 2008—to another 12 years imprisonment on anti-state charges (see **VIOLATIONS OF USER RIGHTS**).
- Decree 72, passed in July 2013, sought to compel international service providers to comply with government censorship and surveillance (see **LIMITS ON CONTENT**).
- Anti-corruption blogger Le Anh Hung was committed to a mental institution without an exam for 12 days in 2013 (see **VIOLATIONS OF USER RIGHTS**).
- In 2013, propaganda officials acknowledged employing 1000 "public opinion shapers" to manipulate online content (see **LIMITS ON CONTENT**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

Decree 72 governing the management, provision, and use of internet services and information online was pending on April 30, 2013 when the coverage period for this report ended. Prime Minister Nguyen Tan Dung signed the decree on July 15, 2013, which subsequently took effect on September 1. The decree stipulated that all service providers operating in the country—including news websites, social networks, mobile service providers, and game service providers—must have at least one domestic server for the purposes of "inspection, storage, and provision of information at the request of competent authorities." This appears to demand intermediaries to cooperate with any authority in Vietnam conducting censorship or monitoring, though how it might be enforced is not clear; penalties for refusing to comply have not been specified.

Other features of the decree were confusing, including sections that appeared to limit social media platforms from sharing externally-generated content, such as news reports. Vietnamese authorities have tried to ban political commentary from personal websites in the past, with mixed success, and debate on homegrown social networks leans towards non-controversial subjects like entertainment, so this far-reaching interpretation is not outside the realm of possibility. However, some experts noted that this section was geared towards businesses complaining about copyright violations.

The decree maintained other vaguely-worded bans on content "opposing Vietnam." As many internet users know to their cost, however, this is not a dramatic departure from the status quo.

INTRODUCTION

The ruling Vietnamese Communist Party's concern that the internet could be used to challenge its political monopoly has resulted in contradictory policies. While investing in information and communication technologies (ICTs) through programs like its "Taking-Off Strategy 2011–2020,"[1] the government has intensified monitoring and censorship of online content. After a relative easing from 2004 to 2006 while Vietnam hosted an Asia-Pacific Economic Cooperation summit and joined the World Trade Organization, internet freedom deteriorated, and a growing number of online activists face harassment and imprisonment.

Reporters Without Borders counted more than 30 bloggers imprisoned in Vietnam on April 30, 2013, making the country the second worst in the world among nations that jail internet users after China.[2] Many were political activists, and in some cases, it was difficult to assess to what extent their arrests were related to online, as opposed to offline, action and expression. Either way, the number of blogger imprisonments has dramatically increased over the past two years, and penalties are getting heavier. Several recent trials have resulted in sentences longer than a decade.

[1] "'Taking-off Strategy,' Does it Stepping Up the Development of the ICT Industry in Vietnam?" *Business in Asia*, accessed June, 2012, http://www.business-in-asia.com/vietnam/vietnam_ict.html.
[2] Reporters Without Borders, "2013: Netizens Imprisoned," http://bit.ly/Wsi72Y.

While the effects of the oppressive Decree 72 on internet management passed in 2013 are yet to be seen, the decree's drafting process was revealing. No timeframe for passing the decree was made public, and there was no open consultation with civil society, technology companies, or other stakeholders about the many contested provisions. However, both local and international service providers, as well as the international free expression community, objected to the drafts, and the final version contained fewer explicit demands on international service providers than many had feared—a possible sign that the state was willing to compromise to sustain foreign support for the developing ICT sector. Unfortunately, the implications for the Vietnamese people remain grave. The decree's provisions on both content and rights are vague enough to allow free interpretation by a seemingly limitless number of "relevant organizations and individuals." Though it did not impact the coverage period of this report, it bodes ill for internet freedom in the years to come.

OBSTACLES TO ACCESS

Internet penetration slowed in 2012 after years of phenomenal growth fuelled by decreasing costs and improving infrastructure since the internet was introduced in 1997. Some areas reached saturation; others suffered from an economic downturn. Available bandwidth grew a modest 10 percent from 2011 to 2012, after a 250 percent increase between 2010 and 2011, according to official figures.[3] Even so, by the end of 2012, internet penetration was above the global average at 39 percent,[4] and Vietnam ranked 81 on the 2012 International Telecommunication Union's index of ICT development, higher than neighboring countries with larger GDPs like Thailand, Indonesia, and the Philippines.[5]

Vietnam does not report figures for computer literacy, but the 93 percent overall literacy rate has helped equip the adult population to use computers.[6] In large cities, the internet has surpassed newspapers as the most popular source for information.[7] Wi-Fi connections are free in many urban spaces such as airports, cafes, restaurants, and hotels. Cybercafés, though affordable for most urban dwellers,[8] provide access for just 36 percent of internet users, and almost 90 percent of citizens can access the internet in their homes and workplaces, 2012 research shows.[9] While access is more limited for the 70 percent of the population living in rural areas, with ethnic minorities and remote, impoverished communities especially disadvantaged, the research documented a remarkable 95 percent of citizens aged 15 to 24 with internet access nationwide. In a country where 54 percent of the population is under 30 and 75 percent of all internet users are under 35, this is a promising trend.

[3] Vietnam Internet Network Information Center, "Statistics on Internet Development."
[4] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://bit.ly/14IlykM.
[5] International Telecommunication Union, "Measuring the Information Society," 2012, http://bit.ly/QfIEtR.
[6] UNICEF, "At a Glance: Vietnam," accessed July 2013, http://www.unicef.org/infobycountry/vietnam_statistics.html.
[7] "*Tình hình sử dụng Internet tại Việt Nam 2011*" [The Situation of Internet Use in Vietnam in 2011], *VNVIC*, August 3, 2011, http://vnvic.com/tin-tuc-cong-nghe/140-tinh-hinh-su-dung-internet-tai-viet-nam-2011.html.
[8] "*Việt Nam: 20% không tin tưởng thông tin trên Internet*" [Vietnam: 20% Do Not Trust Information on the Internet], *PA News*, April 15, 2010, http://news.pavietnam.vn/archives/1547.
[9] We Are Social, "Social, Digital and Mobile in Vietnam," October 30, 2012, http://bit.ly/Stwb8z.

Mobile phone penetration was almost 150 percent in 2012, indicating that some subscribers have more than one device.[10] Fifty-six percent of users accessed the internet via a mobile device in 2012, almost double the number in 2011.[11] A third-generation (3G) network, which enables internet access via mobile phones, has been operating since the end of 2009, and the number of users is slowly expanding. By the first quarter of 2012, 3G users were estimated to account for 11 percent of the overall market.[12]

The three biggest internet service providers (ISPs) are the state-owned Vietnam Post and Telecommunications (VNPT), which dominates 63 percent of the market; the military-owned Viettel (9 percent), and the privately owned FPT (22 percent).[13] VNPT and Viettel also own the three largest mobile phone service providers in the country (MobiFone, VinaPhone, and Viettel), which serve 93 percent of the country's subscriber base, while three privately owned companies share the remainder.[14] While there is no legally-imposed monopoly for access providers, informal barriers still prevent new companies without political ties or economic clout from entering the market. Similarly, there is a concentration of internet-exchange providers, which serve as gateways to the international internet: Four out of six are state or military-owned.[15]

The Vietnam Internet Center (VNNIC) allocates internet resources, such as domain names, under the Ministry of Information and Telecommunication. Three additional ministries—information and culture (MIC), public security (MPS), and culture, sport, and tourism (MCST)—manage the provision and usage of internet services. On paper, the MCST regulates sexually explicit and violent content, while the MPS oversees political censorship. In practice, however, all such guidelines are issued to relevant bodies by the ruling Vietnamese Communist Party in a largely nontransparent manner. In 2008, the MIC created the Administrative Agency for Radio, Television, and Electronic Information. Among other duties, the agency is tasked with regulating online content, which includes drafting guidelines for blogs and managing licenses for online media.[16]

LIMITS ON CONTENT

The impact of the 2013 internet management decree, which introduced vaguely-worded content restrictions and sought to increase companies' liability for implementing them, has yet to be seen. While its implications are potentially far-reaching, however, it was just the latest in a series of decrees that heavily restrict political commentary and instill self-censorship in an otherwise diverse

[10] International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2012;" Vietnam Post and Telecom Hanoi, "*Việt Nam đã có 136 triệu thuê bao di động*," [Vietnam Has 136 Million Mobile Phone Subscribers], July 2, 2013, http://www.vnpt-hanoi.com.vn/web/tintuc_chitiet.asp?news_id=5109.
[11] Thankiu, "Cimigo Net Citizens Report 2012," http://bit.ly/164vsBv.
[12] GSMA Intelligence, "3G growth stalls in Vietnam", April 2012, http://bit.ly/1azUNmE.
[13] "*Thị trường Internet cũng sẽ có những vụ sát nhập?*" [Will the Internet Market see Mergers?], *ICTNews*, September 21, 2012, http://ictnews.vn/home/Internet/77/Thi-truong%C2%A0Internet-cung-se-co-nhung-vu-sap-nhap/105064/index.ict.
[14] GSMA Intelligence, "3G growth stalls in Vietnam."
[15] The four are: VNPT, Viettel, Hanoi Telecom, and VTC.
[16] Geoffrey Cain, "Bloggers the New Rebels in Vietnam," *SFGate*, December 14, 2008, http://bit.ly/1bhBy1W.

and lively blogging community. What's more, while content limits are nothing new in Vietnam, online content was increasingly subject to manipulation in the past year, and officials acknowledged paying commentators for the first time, a sign that information authorities are diversifying their tactics for controlling popular discourse.

While the Vietnamese government has fewer resources to devote to online content control than its counterpart in China, the authorities have nonetheless established an effective and increasingly sophisticated content-filtering system. Censorship is implemented by ISPs rather than at the backbone or international gateway level. No real-time filtering based on keywords or deep-packet inspection has been documented. Instead, specific URLs are identified in advance as targets for censorship and placed on blacklists; ISPs are legally required to block them or lose their license. Some users report being notified that a censored site has been deliberately blocked, while others receive a vague error message saying the browser was unable to locate the website's server.

Censorship ostensibly limits sexually explicit content. In practice, however, it primarily targets topics with the potential to threaten the VCP's political power, including political dissent, human rights and democracy. Websites criticizing the government's reaction to border and sea disputes between China and Vietnam are subject to blocking. Content promoting organized Buddhism, Roman Catholicism, and the Cao Dai religious group is blocked to a lesser but still significant degree.[17] Vietnamese sites critical of the government are generally inaccessible, whether they are hosted overseas, such as *Talawas*, *Dan Luan*, and *Dan Chim Viet*, or domestically, like *Dan Lam Bao* and *Anh Ba Sam*.

Censors largely focus on Vietnamese-language content, so the *New York Times* and Human Rights Watch websites are accessible, while the U.S.-funded Radio Free Asia's Vietnamese-language site is not; BBC websites are accessible in English but not Vietnamese. Blocking is not consistent across ISPs. A 2012 OpenNet Initiative test of 1,446 sites found Viettel blocked 160 URLs, while FPT blocked 121, and VNPT only 77.[18] There is no avenue for managers of blocked websites to appeal censorship decisions.

The unpredictable and nontransparent ways in which topics become forbidden make it difficult for users to know where exactly the "red lines" lie, and many self-censor. Bloggers and forum administrators commonly disable commenting functions to prevent controversial discussions.

Online media outlets and internet portals are state-owned and subject to VCP censorship. The party's Department for Culture and Ideology and the MPS regularly instruct online newspapers or portals to remove content they perceive as critical of the government. Editors and journalists who post such content risk disciplinary warnings, job loss, or imprisonment.

---

[17] "Vietnamese Government Expands Internet Censorship to Block Catholic Websites," Catholic News Agency, August 6, 2009, http://bit.ly/15BVkX4.

[18] OpenNet Initiative, "Update on Threats to Freedom of Expression Online in Vietnam", September 10, 2012, http://opennet.net/blog/2012/09/update-threats-freedom-expression-online-vietnam.

Since 2008, a series of regulations have extended controls on traditional media content to the online sphere. In December of that year, the state passed Decree 97 and MIC Circular 7 ordering blogs to refrain from political or social commentary and barred internet users from disseminating press articles, literary works, or other publications prohibited by the Press Law.[19] Blogging platforms were instructed to remove this "harmful" content, report to the government every six months, and provide information about individual bloggers upon request.[20] Censorship of anti-government content increased, though blogs hosted overseas were unaffected. A decree followed in 2011, giving authorities power to penalize journalists and bloggers for a series of ill-defined infractions, including publishing under a pseudonym. The decree differentiated sharply between journalists accredited by the government and independent bloggers, who are allowed far fewer rights and protections.[21]

The Decree on the Management, Provision, Use of Internet Services and Internet Content Online, introduced by the MIC in May 2012 and passed just over a year later, extends this repressive trajectory by further regulating domestic internet use and replacing "blogs" with a broader definition of "social networks" to encompassing a range of online platforms.[22] Article 5 limited overbroad categories of online activity including "opposing the Socialist Republic of Vietnam," inciting violence, revealing state secrets, and providing false information.

