



FREEDOM ON THE NET 2016

Thailand

34/100

NOT FREE

A. Obstacles to Access	15 /25
B. Limits on Content	12 / ₃₅
C. Violations of User Rights	7/40

Scores are based on a scale of o (least free) to 100 (most free). See the research methodology and report acknowledgements.



Key Developments

- Social media users were put on trial for administering Facebook pages, "liking" posts, and even receiving an antiroyal comment in a Facebook Messenger exchange; decades-long prison sentences were handed down for online activity (see Prosecutions and Detentions for Online Activities).
- Proposed revisions to the Computer-related Crimes Act would permit censorship of any "inappropriate" content or platform and could undermine encryption (see Legal Environment).
- Plans for a single national internet gateway enabling censorship were ostensibly dropped following opposition, though observers remained wary (see Restrictions on Connectivity).
- Penalties in the April 2016 Referendum Act and official threats hampered online discussion of a military-drafted constitution before a national referendum (see Legal Environment).

Introduction

Internet freedom declined in 2016 as the military leadership continued its efforts to codify censorship and surveillance powers through legislation.

General Prayuth Chan-ocha, former commander of the Royal Thai Army, continues to head the junta calling itself the National Council for Peace and Order (NCPO). The period since he seized power in the May 2014 coup has been characterized by increasingly extreme prosecutions of internet users for defamation and criticism of the monarchy. The longest sentence in the history of *lese majeste* cases, 60 years in prison reduced to 30 after a guilty plea, was passed during the coverage period of this report.

Successive governments have blocked tens of thousands of websites in Thailand, but censorship has become more severe and less transparent since 2014. In April, a Referendum Act imposed 10-year prison terms for influencing voters in an August referendum on a draft constitution, chilling online discussion of the document, which

was ultimately approved. Problematic revisions to the Computer-related Crimes Act, the penal code, and other laws are also under consideration. Wide-ranging "digital economy" laws are still pending, despite criticism from academics and internet freedom activists about their implications for privacy and freedom of speech.

Since the coup, journalists, academics, and activists have been subject to overt surveillance, and military officials have interrogated hundreds of people, requiring them to give up their Facebook passwords as a condition of release. Documents leaked during the coverage period documented army and government agencies attempting to procure surveillance equipment as recently as December 2014, which General Prayut Chan-ocha denies. The military leadership was otherwise open about its efforts to step up control of the telecommunications infrastructure, interfering in a spectrum auction through executive order, and developing plans for a single national internet gateway which observers likened to China's Great Firewall.

A. Obstacles to Access

Internet penetration has increased steadily in recent years, in part thanks to affordable government-run access programs, though usage remains concentrated in Bangkok and other urban centers, and speed and quality of service can vary. After the May 2014 coup, officials declared their intention to establish a single gateway to the international internet, potentially enabling them to control or even shut down access nationwide. Plans to strip the regulatory National Broadcasting and Telecommunication Commission of its remaining independence continue to progress.

Availability and Ease of Access

Internet penetration was at 39 percent in 2015, up from 35 percent in 2014. 1 Most Thai internet and smartphone users reside in the Bangkok greater metropolitan and southern regions, which boast a higher average household income. The lowest penetration is in the northeast, in part due to lack of service. 2 Connections functioned at average speeds of 20 Mbps, according to one 2015 report, 3 most reliably in the greater Bangkok area. This represented a significant increase over the 2014 average of 12 Mbps.

Mobile penetration fell from 144 to 126 percent in the same period, in part because of a campaign to disconnect unregistered SIM cards (see Surveillance, Privacy, and Anonymity). The number of active mobile numbers declined by over 10 million in 2015 after providers cleared inactive numbers. A February 2015 Cabinet resolution required registration of all pre-paid mobile users and free Wi-Fi users by July 31, 2015.