The decree sought to force intermediaries—including those based overseas—to regulate third-party contributors in cooperation with the state. Vietnamese authorities have acknowledged this goal in the past. The deputy minister of information and communications said he would request Google and Yahoo cooperate with censors as early as 2008;[23] yet the new decree asks all social network operators to "eliminate or prevent information" prohibited under Article 5. It also mandated that companies maintain at least one domestic server "serving the inspection, storage, and provision of information at the request of competent authorities." Social networks were further instructed to "provide personal information of the users related to terrorism, crimes, and violations of law" on request. It did not outline what penalties non-compliant companies could face, and how the decree might be enforced remains unclear. It came into effect after the coverage period of this report.

---

[19] OpenNet Initiative, "Vietnam," August 7, 2012, https://opennet.net/research/profiles/vietnam; The Government, "Decree No 97/2008/ND-CP of August 28, 2008," *Official Gazette* 11-12, August 2008, http://english.mic.gov.vn/vbqppl/Lists/Vn%20bn%20QPPL/Attachments/6159/31236373.PDF; Ministry of Information and Communications, "Circular No. 07/2008/TT-BTTTT of December 18, 2008," *Official Gazette* 6-7, January 2009, http://english.mic.gov.vn/vbqppl/Lists/Vn%20bn%20QPPL/Attachments/6145/23434370.pdf.

[20] Karin Deutsch Karlekar, ed., "Vietnam," *Freedom of the Press 2009* (New York: Freedom House, 2009).

[21] Article 19, "Comment on the Decree No. 02 of 2011 on Administrative Responsibility for Press and Publication Activities of the Prime Minister of the Socialist Republic of Vietnam," June 2011, http://www.article19.org/data/files/pdfs/analysis/comment-on-the-decree-no.-02-of-2011-on-administrative-responsibility-for-pr.pdf; "Decree 02/2011/ND-CP" [in Vietnamese], January 6, 2011, available at Committee to Protect Journalists, http://cpj.org/Vietnam%20media%20decree.pdf.

[22] "Decree No. 72/2013/ND-CP, dated July 15, 2013 of the Government on Management, Provision and Use of Internet Services and Online Information," Luật Minh Khuê, http://luatminhkhue.vn/copyright/decree-no-72-2013-nd-cp.aspx.

[23] Ann Binlot, "Vietnam's Bloggers Face Government Crackdown," *Time*, December 30, 2008, http://www.time.com/time/world/article/0,8599,1869130,00.html.

Tools for circumventing censorship, such as proxy servers, are relatively well-known among younger, technology-savvy internet users in Vietnam, and many can be found with a simple Google search. The authorities are not known to have instituted restrictions on content transmitted via e-mail or mobile phone text messages.

Besides expanding censorship, the government has adopted new measures to manipulate public opinion online, acknowledging their deployment of up to 1000 "public opinion shapers" to produce and spread progovernment content in early 2013.[24] Hanoi's Propaganda and Education Department revealed that it runs at least 400 online accounts—what kind was not specified—and 20 microblogs to fight "online hostile forces," according to international news reports. Also in 2012, some blogs, such as *Quan Lam Nao*, established themselves as populist voices criticizing high-profile members of the party. Their critics counter that these platforms reflect the party's internal power struggles and are not objective measures of increasing freedom online.

Despite government restrictions, Vietnam's internet is vibrant and offers a diversity of content in the Vietnamese language. The Vietnamese blogosphere started around 2006 with Yahoo! 360 attracting about 15 million Vietnamese users at the height of its popularity.[25] Since Yahoo terminated the service in mid-2009, some stayed with its replacement 360Plus, while others migrated to Blogger, WordPress, or local networks such as YuMe, which are popular for entertainment content.

YouTube, Twitter, and international blog-hosting services are freely available and growing in popularity. Facebook, which faced sporadic—and officially unacknowledged—blocks in 2010 and 2011, was generally accessible on all types of devices in early 2013. Users of the service surged from 4 million in 2011 to 8.5 million by Oct 2012, overtaking local competitor Zing—with 8.2 million subscribers—as the top social network in Vietnam.[26] In 2010, the MIC launched a government-backed social network called Go.VN, which requires users to register with their real name and government-issued identity number when creating an account. The initial response to the new initiative was limited.[27] By early 2013, Go.VN had morphed into a mere entertainment portal.

Although most blogs address personal and nonpolitical topics, citizen journalism has emerged as an important source of information for many Vietnamese, particularly given the tightly controlled traditional media. People now recognize the parallel existence of official media and alternative counterparts operating exclusively online. Websites such as *Anh Ba Sam*, *Que Choa* or *Bauxite Vietnam* react quickly to socio-political events and have established themselves as influential opinion makers that were influential in mobilizing demonstrations on the streets of Hanoi and Ho Chi Minh City to protest China's claim on the Paracel and Spratly Islands in 2011; the protests lasted several months

[24] "Vietnam Admits Deploying Bloggers to Support the Government", BBC, January 11, 2013, http://www.bbc.co.uk/news/world-asia-20982985.
[25] Aryeh Sternberg, "Vietnam Online: Then and Now," *iMedia Connection*, January 5, 2010, http://www.imediaconnection.com/content/25480.asp.
[26] We Are Social, "Social, Digital and Mobile in Vietnam."
[27] James Hookway, "In Vietnam, State 'Friends' You," *Wall Street Journal*, October 4, 2010, http://online.wsj.com/article/SB10001424052748703305004575503561540612900.html.

before the authorities shut them down and sent one of the organizers to an education camp.[28] In 2012, blogs played an important role in rallying public opinion and providing evidence against the local government of some provinces such as Hai Phong and Hung Yen, after local authorities controversially seized agricultural land from farmers, whose violent resistance shocked the country.[29]

VIOLATIONS OF USER RIGHTS

Over the last five years, Vietnam has subjected bloggers and online writers to extended interrogations, imprisonment, and physical abuse, a repressive trend that intensified in 2012 and 2013. Vietnam was the world's second biggest prison for netizens after China in 2013, with more than 30 bloggers and cyber-dissidents detained, according to Reporters Without Borders. Sentences handed down in cursory trials, which are often closed to the press, are getting longer. Blogger Nguyen Van Hai, already jailed since 2008, was sentenced to an additional 12 years in prison on anti-state charges in 2012, while at least three activists—who may have come to police attention in part because of their online activity—were sentenced to 13 years each.

The constitution affirms the right to freedom of expression, but in practice, the VCP has strict control over the media. Legislation, including internet-related decrees, the penal code, the Publishing Law, and the State Secrets Protection Ordinance, can be used to imprison journalists and bloggers. The penal code's notorious Articles 79 and 88 are commonly used to prosecute and imprison bloggers and online activists for subversion and propaganda against the state.[30] The judiciary is not independent but follows the party's command, especially in trials related to free expression, which often last only a few hours. When detaining bloggers and online activists, the police routinely flout due process, arresting individuals without a warrant or retaining them in custody beyond the maximum period allowed by law.

Reporters Without Borders counted 32 netizens imprisoned in Vietnam as of April 30, 2013, a figure which climbed to 35 in June.[31] The same group had documented 17 bloggers jailed in mid-2011. This significant jump—which took Vietnam past Iran's mid-2013 total of 25 bloggers behind bars—was fuelled by a January 2013 court ruling that found 14 Catholic students, bloggers, and human rights activists guilty of subversion under Article 79. The activists, who were mostly in their twenties and thirties, had been arrested after returning from training in Bangkok on non-violent struggle organized by the U.S.-based anti-communist party Viet Tan in 2011. At least five were regular contributors to the Catholic website *Vietnam Redemptorist News;*[32] other online activity was

[28] "*Người biểu tình Thu Hằng bị đưa vào trại*" [Demonstrator Thu Hang Sent to Camp], BBC Vietnamese, December 9, 2011, http://www.bbc.co.uk/vietnamese/vietnam/2011/12/111209_bui_hang_arrested.shtml.
[29] Stuart Grudgings, "Web Snares Vietnam as Bloggers Spread Protests Over Land," Reuters, August 19, 2013, http://www.reuters.com/article/2012/08/19/us-vietnam-bloggers-idUSBRE87I09I20120819.
[30] Reporters Without Borders, "Internet Enemies: Vietnam."
[31] Reporters Without Borders, "2013: Netizens Imprisoned," http://en.rsf.org/press-freedom-barometer-netizens-imprisoned.html?annee=2013.
[32] Committee to Protect Journalists, "Bloggers imprisoned in mass sentencing in Vietnam," news alert, January 9, 2013, http://www.cpj.org/2013/01/bloggers-imprisoned-in-mass-sentencing-in-vietnam.php.

less well-documented, but may well have contributed to the charges against the group, which included participating in "propaganda against the Socialist Republic of Vietnam."[33] The shortest sentence given was 3 years prison followed by 2 years house arrest, while at least three were jailed for 13 years with 3 years house arrest.[34]

Arrests continued to be reported during the coverage period. In October 2012, police detained two students, Nguyen Phuong Uyen, 21, and Dinh Nguyen Kha, 25, for disseminating anti-governmental materials in public places and online; they were jailed for 6 and 10 years respectively in May 2013.[35] Respected lawyer and blogger Le Quoc Quan was also arrested in December 2012, shortly after the BBC Vietnamese service published one of his articles on its website; his trial remains pending.[36]

The longest-serving blogger in prison in 2013 was Nguyen Van Hai, a vocal critic of the government's human rights record and an advocate for Vietnamese sovereignty over the Spratly Islands, also known by the title of his blog, Dieu Cay. He was sentenced in late 2008 to two and a half years in prison on tax evasion charges that observers viewed as politically motivated.[37] After completing that term, authorities kept him in detention until September 2012,[38] when a new trial court sentenced him to an additional 12 years in prison and 5 years under house arrest for "activities against the government."[39] Two others were sentenced at the same trial: Phan Thanh Hai, who blogged as Anh Ba Sai Gon and was arrested in late 2010 on the charge of distributing false information on his website, was sentenced to three years, while Ta Phong Tan, a former female police officer turned social justice blogger arrested in September 2011 for blog posts that allegedly "denigrated the state," was jailed for ten.[40] Ta Phong Tan's mother committed suicide by setting herself on fire outside of the local People's Committee building to protest against her daughter's trial. Others serving long term sentences in 2013 include one of Vietnam's most vocal online dissidents, Cu Ha Huy Vu, who is serving a sentence of seven years in prison and three years house arrest handed down in a 2011 trial that barred access to the public and media.[41]

In addition to imprisonment, bloggers and online activists have been subjected to physical attacks, job loss, termination of personal internet services, travel restrictions, and other violations of their

[33] Seth Mydans, "Activists Convicted in Vietnam Crackdown on Dissent," *New York Times,* January 9, 2013, http://www.nytimes.com/2013/01/10/world/asia/activists-convicted-in-vietnam-crackdown-on-dissent.html?_r=0.
[34] "Long Prison Terms For "Dissident" Vietnam Bloggers," *Global Voices Online*, January 12, 2013, http://globalvoicesonline.org/2013/01/12/long-prison-terms-for-dissident-vietnam-bloggers/.
[35] "*Nguyễn Phương Uyên bị phạt 6 năm tù, Đinh Nguyên Kha 10 năm tù*" [Nguyen Phuong Uyen Sentenced to 6 Years, Dinh Nguyen Kha to 10 Years Prison], *Thanh Nien*, May 16, 2013, http://www.thanhnien.com.vn/pages/20130516/nguyen-phuong-uyen-bi-phat-6-nam-tu-dinh-nguyen-kha-10-nam-tu.aspx.
[36] Human Rights Watch, "Vietnam: Drop Charges Against Le Quoc Quan," July 8, 2013, http://www.hrw.org/news/2013/07/07/vietnam-drop-charges-against-le-quoc-quan.
[37] Human Rights Watch, "Banned, Censored, Harassed and Jailed," news release, October 11, 2009, http://www.hrw.org/en/news/2009/10/11/banned-censored-harassed-and-jailed.
[38] Committee to Protect Journalists, "2012 Prison Census: Vietnam," accessed May, 2013, http://cpj.org/imprisoned/2012.php.
[39] "*Y án với Điếu Cày và Tạ Phong Tần*" [Sentences uphold for Dieu Cay and Ta Phong Tan], BBC Vietnamese, December 28, 2012, www.bbc.co.uk/vietnamese/vietnam/2012/12/121228_xu_khang_an_dieu_cay.shtml+&cd=10&hl=vi&ct=clnk&gl=vn.
[40] "An Odd Online Relationship," *Economist* (Blog), August 9, 2012, http://www.economist.com/blogs/banyan/2012/08/internet-freedom-vietnam.
[41] Reporters Without Borders, "Prime Minister Urged to Free All Imprisoned Bloggers and Journalists," September 1, 2011, http://en.rsf.org/vietnam-prime-minister-urged-to-free-all-01-09-2011,40879.html.

rights. Blogger Nguyen Hoang Vi reported that the police forcibly stripped and sexually assaulted her after she tried to attend Dieu Cay and his co-defendants' December 2012 appeal hearing.[42] In February, Le Anh Hung, whose blog accused high-ranking Vietnamese leaders of corruption, was detained in a mental institution for 12 days, without a medical examination.[43]

Vietnamese authorities monitor online communications and dissident activity on the web and in real time. Cybercafé owners are required to install special software to track and store information about their clients' online activities,[44] and the 2013 internet management decree holds cybercafé owners responsible if their customers are caught surfing "bad" websites.[45] Citizens must also provide ISPs with government-issued documents when purchasing a home internet connection. In late 2009, the MIC announced that all prepaid mobile phone subscribers would be required to register their ID details with the operator, and individuals are allowed to register only up to three numbers per carrier.[46] As of early 2013, however, the registration process is not linked to any central database and could be easily circumvented using fake ID numbers.[47] Real-name registration is not required to blog or post online comments, and many Vietnamese do so anonymously.