The price of mobile data in Thailand has consistently declined since 2008, from THB 1.3 to 0.07 per kilobyte in 2015. **5** Thailand ranks fourth in Southeast Asia, behind Brunei, Singapore, and Cambodia, in terms of affordability, calculated by comparing price to the minimum wage. **6**

The NCPO continued the ICT Free Wi-Fi program initiated under the previous government. Although many users have complained of connectivity issues, such programs help 18 percent of Thai users to access the internet free of charge, while another 16 percent paid less than THB 200 (\$6.73) a month, according to official 2015 figures. 7

In January 2016, the National Broadcasting and Telecommunications Commission (NBTC), Thailand's telecom regulator, and the Ministry of Information and Communication Technology (MICT) announced their collaboration to provide broadband internet access at a reasonable cost to all 70,000 villages nationwide by the end of 2016. The links will be made via both wireless and fixed-line broadband access points. 8

Restrictions on Connectivity

There were no reports of the state blocking or throttling internet and mobile connections for political or security reasons during the coverage period of this report, but the government was developing ways to do so in future by extending state control of the infrastructure.

Within a week of the May 2014 coup, the Deputy Minister of MICT announced plans to establish a "national digital internet gateway" through two state-owned companies, Communication Authority of Thailand (CAT) Telecom and TOT Telecom,

and six other ISPs, with the explicit intention of enabling the MICT to interrupt access directly. **9** Access to the international internet gateway was previously limited to CAT until it opened to competitors in 2006. **10** In a June 30, 2015 resolution, the junta-appointed Cabinet ordered the MICT to proceed with "implementation of a single gateway to be used as a device to control inappropriate websites and flow of news and information from overseas through the internet system." This resolution, and others that reaffirmed it, were not publicized until an internet user found directives describing the policy on government websites in September 2015. **11**

The resolution came under immediate attack from users and experts alike. Many saw it as a Chinese-style "Great Firewall," enabling censorship and personal data collection while undermining speed and security. 12 An online petition opposing the plan attracted over 150,000 signatures in less than two weeks. 13 Many users staged a "virtual sit-in," deliberately crashing government websites by reloading them continuously in their browsers at the same time to simulate a denial of service attack, and briefly disabled websites run by the Office of the Prime Minister, the Defence Ministry, MICT, and CAT Telecom. 14 After two weeks of intense public opposition, Deputy Prime Minister Somkid Jatusripitak said the plan had been halted. 15

Many observers remain wary. In June 2015, the MICT had announced plans to set up a "national broadband company" to consolidate and spearhead the expansion of broadband access, primarily through CAT Telecom, 16 a project which some fear demonstrates that government control over the infrastructure is being expanded anyway. 17 In 2015, *TelecomAsia*, a telecom news website, received leaked documents which suggested that the single gateway project had been a military priority since 2006. 18

Thailand's international bandwidth usage amounted to 2,510 Gbps in February 2016, and domestic bandwidth amounted to 3,510 Gbps, 19 179 percent and 172 percent higher than same month in the previous year respectively.

ICT Market

Although 20 ISPs have licenses to operate in Thailand, high-speed internet is concentrated in a handful of large providers, and the trend points toward more

concentration. According to statistics published in 2014, True Internet—a subsidiary of the communications conglomerate True Corporation, which also controls Thailand's third-largest mobile phone operator True Move—remained the market leader with nearly 40 percent market share, followed by TOT with 31 percent, and 3BB with 29 percent. Other providers serve a fraction of remaining users. 20 In July 2015, the National Telecommunication Commission (NTC), a branch of the NBTC which focuses on telecommunications, deemed that True Internet has "significant dominance" of the fixed-line internet market. The NTC demanded that True submit details of its customers and services in order to determine the appropriate course of action, but had taken no further measures in mid-2016.

The three main mobile phone service providers are the Singaporean-owned Advanced Info Service, the Norwegian-controlled DTAC, and True Move. The first two still operate some spectrum under concessions from state-owned TOT and CAT Telecom, an allocation system that hinders free-market competition.

Regulatory Bodies

The 11-member National Broadcasting and Telecommunication Commission (NBTC), an independent regulator viewed as broadly fair, ²² still managed the industry as of May 2016, but its authority was significantly eroded.

In December 2014 and January 2015, the Thai Cabinet approved a series of draft laws that would establish a Digital Ministry for Economy and Society and a Commission for Digital Economy and Society (CDES). The drafts included proposed amendments to the NBTC law which would transform it from an independent regulator to a government agency under CDES jurisdiction. The CDES would be empowered to penalize noncompliant government or private entities, and take over the allocation of spectrum for state and public interest uses, while the NBTC will only allocate spectrum for commercial use. 23 Many analysts believe this would retard Thailand's spectrum allocation and delay the planned release of spectrum being utilized commercially by military-owned media.

In January 2015, the Cabinet approved changing the ICT Ministry's name to Digital Ministry for Economy and Society—though the original name remains in common

use—and restructuring it in accordance with the subcommittees outlined in the draft digital promotion law: hard infrastructure, soft infrastructure, service infrastructure, digital society, knowledge resources, and digital economy promotion. 24 The draft laws would also transfer assets belonging to the Broadcasting and Telecommunications Research and Development Fund (BTRDF) under the existing NBTC law to a new "Fund for Developing Digital for Economy and Society" (FDDES). While the BTRDF is considered to operate in the public interest, the FDDES would be used to finance digital economy operators, a potential conflict of interest. 25 Furthermore, the draft laws also stipulate that representatives from state-owned TOT and CAT Telecom—which, as telecommunications providers, operate under license from the NBTC—would be appointed to the CDES. This would effectively give the regulated powers over the regulator, undermining the principle of free and fair competition. 26

Civil society and private sector actors called the laws obstructive, and criticized the focus on creating new agencies with broad powers. After much public outcry (see "Digital Activism"), the government established the Preparation Committee for Digital Economy and Society chaired by junta leader General Prayuth Chan-ocha in lieu of the CDES. 27 At its first meeting in February 2016, the Committee approved the 20-year Digital for Economy and Society Development Plan. 28 New versions of the digital economy laws were still being drafted in mid-2016.

In April 2016, the Thai Cabinet approved a new frequency act that, if it becomes law, will formally strip the NBTC of independence, placing it under the jurisdiction of the Commission for Digital Economy and Society (CDES) chaired by the Prime Minister. The new National Broadcasting and Telecommunications Act calls for a single sevenmember NBTC board (reduced from two five-member boards for broadcasting and telecommunications, plus one chairman). A committee consisting of high-ranking members of the judiciary and bureaucrats will select candidates for the board which the new Digital Economy Ministry will forward to the senate for approval; the Prime Minister will have the final say. 29 On May 31, 2016, the proposed law was pending review in the junta-appointed National Legislative Council.

The NBTC's failing authority was already evident. After issuing an order in July 2014 to delay a pending 4G spectrum auction for one year, 30 the NCPO finally allowed the 900MHz auction to go ahead in December 2015. The newcomer Jas Mobile Broadband (JAS), a subsidiary of Jasmine International, won the first licence block by quoting THB 75.6 billion, while True Move H Universal Communication (TUC) of True Corporation won the second block at THB 76.3 billion. The final price per capita MHz was described as one of the highest in the world. 31 After JAS defaulted on its instalment payment for the license in January 2016, junta leader General Prayuth Chan-ocha invoked Clause 44 of the interim constitution, commonly known as the "absolute power" clause, since it is final and cannot be appealed under any court. He ordered the NBTC to hold a new auction for the same spectrum on May 27, 2016, with a reserve price of THB 75.6 billion to match the JAS winning bid. The order also stated that the current spectrum holder, Advanced Info Services Plc. (AIS), could continue to serve its customers until June 30, or until the NBTC grants license to the new winner, whichever comes first. 32 AIS, the only bidder, readily won the auction at the reserve price. 33

B. Limits on Content

Since the May 2014 coup, both the NCPO and the junta-appointed government have issued orders that prohibit online content perceived to criticize the Thai monarchy, the NCPO, or the government. Amendments to the Computer-related Crimes Act (CCA) under consideration during the coverage period would cement that practice. Self-censorship by journalists and social media users continued amid fresh warnings not to debate a draft constitution in advance of a national referendum. Despite more pervasive censorship and pressure from the authorities, online platforms allowed dissidents and activists to organize in opposition to the CCA amendments and other repressive developments, with some success.

Blocking and Filtering

During the reporting period, online censorship by the NCPO and MICT continued under NCPO orders issued after May 2014 coup. NCPO Announcement no. 17/2014 ordered ISPs to monitor and prevent dissemination of any information that distorts

facts, could provoke disorder, or affects national security. **34** In January 2015, the NBTC, in its role as regulator, requested that every ISP monitor and censor online content that may cause conflict or disrupt peace and order. **35** These orders empowered public officials at any level, as well as ISP employees, to block websites directly using their own judgment. As a result, there are no longer official censorship statistics.