Decree 72 may change that, and its privacy implications attracted concern throughout the year before it took effect. As outlined above, all providers and social networks in particular, are ordered to provide user information to "competent authorities" on request, but with no real procedures or oversight to discourage intrusive registration or data collection.[48] Users themselves were given the ambiguous right to "have their personal information kept confidential in accordance with law." Other sections gestured in the direction of improved information security by encouraging providers of online information to "deploy technical systems and techniques." Unfortunately, implementation of these nebulous provisions is left to the discretion of "ministers, heads of ministerial agencies, heads of governmental agencies, the presidents of people's committees of central-affiliated cities and provinces, relevant organizations and individuals" under the guidance of the minister of information and communications, leaving anonymous and private communication subject to invasion from almost any authority in Vietnam in the coming years.

Blogger harassment has coincided with systematic cyberattacks targeting individual blogs as well as websites run by other activists in Vietnam and abroad that were first documented in September 2009.[49] The worst of these occurred in 2010 and involved dozens of sites, including those operated

---

[42] Nguyen Hoang Vi, "What happened on the day of the Appeal Hearing for the members of The Free Journalist Network," *Dan Lam Bao*, January 2013, http://danlambaovn.blogspot.com/2013/01/what-happened-on-day-of-appeal-hearing.html#.UgEGCJK1EwD.

[43] "*Blogger Le Anh Hung duoc tha ve nha*" [Blogger Le Anh Hung released], BBC Vietnamese, February 5, 2013, www.bbc.co.uk/vietnamese/vietnam/2013/02/130205_leanhhung_released.shtml+&cd=2&hl=vi&ct=clnk&gl=vn.

[44] "Internet Censorship Tightening in Vietnam," *Asia News*, June 22, 2010, http://www.asianews.it/news-en/Internet-censorship-tightening-in-Vietnam-18746.html.

[45] OpenNet Initiative, "Update on Threats."

[46] Phong Quan, "Sim Card Registration Now Required in Vietnam," Vietnam Talking Points, January 16, 2010, http://talk.onevietnam.org/sim-card-registration-now-required-in-vietnam/

[47] "*Quản lý thuê bao di động trả trước: Chuyện không dễ*," [Managing Prepaid Mobile Subscribers Isn't Easy], *Vinhphuc*, January 14, 2013, http://www.vinhphuc.vn/ct/cms/Convert/thihanhpl/Lists/tintuc/View_Detail.aspx?ItemID=10.

[48] "Decree No. 72/2013/ND-CP."

[49] Human Rights Watch, "Vietnam: Stop Cyber Attacks Against Online Critics," news release, May 26, 2010, http://www.hrw.org/news/2010/05/26/vietnam-stop-cyber-attacks-against-online-critics.

by Catholics who criticize government confiscation of church property, forums featuring political discussions, and a website raising environmental concerns about bauxite mining.[50] The attackers infected computers with malicious software disguised as a popular keyboard program allowing Microsoft Windows to support the Vietnamese language. Once infected, computers became part of a "botnet," or network whose command-and-control servers were primarily accessed from internet protocol (IP) addresses inside Vietnam. Hackers manipulated that network to carry out denial-of-service (DoS) attacks, according to independent investigations by the internet security firm McAfee and Google. Google's report estimated that "potentially tens of thousands of computers" were affected, most belonging to Vietnamese speakers.[51] McAfee stated that "the perpetrators may have political motivations, and may have some allegiance to the government of the Socialist Republic of Vietnam."[52] The Vietnamese authorities—who have proudly advertised their ability to destroy "'bad' websites and blogs"[53]—took no steps to find or punish the attackers.

In 2012 and 2013, hackers continued to target a handful important alternative blogs, including *Anh Ba Sam* and *Que Choa*.[54] It is now common practice for sites to post a list of alternative URLs in case the current one is hacked.

[50] "Authorities Crush Online Dissent; Activists Detained Incommunicado," *Free News Free Speech* (blog), June 2, 2010, http://freenewsfreespeech.blogspot.com/2010/06/authorities-crush-online-dissent.html.
[51] George Kurtz, "Vietnamese Speakers Targeted in Cyberattack," *CTO* (Blog), March 30, 2010, http://siblog.mcafee.com/cto/vietnamese-speakers-targeted-in-cyberattack/; Neel Mehta, "The Chilling Effect of Malware," *Google Online Security Blog*, March 30, 2010, http://googleonlinesecurity.blogspot.com/2010/03/chilling-effects-of-malware.html.
[52] Kurtz, "Vietnamese Speakers Targeted in Cyberattack."
[53] Human Rights Watch, "Vietnam: Stop Cyber Attacks Against Online Critics."
[54] David Brown, "Mysterious Attack on a Vietnamese Blog," *Asia Sentinel*, March 18, 2013, http://asiasentinel.com/index.php?option=com_content&task=view&id=5257&Itemid=188.

ZIMBABWE

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	17	16
Limits on Content (0-35)	14	14
Violations of User Rights (0-40)	23	24
Total (0-100)	**54**	**54**

* 0=most free, 100=least free

POPULATION: 12.6 million
INTERNET PENETRATION 2012: 17 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- There were no reports of internet content being blocked or filtered during the coverage period, though various ruling party officials publicly expressed the desire to increase control over ICTs, particularly in the lead-up to the July 2013 general elections (see **LIMITS ON CONTENT**).
- An anonymous Facebook user with the pseudonym "Baba Jukwa" became a social media sensation for his posts exposing supposed secrets from within the ZANU-PF ruling party, in addition to his naming and shaming campaign against corrupt party officials (see **LIMITS ON CONTENT**).
- Two mobile phone users were arrested for allegedly sending text messages that insulted the president (see **VIOLATIONS OF USER RIGHTS**).
- An investigative report in early 2013 uncovered evidence of a "massive" cyber training program for Zimbabwean security agents facilitated by Iranian intelligence organizations (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

Zimbabwe's 2013 internet freedom status reflects developments in the country from May 1, 2012 to April 31, 2013, which are covered in this report. However, the July 2013 general elections entailed a number of events that directly impacted the country's internet freedom landscape.

The 2013 political contestations in Zimbabwe were likely the most internet-fueled elections to date, as various parties took to social media to campaign and promote their platforms in advance of the general elections that occurred on July 31, 2013. All major political parties had a presence on Facebook and Twitter,[1] and leading political figures used the internet to engage with citizens both in Zimbabwe and the diaspora on a daily basis. Social media was also widely used to encourage citizens to vote and counter electoral corruption, among other issues, while numerous websites were launched to monitor election irregularities[2]

At the time of writing in August 2013, there were no reports of internet content being blocked, or of online users arrested for their activities related to the elections, though the sensational popularity of the anonymous Facebook user, Baba Jukwa, elicited a desire by the ruling party to crackdown against individuals using social media to express criticism against the government (see "Limits on Content").[3]

Despite the lack of internet censorship, in the week leading up to the July 31 elections, the telecommunications regulator POTRAZ reportedly issued a directive to the private mobile phone provider, Econet, to block the dissemination of bulk SMS messages sent through its international gateway.[4] Meanwhile, the independent community radio station, Radio Dialogue, reported frequent internet disconnections in its office, and internet café owners reported slow internet connectivity.[5] While the government's hand behind the disruptions could not be confirmed, state control over two of the country's five international gateways, as well as the state's ability to issue directives to private telecom providers, increase the likelihood of deliberate government interference.

INTRODUCTION

Zimbabwe has witnessed an upsurge in internet use, and despite the country's recent history of political instability and economic volatility, the past two years have seen a sizeable investment in the ICT sector, which had largely been stagnant over the previous decade. In 2012 and early 2013, access to ICTs remained nominally free from direct government interference with the exception of

[1] Free & Fair Zimbabwe Election's Facebook page, accessed August 1, 2013, http://www.facebook.com/zimbabweelection?hc_location=stream.
[2] "In Heavy Zimbabwe Voting, No Repeat of Disastrous 2008 Events," *New York Times*, July 31, 2013, http://nyti.ms/1aFwwvn.
[3] Cris Chinaka, "Cat-and-Mouse in Zimbabwe's Election Cyber War," Reuters, July 26, 2013, http://www.reuters.com/article/2013/07/26/us-zimbabwe-elections-internet-idUSBRE96P0SU20130726.
[4] Brandon Gregory, "Zimbabwe Authorities Block Award Winning SMS Service for 'Political Reasons,'" *Humanipo*, July 30, 2013, http://www.humanipo.com/news/7611/Zimbabwe-authorities-block-award-winning-SMS-service-for-political-reasons/.
[5] George Mpofu and Nicolette Zulu, "FFZE: Zim Internet, Phones 'Jammed' Day Ahead of Vote," Free & Fair Zimbabwe Election, July 30, 2013, http://zimbabweelection.com/2013/07/30/ffze-zim-internet-phones-jammed-day-ahead-of-vote/.

the July 2013 elections period, though the relative openness is more likely due to a lack of resources to affect control than a lack of intention.

As Zimbabwe's internet community, both local and in the diaspora, has become more assertive in discussing socioeconomic and political issues online, the Zimbabwean African National Union–Patriotic Front (ZANU-PF) ruling party under President Robert Mugabe has become increasingly concerned about the internet's ability to mobilize political opposition, particularly the Movement for Democratic Change (MDC) under Morgan Tsvangirai. Accordingly, ZANU-PF officials made several public demands to stop what it calls the "abuse" of information and communication technologies (ICTs) in 2012.[6] Meanwhile, two citizens were arrested in the past year for sending text messages on their mobile phones that allegedly insulted the president.

Zimbabwe's new constitution was enacted in May 2013, giving freedom of expression a boost both on and offline through its provisions on freedom of the press, access to government information, as well as protection for sources of information. Such guarantees, however, are likely to be nominal, given the ruling party's trend of taking extralegal actions against Zimbabwean citizens. Further, state security officials continue to have the authority to monitor and intercept ICT communications at will, and an investigative report revealed in early 2013 that Zimbabwean security agencies have been receiving cyber training assistance from Iranian intelligence organizations since 2007.

OBSTACLES TO ACCESS

Internet access has continued to expand in Zimbabwe, growing from a penetration rate of nearly 16 percent in 2011 to over 17 percent in 2012, according to the International Telecommunications Union (ITU).[7] This figure, however, may not reflect the growing number of users who are accessing the web on their mobile devices. Research from June 2012 indicated that about 70 percent of Zimbabwean internet users are logging online via mobile phones,[8] which likely accounts for the rapid spike in mobile phone penetration from 72 percent in 2011 to nearly 97 percent in 2012.[9]

Similar to most countries in Africa, Zimbabwe benefits from low-cost, internet-enabled imitation mobile phones from Asia. Internet access on mobile phones has been further facilitated by the introduction of 3G, 4G and EDGE technology in the past few years.[10] The decreasing price of mobile internet access—which dropped from $1.50 per megabyte (MB) in 2011 to $1 per MB as of May 2013—has also facilitated increased access. Subscription fees for 3G services have gone down

[6] Everson Mushava, "Technology a Security Threat: Sekeremayi," *Newsday*, May 9, 2013, http://www.newsday.co.zw/2013/05/09/technology-a-security-threat/.
[7] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[8] Brian Gondo, "Insights into Zim Internet Usage," *Techzim*, June 12, 2012, http://www.techzim.co.zw/2012/06/insights-into-zim-internet-usage/.
[9] International Telecommunication Union,"Mobile-Cellular Telephone Subscriptions, 2000-2012."
[10] EDGE is a faster version of the globally used GSM mobile standard.

to $30 per month for 10 GB, and other services providers are offering 3G services on a pay-as-you-go basis for as little as $0.10 per MB.

While mobile access to the internet has become increasingly affordable, fixed-line internet subscriptions cost $30-$40 per month (including installation fees) and remain expensive for many Zimbabweans who earn an average monthly wage of approximately $180.[11] Nevertheless, market competition among service providers is slowly bringing down prices. For example, the cost of wireless 3G modems has decreased from $60 to $30 and is accessible on prepaid wireless access devices. Computer prices have also declined from an average of $600 in 2011 to between $350 and $450 in 2012.