Prior to the 2014 coup, the process to block websites was more rigorous, though it still lacked transparency. Article 20 of the 2007 Computer-related Crimes Act (CCA) authorizes MICT officials to request court orders to block content that is deemed a threat to natural security, or contravenes public morals or public order. **36** The government also censored content under special laws, such as the State of Emergency Act and Internal Security Act, which it invoked in 2010. The Thai government has been blocking some social and political content since 2007, though some controls on pornography, gaming, and other topics were announced earlier. **37**

In April 2016, a revised draft of the amended CCA was submitted to the National Legislative Assembly. Clause 20(4) would allow the government, under a newly established "computer information screening committee," to remove any online content or platform, including social media platforms such as Facebook and Line, if they are deemed "inappropriate," even without violating any law. ³⁸ In addition, the amended Clauses 15 and 20 said the ICT Ministry would mandate decryption protocols to allow the government to access, block, or delete encrypted content. ³⁹ There was strong opposition to the draft, which remained under review at the end of the coverage period (see Digital Activism).

Content that was most censored after the coup falls into two main categories: criticism of the Thai monarchy, and criticism of the NCPO or junta-appointed government. Blocked websites include foreign news websites such as Reuters and the UK-based *Daily Mail* newspaper; websites of human rights groups such as Human Rights Watch; academic websites such as Midnight University; personal websites of political bloggers and activists; and many Facebook and YouTube pages that contain anti-coup material. 40 None of the affected content was unblocked during the

reporting period. Facebook was blocked entirely by MICT for about half an hour six days after the coup. 41

The military government has also been ramping up its technical censorship capacity. One of the biggest developments in the past two years was the plan to route all internet traffic through a single internet gateway, dubbed by critics the "Great Firewall of Thailand" (see Restrictions on Connectivity). Although the government appeared to back down after intense public opposition, observers fear that the government may still be trying to consolidate gateway traffic through state-owned CAT Telecom to facilitate censorship and surveillance.

Content Removal

As with blocking, takedown requests were expedited and decentralized after the coup. The new process is highly unsystematic and uncoordinated. Arrests and intimidation frequently result in content removal (see Media, Diversity, and Content Manipulation, Prosecutions and Detentions for Online Activities, and Intimidation and Violence).

The CCA allows the prosecution of content providers or intermediaries—such as webmasters, administrators, and managers—accused of posting or allowing the dissemination of content considered harmful to national security or public order. This potential liability encourages compliance with content removal requests. A draft law governing materials that incite dangerous behavior would also hold access providers liable for failing to remove such material from their systems if they know it exists (see Legal Environment). Announcement no. 12/2014 ordered social media users and operators to limit content that incites violence or provokes protests or opposition to NCPO rule. 43

Companies also restrict access to some content. In early 2016, Facebook restricted access within Thailand to "GuKult," a satirical page that sometimes makes fun of the monarchy, replacing it with a message that read, "You're unable to view this content because local laws restrict our ability to show it." 44

Facebook's "report" feature, which allows users to flag content which violates the site's terms, is separately used as a tool to temporarily suppress content. In 2015 and 2016, Facebook users and page administrators periodically complained that their content had been removed during harassment campaigns waged by other users, indicating that their opponents had reported it for contravening community guidelines, requiring them to appeal to the platform to have it reinstated.

Media, Diversity, and Content Manipulation

NCPO content regulations have increased self-censorship and undermined the diversity of information available on the internet in Thailand.

NCPO Announcement no. 18/2014 banned news reporting that disrupts national security, peace, and order. 45 Journalists, editors, and media personalities who report stories that are critical of the government or NCPO are routinely summoned for "attitude adjustment" with the military, which can last up to seven days without charge under NCPO Announcement no. 3/2015. As a result, mainstream media outlets and reporters by and large choose to self-censor. In February 2016, the ministry of foreign affairs issued new guidelines for foreign journalists working in Thailand for longer than three months, introducing discretionary powers to deny visas for disrupting public order or the security of the kingdom," in language similar to NCPO orders regulating Thai media. 46

The minority who still attempted to convey criticism of the NCPO continued to face harassment during the coverage period. Notable cases include Pravit Rojanaphruk, then-senior reporter at *The Nation* (he later moved to *Khao Sod English*), who was blindfolded and taken to an undisclosed location for three days of interrogation in September 2015. He was told that his offense was "tweeting and posting comments questioning the legitimacy of the NCPO and its leader." **47** After the coup in 2014, Pravit was also summoned for seven days. Separately, in October 2015, Sakda Sawlew, the political cartoonist known as Sia who draws for Thailand's largest daily newspaper, *Thai Rath*, was "invited" to report to army headquarters to discuss his critical cartoons, which are frequently shared online. **48** This was also the second time he had been summoned.