Although competition has decreased the cost of broadband internet access, effective broadband for home and individual users has not been realized due to the poor infrastructure of the state-owned fixed-line operator, TelOne. Nonetheless, both the public and private sectors have invested in expanding coverage to other parts of the country. Presenting the 2013 budget in late 2012, Finance Minister Tendai Biti stated that $26 million had been spent on Zimbabwe's fiber-optic cable system since 2009, which included the Harare-Bulawayo fiber-optic link that was completed in 2012.[12] TelOne was also connected to Namibia Telcom's fiber cable near the border towns of Victoria Falls and Katima Mulilo in 2012. Meanwhile, other licensed data carriers are continually rolling out fiber-optic networks across the country and establishing links to international undersea cables, leading to expanding penetration.[13] By the end of 2012, Zimbabwe's largest private telecoms provider, Econet, reported that it had expanded its broadband customer base by 75 percent, with its GSM and WiMAX (voice and data) services covering nearly 80 percent of the country.[14]

Most Zimbabweans access the internet in cybercafes, which have experienced a resurgence since 2010 when the country's economic situation began to improve. Recent ICT investments have also encouraged the reopening of cybercafes in the country's urban centers, in addition to the rising demand for cheaper communication tools such as Voice over Internet Protocol (VoIP) applications,[15] which has been fueled by the growing expatriate population of Zimbabweans seeking to stay in touch with friends and family back home.

Despite the expanding penetration of ICTs across the country, there remains a significant urban-rural divide in access to both internet and mobile technologies, particularly as a result of major infrastructural limitations in rural areas, such as poor roads and electricity distribution. A Zimbabwe All Media Products and Services Survey released in September 2012 found that 41

[11] "Survey to Assist Policymakers: Zimstat," *The Herald* via *AllAfrica*, April 19, 2013, http://allafrica.com/stories/201304190669.html.
[12] Tonderai Rutsito, "Fibre Optic: 2012 Newsmaker," *The Herald*, January 9, 2013, http://www.herald.co.zw/fibre-optic-2012-newsmaker/.
[13] BuddeComm, "Zimbabwe – Telecoms, Mobile and Broadband," accessed July 31, 2013, http://www.budde.com.au/Research/Zimbabwe-Telecoms-Mobile-and-Broadband.html.
[14] Tawanda Karombo, "Econet Revenue and Broadband Users Surge," *ITWebAfrica*, October 26, 2012, http://www.itwebafrica.com/telecommunications/154-zimbabwe/230183-econet-revenue-and-broadband-user-numbersurge.
[15] "Econet Wireless launches VoiP," *TeleGeography*, January 26, 2012, http://www.telegeography.com/products/commsupdate/articles/2012/01/26/econet-wireless-launches-voip/.

percent of adults living in urban centers are using the internet,[16] with 83 percent of users accessing the web at least once a month. By contrast, an official government report estimates rural internet penetration to be 22 percent, though this figure is likely inflated given the national penetration rate of 17 percent according to the latest ITU data.

The government has endeavored to transform rural postal centers into ICT access points where internet services would be provided, but this initiative has yet to be fully realized. Even in urban areas, electricity is regularly rationed for six to seven hours a day, leading to uneven access to the internet and mobile phone service. Power outages affect not only households but also business entities such as cybercafes, while prolonged power blackouts often affect mobile telephony signal transmission equipment, resulting in cut-offs of both mobile networks and internet connections.

Zimbabwe currently has 28 licensed internet access providers (IAPs) and 128 internet service providers (ISPs),[17] the former of which offer only internet access while ISPs may provide additional services. However, ISP connections are constrained by the limited infrastructure of IAPs through which they must connect. As set by the telecoms regulator, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), the license fees for IAPs and ISPs range from $2-4 million, depending on the type of service to be provided, and must be vetted and approved by the regulator prior to installation.[18] Providers must also pay 3.5 percent of their annual gross income to POTRAZ. Application fees for operating a mobile phone service in Zimbabwe are also steep, and in 2013, the regulator increased the license fees for mobile networks from $100 million to $180 million.[19] There are no stringent fees or regulations that hinder the establishment of cybercafés.

While POTRAZ handles the official licensing process for telecoms, insider reports have revealed that the Zimbabwean military may be involved in screening and approving license applications, demonstrating that ICTs are regarded as a security matter for the state. There nevertheless have been no reports of harassment or license denials on the basis of political affiliation. Otherwise, internet access prices in Zimbabwe are set by ISPs and cybercafe owners and have thus far been free from state intervention. Individual ISPs submit tariff proposals to POTRAZ, which approves proposals on a per case basis.

Zimbabwe currently has five international gateways for internet and voice traffic, two of which are operated by the state-owned fixed network, TelOne, and mobile network, NetOne. The private mobile operators—Econet, TeleCel and Africom—operate the other three international

[16] Zimbabwe All Media Products Survey, Research International Bureau, Harare September, Third Quarter Report, 2012.
[17] Zimbabwe Internet Service Providers Association membership list, http://www.zispa.org.zw/members.html.
[18] L.S.M Kabweza, "Zimbabwe Raises Telecoms Licence Fees, Migrates to Converged Licensing," *TechZim*, March 12, 2013, http://www.techzim.co.zw/2013/03/zimbabwe-raises-telecoms-licence-fees-migrates-to-converged-licencing/.
[19] M. Kadzere, "Mobile License Fees Raised," *The Herald* via *AllAfrica*, March 12, 2013, http://allafrica.com/stories/201303130892.html.

gateways.[20] There are also two trunk switches for the TelOne fixed network and nine mobile switching centers,[21] set up by the country's three mobile operators.[22]

ISPs and mobile phone companies are regulated by the telecommunications regulatory body, POTRAZ, whose leaders are appointed by the president in consultation with the minister of transport and communication. POTRAZ has been widely accused of partisanship and politicized decision-making, such as demanding Econet to reconnect the state-owned mobile phone service provider NetOne after Econet had cut NetOne's service in August 2012 for defaulting on its interconnection fee payments.[23]

LIMITS ON CONTENT

In 2012 and early 2013, there were no reports of internet content being blocked or filtered, though various ruling party officials publicly expressed a desire and intent to increase control over ICTs. Civic engagement on social media platforms increased in the last year, fueled in large part by debates and discussions surrounding the general elections that took place in July 2013, during which bulk SMS text messaging via the international gateway was blocked while internet connections were reportedly slow. An anonymous Facebook user with the pseudonym Baba Jukwa became a social media sensation for its frequent posts that exposed alleged secrets from within the ZANU-PF ruling party, in addition to its naming and shaming campaign against corrupt party officials.

Several incidents in previous years hint at the extent to which the authorities are capable of filtering web content and their intent to do so. The most recent instance of online censorship was reported in 2006, when the Zimbabwean Reserve Bank had installed an e-mail content filtering system that blocked e-mails containing the words "Morgan Tsvangirai" or "MDC" and other political content.[24] It is uncertain whether this practice is still ongoing. There was also a case reported in 2005 in which the authorities had traced anti-government e-mail content and arrested its suspected senders.[25]

[20] Econet Wireless, "Statement on the Operation and Management of International Gateways,"via *Kubatana*, October 3, 2006, http://www.kubatana.net/html/archive/inftec/061002econet.asp?sector=inftec&year=2006&range_start=1.

[21] A "trunk switch" is a system that provides network access to many clients by sharing a set of lines or frequencies instead of providing them individually. A "mobile switching center" (MSC) connects calls by switching the digital voice data packets from one network path to another (also called routing). The MSC also provides information that is needed to support mobile service subscribers, such as user registration and authentication information.

[22] L.S.M Kabweza, "An Overview of Zimbabwe's Telecommunications—POTRAZ Presentation Download," *TechZim,* March 5, 2010, http://www.techzim.co.zw/2010/03/zimbabwe-telecoms-overview/.

[23] "Zimabwe's Econet Cuts Off Operator Over Fees," Reuters, August 23, 2012, http://www.reuters.com/article/2012/08/23/zimbabwe-econet-netone-idUSL6E8JN94C20120823; "Econet Reverses Decision to Terminate NetOne Interconnection," *The Herald* via *AllAfrica*, August 24, 2012, http://allafrica.com/stories/201208240359.html.

[24] Anonymous interviews with state media journalists at Zimpapers and Zimbabwe Broadcasting Holdings in January 2013; Clapperton Mavhunga, "The Glass Fortress: Zimbabwe's Cyber-Guerrilla Warfare," *Concerned Africa Scholars*, Bulletin 80 – Winter 2008, http://concernedafricascholars.org/docs/acasbulletin80-4.pdf.

[25] Open Net Initiative, "Country Profile: Zimbabwe," 2009, http://opennet.net/research/profiles/zimbabwe.

The last attempt by the authorities to implement a more systematic internet censorship regime occurred in 2004 when the government proposed a contract for all ISPs requiring them to block "objectionable" content and communications that were "inconsistent with the laws of Zimbabwe" as well as report "malicious messages" to the authorities.[26] Some ISPs agreed to comply with the proposed contract before it was declared unconstitutional by the Supreme Court a few months later.[27] No other such attempts to impose systematic restrictions on ICTs have been reported since.

Nevertheless, the government has routinely exhibited a desire to control digital communications, particularly during times of high political tension, such as elections or other potentially volatile situations. These efforts have been made primarily through intimidation and threats. Around the time of ZANU-PF's December 2009 party congress, for example, the authorities issued a warning to operators against allowing subscribers to use their networks for political purposes, which came in response to a mass circulation of text messages that had castigated the ruling party. The private telecom provider, Econet, in turn warned its subscribers that their service would be cut off if they sent political messages.[28]

Similarly in 2010, after the MDC announced that it would be using an Econet line to send bulk SMSs to keep in contact with its supporters, a column appeared in the government-controlled *Herald* newspaper that threatened to cancel Econet's operating license.[29] In response, Econet openly complained about the MDC's use of the network for political purposes and announced that it was installing software to identify and block problematic messages. These threat tactics from the authorities remain to this day and serve as a constant reminder to service providers of the need to remain in government favor. Mass SMS texting of apolitical nature is largely approved, but mobile service providers often refrain from carrying bulk messages sent by the MDC. To bypass such restrictions, the civic organization Kubatana, an online community of Zimbabwean activists and NGOs, uses an international gateway to send bulk text messages in the country, though this strategy failed in July 2013 when the regulator POTRAZ blocked international gateway bulk messaging in advance of the general elections.[30]

State employees, including those working for state-owned media, exercise self-censorship when sharing politically sensitive information. The pronounced lack of anonymity on social media platforms coupled with the attendant fear of repercussions tends to limit politically oriented statements, since they can be traced back to their authors. Although many journalists contribute to

---

[26] "MWeb 'Will Obey' Zim E-mail Snooping Laws," *New Zimbabwe*, June 2, 2004, http://www.newzimbabwe.com/pages/e-mail4.11921.html.

[27] "Supreme Court Bars Mugabe E-mail Snooping," *New Zimbabwe*, March 16, 2004, http://www.newzimbabwe.com/pages/email3.1537.html.

[28] "Zanu PF Texts Sent from Sweden: Econet," *New Zimbabwe*, December 17, 2009, http://www.newzimbabwe.com/news-1491-Zanu+PF+texts+sent+from+Sweden/news.aspx.

[29] The column was written under the pseudonym "Nathaniel Manheru," who is believed to be President Mugabe's spokesperson. See, Beth Jones, "Zimbabwe - ZANU-PF Threatens to Close Econet for Carrying a Political Campaign," *Zimbio*, June 19, 2010, http://www.zimbio.com/Zimbabwe/articles/r4ouXmtsT5e/Zimbabwe+ZANU+PF+threatens+close+Econet+carrying.

[30] Gareth van Zyl, "Zimbabwean Regulator 'Blocks' Bulk SMS as Election Nears," *ITWebAfrica*, July 29, 2013, http://www.itwebafrica.com/ict-and-governance/273-zimbabwe/231381-zimbabwean-regulator-blocks-bulk-sms-as-election-nears.

online news platforms, quite a number use pseudonyms when writing about sensitive issues for fear of harassment, and citizens are increasingly using pseudonyms online to discuss political topics.[31] Debates on the country's political and socioeconomic issues as well as reactions to online articles about Zimbabwe are mostly confined to chat rooms and feedback sections of online news sites. Concerns over state surveillance has also led to increasing self-censorship, and journalists and human rights defenders who feel threatened often resort to secure e-mail platforms such as Hush-Mail for correspondence out of concern that the Zimbabwe domain name .co.zw is an open book for state security.