Ordinary internet users were warned not to discuss a constitution drafted by the military in advance of a national referendum to approve its adoption, threatening the diversity of opinions online. In March 2016, General Teerachai Nakvanich, army chief and secretary-general of the NCPO, ordered an "immediate crackdown" on any action the government believes will lead people to "misunderstand" or be "confused" about the government's work before the referendum, which was scheduled for August. 49 A law passed in April 2016 governing the referendum process carries harsh prison terms for "influencing" voters, undermining freedom of expression (see Legal Environment). However, social media platforms like Facebook and Twitter still offered a vital platform for Thai people to express their opinions and criticize the government (see Digital Activism).

There was no public documentation of paid actors manipulating political content on the internet during the coverage period, though there were organized efforts to restrict political engagement online. Officials offered financial incentives to citizens to monitor one another online (see Surveillance, Privacy, and Anonymity), and many organized informally to harass the junta's opponents (see Intimidation and Violence).

A number of outspoken activists and academics have fled Thailand since the coup, but remain active on social media. For example, Somsak Jiamteerasakul and Pavin Chachavalpongpun, two prominent academics, relocated abroad and continue to publish commentaries and political analysis via Facebook. Being physically outside the country allows them to be more outspoken.

Digital Activism

Social media platforms such as Facebook and Twitter, chat applications such as Line, and online petition sites such as Change.org have become indispensable as more Thais access the internet. Since the coup, many bloggers, activists, and human rights lawyers have formed coalitions such as Thai Lawyers for Human Rights (TLHR) to monitor the situation and document human rights violations by the junta. Anonymously operated Facebook pages allow individuals to share their opinions and organize political activities, including *Stop Fake Thailand*, which has over half a million followers.

Two recent online campaigns are notable for their success in rallying users to defend internet freedom. The Foundation for Internet and Civic Culture (Thai Netizen Network) gathered over 20,000 signatures opposing the junta's draft digital economy laws in February 2015, leading the government to announce that the drafts would be improved. 50 Separately, a Change.org campaign set up in September 2015 to oppose the "single gateway" plan attracted over 150,000 signatures in less than two weeks, prompting the deputy prime minister to announce that the plan had been scrapped, though observers remained sceptical (see Restrictions on Connectivity).

A third campaign was ongoing in mid-2016. A user-mounted campaign to oppose amendments to the Computer-related Crimes Act (see Blocking and Filtering) had gathered over 34,000 signatures as of June 30. 51

C. Violations of User Rights

Internet users, bloggers, citizen journalists, and independent media practitioners continued to face persecution in 2015 and 2016. In addition to problematic draft digital laws that remain pending, legislation to suppress materials that incite dangerous behavior, as well as amendments to the CCA and the penal code could further erode internet freedom. The longest prison sentences for criticizing the monarchy were documented during the reporting period, and dozens of people were detained or interrogated for legitimate online speech.

Legal Environment

Clause 45 of the Constitution of the Kingdom of Thailand 2007 guaranteed broad freedom of speech, but was replaced with a 2014 interim constitution after the May coup d'etat. Although it maintains the same safeguards, Thailand remains subject to various NCPO orders which prohibit individuals and the media from any public political activity.

Internet users are frequently charged under Clause 14 of the 2007 Computer-related Crimes Act (CCA), pertaining to content that affects national security, and Clause 112 of the criminal code pertaining to *lese majeste*, or criticism of the monarchy.

Defamation is a criminal offense under the penal code, and Clause 14(1) of the CCA

criminalizes "bringing false computer information into the system," which has been used to punish alleged libel (see Prosecutions and Detentions for Online Activities).