There is a sense that the dominant political elite are losing the online battle. With the growing use of digital and social media tools, the ruling party has identified ICT-based communication platforms as a threat to its hold on power and has accordingly grown more intent on regulating and influencing online content.[32] For example, at its December 2012 party conference, a ZANU-PF official expressed the broad intention to invest at least $5 million in ICT and social media development to "fight cyber warfare."[33] Also in December 2012, during a meeting with the Chinese deputy minister of the State Counsel Information Office who was visiting Zimbabwe at the time, a ZANU-PF cabinet minister was quoted as stating that "there should be some form of control of the internet and other social media platforms because they [have] the potential to cause strife."[34]

Meanwhile, Facebook, Google, Yahoo, and YouTube, are among the most popular websites among Zimbabwean internet users. Media surveys indicate a declining readership of newspapers coinciding with the rising use of ICT-based platforms for news and other information.[35] In keeping with this shift, traditional media outlets are increasingly resorting to Facebook, Twitter, and other social media platforms to enhance their engagement with readers and listeners, receive feedback, and crowd-source news on various issues.[36] Due to the restrictive communications space in the country, blogs have become an important alternative platform for community organizations, minorities, individuals and online journalists to express their views. New blogs hosted by Blogspot and WordPress are on the rise, though as with journalists, some bloggers use pseudonyms out of fears of reprisal.

---

[31] Vladimir Mzaca, "What Online News Means for Zimbabwe," *Free African Media*, April 5, 2011, http://www.thezimbabwemail.com/opinion/7745.html; Tendai Chari, "Ethical Challenges Facing Zimbabwean Media in the Context of the Internet," *Global Media Journal - Africa Edition*, Zimbabwe, 2009, Vol 3 (1), globalmedia.journals.ac.za/pub/article/download/19/51; Committee to Protect Journalists, "Sweeping Surveillance Law to Target 'Imperialist-Sponsored Journalists,'" press release, August 9, 2007, http://allafrica.com/stories/200708090943.html; Barbara Borst, "African Journalists Struggle to Find their Role in Building Democracies," *Perspectives on Global Issues*, Volume 2, Issue 2, spring 2008, http://www.perspectivesonglobalissues.com/0301/borst.htm.

[32] Everson Mushava, "Technology a Security Threat: Sekeremayi," *Newsday*, May 9, 2013, http://www.newsday.co.zw/2013/05/09/technology-a-security-threat/.

[33] Tawanda Majoni, "ZANU PF Resolves to Jam Private Radio Stations," Nehanda Radio, December 11, 2012, http://nehandaradio.com/2012/12/11/zanu-pf-resolves-to-jam-private-radio-stations/.

[34] Everson Mushava, "Shamu Attacked over Internet Control," *Newsday*, December 20, 2012, http://www.newsday.co.zw/2012/12/20/shamu-attacked-over-internet-control/.

[35] Zimbabwe All Media Products Survey, Research International Bureau, Harare September, Third Quarter Report, 2012.

[36] The Newsday's Facebook page, http://www.facebook.com/pages/NewsDay-Zimbabwe/215170571826981 and ZiFM's Twitter account, https://twitter.com/ZiFMStereo.

Independent news websites and other digital media outlets based overseas have emerged as an important source of alternative information for those able to access them. The websites of outlets such as *New Zimbabwe* and Nehanda Radio publish information often obtained from stringers or other contacts based inside Zimbabwe, at times generating news that is later picked up by mainstream media outlets. There is no concrete evidence of government manipulation of online content, though there is some concern over the quality of the news in online publications that often re-publish content from state-owned sources.

Civil society groups use social media platforms to support imprisoned political activists and human rights defenders by providing instant updates on the country's human rights situation and other political developments.[37] Radio stations such as Star and ZiFM are also increasingly using social media as a tool to facilitate listener feedback and participation in their programs. Meanwhile, Zimbabwean journalists, long divided across state-owned and independent media lines, have found space on social media platforms to discuss current affairs and share information, contacts, and tips on story ideas.[38] Nevertheless, the growing use of social media platforms has yet to manifest in concrete social, political, or economic change in Zimbabwe.

In March 2013, a self-proclaimed disaffected ZANU-PF member created a Facebook page under the moniker Baba Jukwa, which had drawn a following of over 300,000 Facebook users (compared to the 100,000 followers both Mugabe and Tsvangirai have each) by July 2013. Characterizing himself as a "Concerned father, fighting nepotism and directly linking community with their Leaders, Government, MPs, and Ministers,"[39] Baba Jukwa quickly became a social media sensation for daily posts that named and shamed politicians for alleged corruption and informed on the ruling party's supposed secrets. Most notably, the anonymous informant was credited with predicting the death of a ZANU-PF member of parliament, Edward Chindori Chininga, who died in a suspicious car accident in June 2013, nine days after Chininga had released a report on widespread corruption in the country's diamond mines.[40] Threatened by the Facebook page's growing influence, Mugabe reportedly offered a $300,000 reward for Baba Jukwa's identity.[41] While the whistleblower's efforts on Facebook have yet to affect concrete change on the country's political and social reality, Baba Jukwa's popularity has been described as representing "the Zimbabwean people's growing appetite for information and transparency, which will only be fuelled by increasing access to information technology."[42]

---

[37] "Free Cynthia Manjoro and 23 Other Glen View Residents NOW!" Facebook group, http://www.facebook.com/groups/212089078834518/?fref=ts; Crisis Coalition Twitter page, https://twitter.com/crisiscoalition.

[38] Newsroom Lingo's Facebook page that brings Zimbabwe journalists from state and independent media, http://www.facebook.com/groups/390978400932282/?fref=ts.

[39] Baba Jukwa's Facebook page, accessed July 31, 2013, https://www.facebook.com/pages/Baba-Jukwa/232224626922797.

[40] "The Spirit of Wrath is Upon Us," *Economist*, June 19, 2013, http://www.economist.com/news/middle-east-and-africa/21580163-mysterious-facebook-character-predicting-murder-and-mayhem-spirit.

[41] Mary Ann Jolley, "Mugabe Offers $300,00 for Outing of Anonymous Whistleblower Baba Jukwa," ABC News, July 17, 2013, http://www.abc.net.au/news/2013-07-17/mugabe-offers-243002c000-for-outing-of-anonymous-whistleblower/4824498.

[42] Rebecca Regan-Sachs, "Baba Jukwa vs. Mugabe – the Man On Facebook Standing Up to Zimbabwe's President," Think Africa Press via *All Africa*, July 24, 2013, http://allafrica.com/stories/201307241382.html?viewall=1.

VIOLATIONS OF USER RIGHTS

A new constitution came into force in May 2013 that included provisions for freedom of expression and of the press. Nevertheless, legal restrictions that contradicted the new constitutional guarantees remained in place and were frequently used against journalists, particularly for violations in the traditional media in the lead-up to the July 2013 general elections. Two mobile phone users were arrested during the coverage period for sending text messages that allegedly insulted the president. An investigative report in early 2013 uncovered evidence of a "massive" cyber training program for Zimbabwean security agents facilitated by Iranian intelligence organizations.

In 2013, Zimbabwe adopted a new constitution that was approved by parliament in May and signed into law by the president shortly thereafter.[43] Sections 60, 61, and 62 of the constitution guarantees freedom of expression, press freedom, access to information, protection of sources of information as well as the editorial independence of state-owned media. While these provisions are focused on the traditional media, it is expected that the new rights will also extend online. Accordingly, online journalists, bloggers, and citizens using social media platforms to share information can potentially seek protection under the new constitution.

Nevertheless, there are no laws that specifically protect online modes of communication, and bloggers are not recognized as eligible for accreditation as journalists. While the judiciary has sometimes demonstrated a degree of autonomy through rulings that are not necessarily favorable to the state, some in freedom of expression cases, the government often ignores such decisions. An appointment process that allows for high levels of executive interference further compromises judicial independence.

Meanwhile, the country's civil and criminal defamation laws, the Interception of Communications Act of 2007, and the Criminal Law Codification and Reform Act (CODE) remain on the books and apply equally to reporters in the traditional media and online. The CODE punishes anyone who publicly undermines the authority of the president or insults him in any printed or electronic medium with a sentence of up to 20 years in prison.[44] In addition, Zimbabwe maintains restrictive access to information and media laws, which include the Access to Information and Protection of Privacy Act, the Criminal Codification Act, the Public Order and Security Act, and the Officials Secrets Act, among others. Combined with the extrajudicial actions of both state and non-state actors, these laws severely limit Zimbabweans' ability to access and share information.[45]

Since the signing of the Global Political Agreement at the end of 2008 that brokered a power-sharing deal between Robert Mugabe and Morgan Tsvangirai, violations against journalists have decreased significantly, though the improvement has not entailed a change in the dominant political

[43] Cris Chinaka, "Mugabe Signs Zimbabwe Constitution, Paving Way for Vote," Reuters, May 22, 2013, http://www.reuters.com/article/2013/05/22/us-zimbabwe-constitution-idUSBRE94L0RT20130522.
[44] Criminal Law (Codification and Reform) Act [Chapter 9:23], Act 23/2004, Government Gazette, June 3, 2005, http://www.kubatana.net/docs/legisl/criminal_law_code_050603.pdf.
[45] Constitution of Zimbabwe, http://www.gta.gov.zw/index.php/documents/constitution-of-zimbabwe.

elite's attitude against the independent media. Arrests,[46] verbal attacks, and harassment against traditional media journalists, including expulsion from press conferences, still continue.[47]

Penalties for online activities, however, have been less common. In one recent case, a South African-based Zimbabwean man, Benias Madhakasi, was thrown in police custody in April 2012 and held for three months for insulting the president after it was discovered that he had an image and inscription on his mobile phone that read, "Happy 87th Birthday (Operation Matibili)," referring to the president's nickname. The prosecutor opposed bail until the High Court threw out the charges in July 2012.[48] In a second case, Bulawayo resident Shantel Rusike was arrested on December 24, 2012 and held for four days after she was reported to the police for sending an image depicting President Mugabe in a nude state via WhatsApp on her mobile phone.[49] Rusike, out on $100 bail, faces charges of "causing hatred, contempt or ridicule of the president," as delineated in the CODE.[50] As of mid-2013, her case was still before the courts.

Website owners, bloggers, and internet users are not required to register with the government, though mobile phone users must register their SIM cards by submitting personal identity details to the mobile operator, ostensibly to combat crime and curtail threatening or obscene communications.[51] POTRAZ reported that approximately two million subscribers were disconnected in mid-2011 as a result of non-compliance,[52] though the number of registered mobile telephone users increased thereafter.

Meanwhile, POTRAZ has maintained a September 2011 ban—reportedly enacted for security reasons—on the use of the BlackBerry messenger service that enables users to send free messages.[53] The ban went into effect in response to unfounded fears that the service had facilitated the 2011 Arab uprisings as well as the violent protests that took place in England in August of the same year.[54] In mid-2011, POTRAZ director general Charles Manzi Sibanda announced that the regulator was examining the compliance of BlackBerry's encryption technology with the Interception of Communications Act, which requires that all telecommunication services allow

[46] "Police Charge Zimind Editor, Reporter," *Newsday,* May 8, 2013, http://www.newsday.co.zw/2013/05/08/police-charge-zimind-editor-reporter/.
[47] Ndakaziva Majaka, "Mudede gags Media," *Daily News,* accessed 7 January 2013, http://www.dailynews.co.zw/mobi/article/News/7ae212a6-d66b-490c-927d-a75af2da46ce.
[48] "Court Frees Man Found with 'Nude' Mugabe Pictures," Nehanda Radio, July 25, 2012, http://nehandaradio.com/2012/07/25/court-frees-man-found-with-nude-mugabe-pictures/.
[49] Alex Bell, "'Naked' Mugabe Picture Lands Woman in Court," Nehanda Radio, January 9, 2013, http://nehandaradio.com/2013/01/09/naked-mugabe-picture-lands-woman-in-court/.
[50] Section 33(2)(a)(ii) of the Criminal Law (Codification and Reform) Act/CODE Chapter 9:23.
[51] "POTRAZ Issues Mobile Phone Registration Reminder," *Technology Zimbabwe*, January 31, 2011, http://www.techzim.co.zw/2011/01/potraz-registration-reminder/.
[52] Tawanda Musarurwa, "Zimbabwe: Tele-Density Rate takes Dip," *The Herald* via *AllAfrica*, May 10, 2011, http://allafrica.com/stories/201105110010.html, cited in L.S.M Kabweza, "ICT Policy and New Media Cultures in Southern Africa – Zimbabwe Report, Internal report for the Department of Media Studies" (South Africa: University of the Witwatersrand, 2011).
[53] BlackBerry formerly operated as Research in Motion. "BlackBerry Messenger a Dream," *The Zimbabwean,* June 5, 2012, http://www.thezimbabwean.co.uk/technology/58636/blackberry-messenger-a-dream.html.
[54] "Mugabe Vetoes Blackberry Service," *The Zimbabwean*, September 28, 2011, http://www.thezimbabwean.co.uk/news/zimbabwe/53208/mugabe-vetoes-blackberry.html.

official interception.[55] The POTRAZ decision was still outstanding as of October 2012.[56] Other encrypted communication applications, such as Skype, remain accessible.

The Post and Telecommunications Act of 2000 allows the government to monitor communications, including e-mail, and requires ISPs to supply information to government officials upon request.[57] The act also obligates ISPs to report any e-mail with "offensive" or "threatening" content. Meanwhile, the Interception of Communications Act of 2007 established a Monitoring of Interception of Communications Center with the powers to oversee traffic in all telecommunications services and to intercept phone calls, e-mails, and faxes under the pretext of national security.[58] The Act further requires telecommunications operators and ISPs to install necessary surveillance technology at their own expense and to intercept information on the state's behalf.[59] Failure to comply is punishable with a fine and sentence of up to three years in prison.

Warrants allowing the monitoring and interception of communications are issued by the minister of information at his discretion; consequently, there is no substantial judicial oversight or other independent safeguard against abuse. The extent and frequency of monitoring therefore remains uncertain. There are also reports that the Central Intelligence Organization monitors all networks connected to the IP world's routing system through the Interception of Communications Unit, which is administered by a top ZANU-PF politician.[60]

Following the passage of the ICA in 2007, there were unconfirmed reports that Zimbabwe's government had received surveillance technology and training from China,[61] and suspicions of Chinese technical assistance in controlling ICTs remain strong.[62] More recently in March 2013, the news and internet radio station, Nehanda Radio, reported that it had confirmed a "massive" cyber training program that had begun in 2007 with assistance from Iranian intelligence organizations.[63] According to the report, personnel from the Zimbabwean armed forces and the CIO have been undergoing intensive cyber training in "technological warfare techniques, counter-intelligence and methods of suppressing popular revolts among others, every six months."

---

[55] Section 12 (1) (a) of the Act reads: "Notwithstanding any other law, a telecommunication service provider shall provide a telecommunication service which has the capacity to be intercepted."
[56] BlackBerry Zimbabwe's Facebook post, October 14, 2012, https://www.facebook.com/BlackBerry.Zimbabwe.
[57] Postal and Telecommunications Act, http://www.potraz.gov.zw/files/Postal_Act.pdf.
[58] Reporters Without Borders, "All Communications Can Now be Intercepted Under New Law Signed by Mugabe," news release, August 6, 2007, http://en.rsf.org/zimbabwe-all-communications-can-now-be-06-08-2007,17623.html. The law is available at *Kubatana,* http://kubatana.net/docs/legisl/icb_070508.pdf.
[59] Nqobizitha Khumalo, "Zim Internet Service Providers Struggle to Buy Spying Equipment," *ZimOnline*, August 10, 2007, http://www.kubatana.net/html/archive/inftec/070810zol1.asp?spec_code=060426commdex&sector=INFTEC&year=0&range_start=1&intMainYear=0&intTodayYear=2010.
[60] "Mugabe Vetoes Blackberry Service," *The Zimbabwean*, September 28, 2011, http://www.thezimbabwean.co.uk/news/zimbabwe/53208/mugabe-vetoes-blackberry.html.
[61] Lance Guma, "Too Much to Monitor for Snooping Squads," SW Radio Africa, August 7, 2007, http://www.swradioafrica.com/news070807/snoop070807.htm; Reporters Without Borders, "All Communications Can Now Be Intercepted under New Law Signed by Mugabe," news release, August 6, 2007; "Zimbabwe's bugging bill condemned," BBC News, June 15, 2007, http://news.bbc.co.uk/2/hi/africa/6755753.stm.
[62] Amber Will, "Peeking Behind the Curtain: Analyzing Chinese Aid and Influence in Zimbabwe," *The First Tranche* (blog), AidData, July 30, 2013, http://blog.aiddata.org/2013/07/updated-peeking-behind-curtain.html.
[63] Itai Mushekwe, "Iran Helping Zimbabwe Snoop on Internet," Nehanda Radio, March 27, 2013, http://bit.ly/YKatMO.

There have been no reported cases of attacks against bloggers and online journalists, despite concerns over potential violence and unrest surrounding the 2013 elections in July and its aftermath. In the first half of 2013, there was an explosion of political content on social media platforms, with bold and unrestrained political discussions taking place, such as on the Facebook page of the anonymous informant, Baba Jukwa (see "Limits on Content").[64] These activities, particularly those linked to the July 2013 elections, have purportedly alarmed the security and political sector, and reports indicate that the ruling party and its security agencies are increasingly focusing on attacking and uncovering the identities of anonymous social media activists.[65] What technology the Zimbabwean authorities do have to monitor internet users has nonetheless failed to expose the true identity of Baba Jukwa,[66] though the whistleblower's Facebook and Twitter accounts have reportedly been subject to several hacking attacks, resulting in the deletion of some of Jukwa's damaging posts.[67]

The government has reportedly used Chinese assistance to hack into websites of independent newspapers, although this also cannot be confirmed. In December 2011, for example, the website of the *Daily News*, one of Zimbabwe's private newspapers, experienced a series of attacks on its website, which the *Daily News's* information technology department blamed on Chinese hackers working with in conjunction with the Zimbabwean authorities.[68] Meanwhile, government websites are increasingly the target of hacking attacks, with the website of the Ministry of Mines most recently hacked in March 2013.

[64] Everson Mushava, "Baba Jukwa distresses ZANU PF," *Newsday*, April 30, 2013, http://www.newsday.co.zw/2013/04/30/baba-jukwa-distresses-zanu-pf/.
[65] "Baba Jukwa: Legion of Malicious Engagement," *The Herald* via *All Africa*, May 14, 2013, http://allafrica.com/stories/201305140292.html.
[66] "Should Africa Be Worried About Chinese Cyber-Espionage?" ICT Africa, June 2, 2013, http://ictafrica.info/FullNews.php?id=9480.
[67] "Julian Assange, Baba Jukwa and Cyberpunks," ICT Africa, May 4, 2013, http://ictafrica.info/FullNews.php?id=9002.
[68] "Chinese Cyber Spooks Intensify Zimbabwe Media Attacks, The Zimbabwe Mail targeted," *The Zimbabwe Mail*, December 30, 2011, https://groups.google.com/forum/#!topic/InfoAccessNow/PD-F_uU-5Uk.

GLOSSARY

Definitions are based on **Freedom on the Net 2013** *research, Merriam Webster Online, www.merriam-webster.com and Webopedia: Online Computer Dictionary for Computer and Internet Terms and Definitions, www.webopedia.com.*

- **3G:** Third generation mobile communications technology, which allows internet access through mobile phones.
- **4G:** Fourth generation wireless communications standard, allowing broadband mobile internet access. Several technologies are considered 4G standards, including **4G LTE** and **WiMAX**.
- **4G LTE:** Short for long term evolution, 4G LTE allows mobile internet access up to 10 times faster than 3G.
- **ADSL**: (see DSL)
- **Apps:** Short for software applications, apps are programs designed for use online or on a mobile device. Communications apps like WhatsApp and Skype allow real-time messaging or voice calls.
- **Blog:** Short for weblog, blogs are highly-customizable personal websites, often published on specific **Hosting Services**. While blogs cover a broad range of issues and activities, many provide an important platform for free expression and political debate.
- **Blogosphere:** All the blogs on the internet or within a specific country, for example, the Tunisian blogosphere.
- **Broadband:** A high-speed internet connection in which a single wire can carry many channels at once, allowing a high data-transfer rate. Broadband is necessary for viewing multimedia content.
- **Bulletin Board System (BBS):** An electronic message center. Most bulletin boards serve specific interest groups; users can post information or products for sale, and other posters can respond.

- **CDMA:** Short for code-division multiple access, CDMA is a **3G** mobile technology with high bandwidth, allowing efficient internet access via cellphone.
- **Chat Room:** An online location that allows multiple users to engage in a real-time, text-based conversation or discussion

- **Cybercafe:** Any commercial location where patrons can use computers to access the internet for a specified fee and time.

- **Cyberspace:** The nonphysical world created by computer systems. The internet, for example, creates a cyberspace within which people can communicate with one another, do research, or simply window shop.

- **DDoS Attack:** Distributed denial of service attacks try to prevent a website from functioning, either temporarily or indefinitely, by overloading it with so many requests for data that it slows down or crashes. Those responsible often infiltrate computers around the world and program them to join in the assault as an automated network, or "botnet."

- **Dial-up:** An internet connection over a standard telephone line, usually with a very slow speed that makes it difficult to access some features, especially multimedia applications.

- **Dongle:** A device that attaches to a computer via a **USB** or other port to provide access to certain applications. If equipped with **3G** or **WiMax** technology, a dongle allows portable internet access.

- **DNS:** Short for domain name system. DNS is an internet service that translates alphabetic domain names—the appellations commonly used to identify websites—into numerical **IP addresses**. Every time a user enters a domain name, a DNS service must translate the name into the corresponding IP address; for example, the domain name example.com might translate to 198.105.232.4.

- **DSL and ADSL:** Digital subscriber lines allow data transmission over the wires of a local telephone network, at a faster speed than **dial-up** but without obstructing telephone use on the same line. Variations, grouped as xDSL, include **ADSL** or asymmetric digital subscriber lines, which feature a greater flow of data in one direction than in the other, so that download speeds are often much faster than upload speeds.

- **Fiber optic cables**: Cables made of glass or plastic fibers, used to transmit data. Fiber optic cables have a much greater bandwidth than metal wires typically used for local telephone networks, can carry more data, and are less susceptible to interference.

- **FTTH:** Short for fiber-to-the-home, FTTH indicates the installation of internet-capable **fiber optic cables** directly into a subscriber's home. Variations include fiber-to-the-curb (FTTC) and fiber-to-the-building (FTTB).

- **Firewall:** A system designed to prevent unauthorized access to or from a private network; implemented in either hardware or software. A firewall blocks any messages entering or leaving the protected network if they do not meet specific criteria. Companies can use them to prevent employees from accessing select websites, and several countries—notably China and Iran—employ firewalls on a national level to prevent citizens from accessing content from abroad.

- **Forum:** An online discussion group in which participants with common interests can exchange open messages.

- **GSM:** Short for global system for mobile communications, GSM is a narrowband mobile standard widely used around the world.

- **Hashtag:** A word or phrase pre-fixed by the hash symbol, used to make social media conversations searchable by topic. For example, Twitter users can follow the *Freedom on the Net 2013* launch by searching for the hashtag #FOTN2013.

- **Hosting service:** A service provider that houses, or hosts, multiple websites on its server computers in exchange for a fee.

- **ICT:** Information and communications technology, including computers and mobile devices.

- **Instant Messaging:** Real-time, text-based communication between individuals in what amounts to a temporary private chat room.

- **IP address:** The numeric address of a computer on the internet. An IP address is used to identify a computer and network in much the same way as a social security number is used to identify a person.

- **ISP:** Internet service providers are companies that provide access to the internet for a fee, supplying customers with a software package, a username, a password, and telephone numbers to initiate a connection.

- **IT:** Information technology, the broad subject concerned with all aspects of managing and processing information.

- **Local Area Network (LAN):** A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

- **Malware:** Software designed to damage or disrupt a system, such as a virus. This includes spyware, that may retrieve data about a computer user's behavior without their knowledge.

- **Microblog**: A type of **blog** that allows users to publish short text updates that are disseminated to a large number of followers. Twitter is an example of a microblogging site that allows posts of up to 140 characters.

- **Netizen:** Citizen of the internet; a person actively involved in the online community.

- **Packet sniffer:** Computer software or hardware that can intercept and log traffic passing over a network. Packet sniffers, often part of a firewall system, can be used to spy on users and collect sensitive information such as passwords.

- **Proxy server:** A server or computer that sits between a user and a website to intercept requests. Proxy servers have various uses. In *Freedom on the Net 2013,* they typically refer to a tool used to circumvent blocks on accessing certain websites.

- **Real name registration**: A system by which users who want to post a comment online have to supply their real name, ID card number, contact phone or address.

- **Secure Sockets Layer (SSL):** A method for transmitting private documents and data over the internet using two-layer encryption for security. SSL is most often used in websites that handle private or financial data, and is denoted by the use of "https" in the URL rather than the standard "http."

- **SIM card:** Short for subscriber identity module, SIM cards are used in phones on the GSM network to store an individual's phone number, authorize their connection, and encrypt their data. SIM cards can be switched between phones.

- **SMS/Text Messaging:** Short message service or SMS messages are brief text messages of no more than a few hundred characters, sent electronically between mobiles.
- **Spyware:** See Malware.

- **Trolling:** Maliciously disrupting conversations on a **microblog, chat room, forum** or **BBS** with inflammatory or derogatory comments, is known as trolling, while the individual who does so is identified as a troll. Lingering in chat rooms without participating, which may be a sign of spying on other internet users, can also be described as trolling.

- **URL:** Short for uniform resource locator, a URL is the global address of a document or page on the world wide web. The URL for Freedom House is http://www.freedomhouse.org/.

- **USB Modem:** A portable USB or universal serial bus device that looks similar to a USB flash drive (a data storage device) and can be plugged into any USB port on a computer to allow broadband internet access.

- **Value-added Network Service (VANS):** A network provider hired to facilitate electronic data interchange or provide other services such as data translation, encryption, or secure e-mail.

- **Virtual Private Network (VPN):** VPNs offer a means to communicate privately through a public network by creating an encrypted tunnel between two or more locations. This can be used to circumvent national censorship, and corporations that operate in repressive internet environments often purchase the right to use VPNs to connect to their home offices from the government.

- **VoIP:** Voice over Internet Protocol is a category of hardware and software that enables users to make telephone calls via the internet; these calls do not incur a surcharge beyond what the user is paying for internet access.

- **Wi-Fi:** Wireless technology that provides an internet or network connection for properly equipped computers, mobile phones, and other devices within a given area.

- **WiMAX:** Scalable wireless technology that works over much longer distances than **Wi-Fi**, providing an alternative for both fixed and mobile internet access. WiMAX stands for worldwide interoperability for microwave access.

METHODOLOGY

This fourth edition of *Freedom on the Net* provides analytical reports and numerical ratings for 60 countries worldwide. The countries were chosen to provide a representative sample with regards to geographical diversity and economic development, as well as varying levels of political and media freedom. The ratings and reports included in this study particularly focus on developments that took place between May 1, 2012 and April 30, 2013.

WHAT WE MEASURE

The *Freedom on the Net* index aims to measure each country's level of internet and digital media freedom based on a set of methodology questions described below (see "Checklist of Questions"). Given increasing technological convergence, the index also measures access and openness of other digital means of transmitting information, particularly mobile phones and text messaging services.

Freedom House does not maintain a culture-bound view of freedom. The project methodology is grounded in basic standards of free expression, derived in large measure from Article 19 of the Universal Declaration of Human Rights:

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers."*

This standard applies to all countries and territories, irrespective of geographical location, ethnic or religious composition, or level of economic development.

The project particularly focuses on the transmission and exchange of news and other politically relevant communications, as well as the protection of users' rights to privacy and freedom from both legal and extralegal repercussions arising from their online activities. At the same time, the index acknowledges that in some instances freedom of expression and access to information may be legitimately restricted. The standard for such restrictions applied in this index is that they be implemented only in narrowly defined circumstances and in line with international human rights standards, the rule of law, and the principles of necessity and proportionality. As much as possible, censorship and surveillance policies and procedures should be transparent and include avenues for appeal available to those affected.

The index does not rate governments or government performance per se, but rather the real-world rights and freedoms enjoyed by individuals within each country. While digital media freedom may be primarily affected by state actions, pressures and attacks by nonstate actors, including the criminal underworld, are also considered. Thus, the index ratings generally reflect the interplay of a variety of actors, both governmental and nongovernmental, including private corporations.

THE SCORING PROCESS

The index aims to capture the entire "enabling environment" for internet freedom within each country through a set of 21 methodology questions, divided into three subcategories, which are intended to highlight the vast array of relevant issues. Each individual question is scored on a varying range of points. Assigning numerical points allows for comparative analysis among the countries surveyed and facilitates an examination of trends over time. Countries are given a total score from 0 (best) to 100 (worst) as well as a score for each sub-category. Countries scoring between 0 to 30 points overall are regarded as having a "Free" internet and digital media environment; 31 to 60, "Partly Free"; and 61 to 100, "Not Free". An accompanying country report provides narrative detail on the points covered by the methodology questions.

The methodology examines the level of internet freedom through a set of 21 questions and nearly 100 accompanying subpoints, organized into three groupings:

- ***Obstacles to Access***—including infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; legal and ownership control over internet and mobile phone access providers.
- ***Limits on Content***—including filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.
- ***Violations of User Rights***—including legal protections and restrictions on online activity; surveillance and limits on privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

The purpose of the subpoints is to guide analysts regarding factors they should consider while evaluating and assigning the score for each methodology question. After researchers submitted their draft scores, Freedom House convened five regional review meetings and numerous international conference calls, attended by Freedom House staff and over 70 local experts, scholars, and civil society representatives from the countries under study. During the meetings, participants reviewed, critiqued, and adjusted the draft scores—based on the set coding guidelines—through careful consideration of events, laws, and practices relevant to each item. After completing the regional and country consultations, Freedom House staff did a final review of all scores to ensure their comparative reliability and integrity.

CHECKLIST OF QUESTIONS

- Each country is ranked on a scale of 0 to 100, with 0 being the best and 100 being the worst.
- A combined score of 0-30=Free, 31-60=Partly Free, 61-100=Not Free.
- Under each question, **a lower number of points is allotted for a more free situation, while a higher number of points is allotted for a less free environment.**
- Unless otherwise indicated, the sub-questions listed are meant to provide guidance as to what issues should be addressed under each methodology question, though not all will apply to every country.

A. OBSTACLES TO ACCESS (0-25 POINTS)

1. **To what extent do infrastructural limitations restrict access to the internet and other ICTs? (0-6 points)**
   - *Does poor infrastructure (electricity, telecommunications, etc) limit citizens' ability to receive internet in their homes and businesses?*
   - *To what extent is there widespread public access to the internet through internet cafes, libraries, schools and other venues?*
   - *To what extent is there internet and mobile phone access, including via 3G networks or satellite?*
   - *Is there a significant difference between internet and mobile-phone penetration and access in rural versus urban areas or across other geographical divisions?*
   - *To what extent are broadband services widely available in addition to dial-up?*

2. **Is access to the internet and other ICTs prohibitively expensive or beyond the reach of certain segments of the population? (0-3 points)**
   - *In countries where the state sets the price of internet access, is it prohibitively high?*
   - *Do financial constraints, such as high costs of telephone/internet services or excessive taxes imposed on such services, make internet access prohibitively expensive for large segments of the population?*
   - *Do low literacy rates (linguistic and "computer literacy") limit citizens' ability to use the internet?*
   - *Is there a significant difference between internet penetration and access across ethnic or socio-economic societal divisions?*
   - *To what extent are online software, news, and other information available in the main local languages spoken in the country?*

3. **Does the government impose restrictions on ICT connectivity and access to particular social media and communication apps permanently or during specific events? (0-6 points)**

- *Does the government place limits on the amount of bandwidth that access providers can supply?*
- *Does the government use control over internet infrastructure (routers, switches, etc.) to limit connectivity, permanently or during specific events?*
- *Does the government centralize telecommunications infrastructure in a manner that could facilitate control of content and surveillance?*
- *Does the government block protocols and tools that allow for instant, person-to-person communication (VOIP, instant messaging, text messaging, etc.), particularly those based outside the country (i.e. YouTube, Facebook, Skype, etc.)?*
- *Does the government block protocols, social media, and/or communication apps that allow for information sharing or building online communities (video-sharing, social-networking sites, comment features, blogging platforms, etc.) permanently or during specific events?*
- *Is there blocking of certain tools that enable circumvention of online filters and censors?*

4. **Are there legal, regulatory, or economic obstacles that prevent the existence of diverse business entities providing access to digital technologies? (0-6 points)**

Note: Each of the following access providers are scored separately:

1a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)
1b. Cybercafes and other businesses entities that allow public internet access (0-2 points)
1c. Mobile phone companies (0-2 points)

- *Is there a legal or de facto monopoly over access providers or do users have a choice of access provider, including ones privately owned?*
- *Is it legally possible to establish a private access provider or does the state place extensive legal or regulatory controls over the establishment of providers?*
- *Are registration requirements (e.g. bureaucratic "red tape") for establishing an access provider unduly onerous or are they approved/rejected on partisan or prejudicial grounds?*
- *Does the state place prohibitively high fees on the establishment and operation of access providers?*

5. **To what extent do national regulatory bodies overseeing digital technology operate in a free, fair, and independent manner? (0-4 points)**

- *Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (exclusively or as part of a broader mandate) from political or commercial interference?*
- *Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' interests?*

- *Are decisions taken by the regulatory body, particularly those relating to ICTs, seen to be fair and apolitical and to take meaningful notice of comments from stakeholders in society?*
- *Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?*
- *Does the allocation of digital resources, such as domain names or IP addresses, on a national level by a government-controlled body create an obstacle to access or are they allocated in a discriminatory manner?*

B. LIMITS ON CONTENT (0-35 POINTS)

1. **To what extent does the state or other actors block or filter internet and other ICT content, particularly on political and social issues? (0-6 points)**
   - *Is there significant blocking or filtering of internet sites, web pages, blogs, or data centers, particularly those related to political and social topics?*
   - *Is there significant filtering of text messages or other content transmitted via mobile phones?*
   - *Do state authorities block or filter information and views from inside the country—particularly concerning human rights abuses, government corruption, and poor standards of living—from reaching the outside world through interception of e-mail or text messages, etc?*
   - *Are methods such as deep-packet inspection used for the purposes of preventing users from accessing certain content or for altering the content of communications en route to the recipient, particularly with regards to political and social topics?*

2. **To what extent does the state employ legal, administrative, or other means to force deletion of particular content, including requiring private access providers to do so? (0-4 points)**
   - *To what extent are non-technical measures—judicial or extra-legal—used to order the deletion of content from the internet, either prior to or after its publication?*
   - *To what degree does the government or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?*
   - *Are access providers and content hosts legally responsible for the information transmitted via the technology they supply or required to censor the content accessed or transmitted by their users?*
   - *Are access providers or content hosts prosecuted for opinions expressed by third parties via the technology they supply?*

3. **To what extent are restrictions on internet and ICT content transparent, proportional to the stated aims, and accompanied by an independent appeals process? (0-4 points)**
   - *Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?*

- *Are state authorities transparent about what content is blocked or deleted (both at the level of public policy and at the moment the censorship occurs)?*
- *Do state authorities block more types of content than they publicly declare?*
- *Do independent avenues of appeal exist for those who find content they produced to have been subjected to censorship?*

4. **Do online journalists, commentators, and ordinary users practice self-censorship? (0-4 points)**

- *Is there widespread self-censorship by online journalists, commentators, and ordinary users in state-run online media, privately run websites, or social media applications?*
- *Are there unspoken "rules" that prevent an online journalist or user from expressing certain opinions in ICT communication?*
- *Is there avoidance of subjects that can clearly lead to harm to the author or result in almost certain censorship?*

5. **To what extent is the content of online sources of information determined or manipulated by the government or a particular partisan interest? (0-4 points)**

- *To what degree do the government or other powerful actors pressure or coerce online news outlets to follow a particular editorial direction in their reporting?*
- *Do authorities issue official guidelines or directives on coverage to online media outlets, blogs, etc., including instructions to marginalize or amplify certain comments or topics for discussion?*
- *Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the online content they produce or host?*
- *Does the government employ, or encourage content providers to employ, individuals to post pro-government remarks in online bulletin boards and chat rooms?*
- *Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?*

6. **Are there economic constraints that negatively impact users' ability to publish content online or online media outlets' ability to remain financially sustainable? (0-3 points)**

- *Are favorable connections with government officials necessary for online media outlets or service providers (e.g. search engines, e-mail applications, blog hosting platforms, etc.) to be economically viable?*
- *Are service providers who refuse to follow state-imposed directives to restrict content subject to sanctions that negatively impact their financial viability?*
- *Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it limit advertisers from conducting business with disfavored online media or service providers?*

- *To what extent do ISPs manage network traffic and bandwidth availability to users in a manner that is transparent, evenly applied, and does not discriminate against users or producers of content based on the content/source of the communication itself (i.e. respect "net neutrality" with regard to content)?*
- *To what extent do users have access to free or low-costs blogging services, webhosts, etc. to allow them to make use of the internet to express their own views?*

7. **To what extent are sources of information that are robust and reflect a diversity of viewpoints readily available to citizens, despite government efforts to limit access to certain content? (0-4 points)**

- *Are people able to access a range of local and international news sources via the internet or text messages, despite efforts to restrict the flow of information?*
- *Does the public have ready access to media outlets or websites that express independent, balanced views?*
- *Does the public have ready access to sources of information that represent a range of political and social viewpoints?*
- *To what extent do online media outlets and blogs represent diverse interests within society, for example through websites run by community organizations or religious, ethnic and other minorities?*
- *To what extent do users employ proxy servers and other methods to circumvent state censorship efforts?*

8. **To what extent have individuals successfully used the internet and other ICTs as tools for mobilization, particularly regarding political and social issues? (0-6 points)**

- *To what extent does the online community cover political developments and provide scrutiny of government policies, official corruption, or the behavior of other powerful societal actors?*
- *To what extent are online communication tools (e.g. Twitter) or social networking sites (e.g. Facebook, Orkut) used as a means to organize politically, including for "real-life" activities?*
- *Are mobile phones and other ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?*

C. VIOLATIONS OF USER RIGHTS (0-40 POINTS)

1. **To what extent does the constitution or other laws contain provisions designed to protect freedom of expression, including on the internet, and are they enforced? (0-6 points)**

- *Does the constitution contain language that provides for freedom of speech and of the press generally?*
- *Are there laws or legal decisions that specifically protect online modes of expression?*
- *Are online journalists and bloggers accorded the same rights and protections given to print and broadcast journalists?*
- *Is the judiciary independent and do the Supreme Court, Attorney General, and other representatives of the higher judiciary support free expression?*

- *Is there implicit impunity for private and/or state actors who commit crimes against online journalists, bloggers, or other citizens targeted for their online activities?*

2. **Are there laws which call for criminal penalties or civil liability for online and ICT activities? (0-4 points)**

- *Are there specific laws criminalizing online expression and activity such as posting or downloading information, sending an e-mail, or text message, etc.? (Note: this excludes legislation addressing harmful content such as child pornography or activities such as malicious hacking)*
- *Do laws restrict the type of material that can be communicated in online expression or via text messages, such as communications about ethnic or religious issues, national security, or other sensitive topics?*
- *Are restrictions of internet freedom closely defined, narrowly circumscribed, and proportional to the legitimate aim?*
- *Are vaguely worded penal codes or security laws applied to internet-related or ICT activities?*
- *Are there penalties for libeling officials or the state in online content?*
- *Can an online outlet based in another country be sued if its content can be accessed from within the country (i.e. "libel tourism")?*

3. **Are individuals detained, prosecuted or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs, particularly on political and social issues? (0-6 points)**

- *Are writers, commentators, or bloggers subject to imprisonment or other legal sanction as a result of posting material on the internet?*
- *Are citizens subject to imprisonment, civil liability, or other legal sanction as a result of accessing or downloading material from the internet or for transmitting information via e-mail or text messages?*
- *Does the lack of an independent judiciary or other limitations on adherence to the rule of law hinder fair proceedings in ICT-related cases?*
- *Are individuals subject to abduction or arbitrary detention as a result of online activities, including membership in certain online communities?*
- *Are penalties for "irresponsible journalism" or "rumor mongering" applied widely?*
- *Are online journalists, bloggers, or others regularly prosecuted, jailed, or fined for libel or defamation (including in cases of "libel tourism")?*

4. **Does the government place restrictions on anonymous communication or require user registration? (0-4 points)**

- *Are website owners, bloggers, or users in general required to register with the government?*
- *Are users able to post comments online or purchase mobile phones anonymously or does the government require that they use their real names or register with the government?*
- *Are users prohibited from using encryption software to protect their communications?*
- *Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?*

5. **To what extent is there state surveillance of internet and ICT activities without judicial or other independent oversight, including systematic retention of user traffic data? (0-6 points)**

- *Do the authorities regularly monitor websites, blogs, and chat rooms, or the content of e-mail and mobile text messages, including via deep-packet inspection?*
- *To what extent are restrictions on the privacy of digital media users transparent, proportional to the stated aims, and accompanied by an independent process for lodging complaints of violations?*
- *Where the judiciary is independent, are there procedures in place for judicial oversight of surveillance and to what extent are these followed?*
- *Where the judiciary lacks independence, is there another independent oversight body in place to guard against abusive use of surveillance technology and to what extent is it able to carry out its responsibilities free of government interference?*
- *Is content intercepted during internet surveillance admissible in court or has it been used to convict users in cases involving free speech?*

6. **To what extent are providers of access to digital technologies required to aid the government in monitoring the communications of their users? (0-6 points)**

Note: Each of the following access providers are scored separately:

6a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)
6b. Cybercafes and other business entities that allow public internet access (0-2 points)
6c. Mobile phone companies (0-2 points)

- *Are access providers required to monitor their users and supply information about their digital activities to the government (either through technical interception or via manual monitoring, such as user registration in cybercafes)?*
- *Are access providers prosecuted for not doing so?*
- *Does the state attempt to control access providers through less formal methods, such as codes of conduct?*
- *Can the government obtain information about users without a legal process?*

7. **Are bloggers, other ICT users, websites, or their property subject to extralegal intimidation or physical violence by state authorities or any other actor? (0–5 points)**

- *Are individuals subject to murder, beatings, harassment, threats, travel restrictions, or torture as a result of online activities, including membership in certain online communities?*
- *Do armed militias, organized crime elements, insurgent groups, political or religious extremists, or other organizations regularly target online commentators?*
- *Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such action?*

- *Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property as retribution for online activities or expression?*

8. **Are websites, governmental and private entities, ICT users, or service providers subject to widespread "technical violence," including cyberattacks, hacking, and other malicious threats? (0-3 points)**

- *Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks (e.g. cyber espionage, data gathering, DoS attacks), including those originating from outside of the country?*
- *Have websites belonging to opposition or civil society groups within the country's boundaries been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?*
- *Are websites or blogs subject to targeted technical attacks as retribution for posting certain content (e.g. on political and social topics)?*
- *Are laws and policies in place to prevent and protect against cyberattacks (including the launching of systematic attacks by non-state actors from within the country's borders) and are they enforced?*

CONTRIBUTORS

FREEDOM HOUSE RESEARCH TEAM

- Sanja Kelly, Project Director, Freedom on the Net
- Mai Truong, Research Analyst (Africa) and Staff Editor, Freedom on the Net
- Madeline Earp, Research Analyst (Asia), Freedom on the Net
- Laura Reed, Research Analyst (Eurasia & EU), Freedom on the Net
- Adrian Shahbaz, Research Analyst (MENA & EU), Freedom on the Net
- Ashley Greco-Stoner, Senior Research Assistant (Latin America), Freedom on the Net

REPORT AUTHORS AND ADVISORS

- **Argentina:** Eduardo Andres Bertoni, Director, Center for Studies on Freedom of Expression and Access to Information (CELE), Palermo University School of Law, Argentina; Atilio Grimani, Research Assistant, CELE
- **Australia:** Dr. Alana Maurushat, Senior Lecturer, University of New South Wales
- **Azerbaijan:** Arzu Geybullayeva, Analyst
- **Bangladesh:** Faheem Hussain, Assistant Professor of ICT and Computer Science, Asian University for Women
- **Brazil:** Carolina Rossini, Project Director, Latin America Resource Center, New America Foundation
- **Burma:** Min Zin, Ph.D. Candidate, Department of Political Science, University of California, Berkeley and Contributor, *Foreign Policy* Transitions blog
- **Cambodia:** Sopheap Chak, Program Director of the Cambodian Center for Human Rights and Blogger
- **China:** Madeline Earp, Research Analyst, Freedom on the Net, Freedom House
- **Cuba:** Ernesto Hernández Busto, Cuban journalist and writer based in Barcelona, Spain
- **Estonia:** Linnar Viik, Associate Professor, Estonian IT College
- **France:** Jean-Loup Richet, Researcher, University of Nantes
- **Georgia:** Giga Paitchadze, Blogger
- **Germany:** Dr. Jeanette Hofmann, Research Director at the Alexander von Humboldt Institute for Internet and Society, Berlin and Researcher at the Social Science Research Center, Berlin; Christian Katzenbach, Project Coordinator, and Kirsten Gollatz, Project Manager, Alexander von Humboldt Institute for Internet and Society

- **Hungary:** Borbála Tóth, Independent Researcher; Sandor Orban, Program Director, South East European Network for Professionalization of Media
- **Iceland:** Caroline Nellemann, Independent Consultant and Specialist in Digital Media and Civic Engagement
- **Indonesia:** Enda Nasution, Co-Founder, Sebangsa.com
- **Iran:** Mahmood Enayat, Director, Small Media
- **Italy:** Giampiero Giacomello, Assistant Professor of International Relations, University of Bologna
- **Japan:** Izumi Aizu, Professor and Senior Research Fellow, Institute for InfoSocionomics, Tama University, Tokyo and Executive Director, Institute for HyperNetwork Society, Oita
- **Jordan:** Abeer al-Najjar, Assistant Professor of Journalism and Media Studies, American University of Sharjah
- **Kazakhstan**: Adil Nurmakov, Founder of the "Basta" Citizen Initiative and Editor of the Blogbasta.kz website
- **Kenya:** Grace Githaiga, Kenya ICT Action Network (KICTANet)
- **Kyrgyzstan:** Tattu Mambetalieva, Director, Civil Initiative on Internet Policy (CIIP); Artem Goriyanov, IT Programs Director, CIIP
- **Lebanon:** Dr. Jad Melki, Assistant Professor of Journalism and Media Studies and Director, Media Studies Program, American University of Beirut
- **Malawi:** Vitus-Gregory Gondwe, Senior Reporter for Blantyre Newspapers Limited, Specialist Writer on ICT News for BizTechAfrica.com and Bizcommunity.com
- **Malaysia:** K. Kabilan, Chief Editor, FMTNews.com
- **Mexico:** Alejandra Ezeta, Social Media Consultant at EEB Consultaoria/Ciudadanos en Medios, A.C., Mexico
- **Morocco:** Bouziane Zaid, Assistant Professor of Media and Communication, Al Akhawayn University in Ifrane
- **Nigeria:** 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria
- **Pakistan:** Nighat Dad, Executive Director, Digital Rights Foundation, Pakistan, Lawyer, and Internet Freedom Activist
- **Philippines:** Jacques DM Gimeno, Assistant Professor, Communication Research Department, University of the Philippines-Diliman
- **South Africa:** Alex Comninos, Doctoral Candidate, Justus Liebig University Giessen
- **South Korea:** Yenn Lee, Research Skills Coordinator, School of Oriental and Africa Studies, University of London
- **Sri Lanka:** Nigel V. Nugawela, Independent Writer and Researcher
- **Sudan:** GIRIFNA, a Sudanese non-violent resistance movement
- **Syria:** Mohammad al-Abdallah, Syrian Human Rights Activist and Independent Researcher
- **Thailand:** Sawatree Suksri, Lecturer in Criminal Law and Criminal Procedural Law, Thammasat University, Bangkok

CONTRIBUTORS

- **Turkey:** Yaman Akdeniz, Professor of Law, Istanbul Bilgi University and Founder of Cyber-Rights.org
- **Uganda:** Peter Mwesige, Executive Director, African Centre for Media Excellence (ACME); Grace Natabaalo, Program Associate, ACME; and Ashnah M. Kalemera, Program Officer, Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
- **Ukraine:** Tetyana Lokot, Doctoral Student and Researcher at the Philip Merrill College of Journalism, University of Maryland, College Park
- **United Kingdom:** LSE Media Policy Project, London School of Economics and Political Science
- **United States:** Emily Barabas, Policy Analyst, Center for Democracy and Technology
- **Uzbekistan:** Zhanna Hördegen, Postdoctoral Research Fellow, University Researcher Priority Program Asia and Europe, University of Zurich (at time of writing)
- **Zimbabwe:** Rashweat Mukundu, Journalist, Media and Freedom of Expression Activist, Zimbabwe

The analysts for the reports on Armenia, Bahrain, Belarus, Egypt, Ethiopia, Libya, Russia, Rwanda, Saudi Arabia, Tunisia, the United Arab Emirates, Venezuela, and Vietnam are independent internet researchers who have requested to remain anonymous. Freedom House researchers Madeline Earp, Mai Truong, and Ashley Greco-Stoner provided analysis for the India, Angola, and Ecuador reports, respectively, in consultation with a range of in-country stakeholders. Xiao Qiang, Director of the China Internet Project at the University of California, Berkeley, was an advisor for the China report.

ABOUT FREEDOM HOUSE

Freedom House is an independent private organization supporting the expansion of freedom throughout the world.

Freedom is possible only in democratic political systems in which governments are accountable to their own people, the rule of law prevails, and freedoms of expression, association, and belief are guaranteed. Working directly with courageous men and women around the world to support nonviolent civic initiatives in societies where freedom is threatened, Freedom House functions as a catalyst for change through its unique mix of analysis, advocacy, and action.

- **Analysis:** Freedom House's rigorous research methodology has earned the organization a reputation as the leading source of information on the state of freedom around the globe. Since 1972, Freedom House has published *Freedom in the World*, an annual survey of political rights and civil liberties experienced in every country of the world. The survey is complemented by an annual review of press freedom, an analysis of transitions in the post-communist world, and other publications.
- **Advocacy:** Freedom House seeks to encourage American policymakers, as well as other government and international institutions, to adopt policies that advance human rights and democracy around the world. Freedom House has been instrumental in the founding of the worldwide Community of Democracies, has actively campaigned for a reformed Human Rights Council at the United Nations, and presses the Millennium Challenge Corporation to adhere to high standards of eligibility for recipient countries.
- **Action:** Through exchanges, grants, and technical assistance, Freedom House provides training and support to human rights defenders, civil society organizations, and members of the media in order to strengthen indigenous reform efforts in countries around the globe.

Founded in 1941 by Eleanor Roosevelt, Wendell Willkie, and other Americans concerned with mounting threats to peace and democracy, Freedom House has long been a vigorous proponent of democratic values and a steadfast opponent of dictatorships of the far left and the far right. The organization's diverse Board of Trustees is composed of a bipartisan mix of business and labor leaders, former senior government officials, scholars, and journalists who agree that the promotion of democracy and human rights abroad is vital to America's interests.

1301 Connecticut Avenue, NW; Washington, DC 20036
(202) 296-5101

120 Wall Street, New York; NY 10025
(212) 514-8040

1301 Connecticut Avenue, NW; Washington, DC 20036
(202) 296-5101

120 Wall Street, New York; NY 10025
(212) 514-8040