Many NCPO decrees and orders criminalize speech, and NCPO announcements 37/2014, 38/2014, and 50/2014 also expanded military court jurisdiction over civilians, including violations of Clause 116 of the penal code, the equivalent of sedition, which punishes actions that "aim to change the government, create unrest amongst people, or cause people to transgress the law" with a maximum seven years' imprisonment. Clause 116 has been used to charge politicians, human rights defenders, students, and individuals who peacefully express critical opinions of the junta government. At least 47 people were arrested under the clause between the coup and the end of this coverage period, and several were subsequently charged and sentenced. 52

The military court has no appellate or higher division, and has handed down more severe punishments than civilian judges. In *lese majeste* cases judged between 2010 and 2015, regular courts handed down average jail terms of 4.4 years out of a possible 3-15 years. Sentences issued by martial courts are much higher. In August 2015, separate military courts in Bangkok and Chiang Mai found two internet users guilty of *lese majeste* over Facebook posts, and handed down jail terms of 60 and 58 years respectively before guilty pleas reduced the final verdicts. These marked the highest imprisonments ever recorded in Thailand for *lese majeste* offences (see Prosecutions and Detentions for Online Activities). **53**

Military control was further entrenched during the coverage period. On March 29, 2016, General Prayuth Chan-ocha issued NCPO Announcement no. 13/2016, allowing military officers and anyone appointed by the junta leader to arrest anyone who commits one of 27 categories of crimes, including those considered to involve threats to "public peace." They can also carry out search, seizure, and any other act instructed by the NCPO, with impunity. 54 Local and international human rights organizations feared the order will be used to silence dissent. 55

In April, the Referendum Act was introduced to govern a national referendum on a draft constitution scheduled for August. Clause 62 punishes anyone "deceiving, forcing, or influencing a voter" with up to 10 years' imprisonment or fines up to THB 200,000. 56 Critics said this broad wording effectively criminalized free speech and

campaigning. **57** In June, after the coverage period of this report, the Constitutional Court upheld the law, **58** and the referendum approved the military-drafted constitution in August. **59**

The digital economy package of 10 draft laws was still under consideration during the coverage period (see Regulatory Bodies). 60 The draft Commission for Digital Economy and Society (CDES) law stipulates that CDES would have authority over every other ministry and government agency, including the power to initiate disciplinary action against any government official or citizen that does not comply with their orders. 61 The draft cybersecurity law would also grant authorities lawful interception powers without a warrant, based on a perceived threat which is not properly defined.

A revised criminal procedural law also pending before the National Legislative Council separately grants surveillance powers to authorized police officials. The draft stipulates a wide range of offenses for which surveillance is lawful; in addition to violations of national security and organized crime, it includes very broad categories like "complex" crimes. 62

Under a separate draft law for the prevention and suppression of materials that incite dangerous behavior, officials would require a warrant to access any private information that is deemed to provoke dangerous behavior such as sexually deviant acts, child molestation, or terrorism. Creating and distributing such information would be punishable by one to seven years in prison and fines up to THB 700,000. Access providers (as defined by the CCA) that know such information exists in the computer system under their control but fail to remove it also face a maximum 5-year jail term and THB 500,000 fine. 63

A revised draft of the amended Computer-related Crimes Act was also submitted to the National Legislative Assembly in April 2016, sparking opposition (see Blocking and Filtering). At the end of the coverage period, all of these draft laws were under review pending submission to the National Legislative Assembly.

Besides the problematic content of these laws, critics called the lawmaking process—which lacked participation from relevant stakeholders or public hearings—rushed

and secretive. The Electronic Transactions Development Agency director, who heads the legal drafting team, said the top-down drafting process resulted from the urgency of the policy for the interim government. 64

Prosecutions and Detentions for Online Activities

Prosecutions and detentions of internet users increased in frequency and became more extreme during the reporting period, as military or police officers interpreted even symbolic acts of dissent as national security threats violating the CCA and various NCPO announcements.

Four cases stand out as examples that suppressed freedom of speech in Thailand's online space:

- Eight internet users were arrested in April 2016 and charged under Clause 116 of the penal code and Clause 14 of the CCA. They collectively ran "We Love Gen Prayut," a satirical Facebook page with over 70,000 followers famous for popularizing memes and doctored photos of General Prayut Chan-ocha accompanied by satirical quotes. They were denied bail by the military court; the case was pending trial in mid-2016. 65
- Thanakorn, a 27-year-old factory worker, was arrested on December 8, 2015 for sharing infographics on Facebook linking General Prayut Chan-ocha and other NCPO members to a scandal involving Rajabhakti Park. Media reports have accused high-level army officers of accepting kickbacks during construction of the park, newly built on army-owned land in Prachuab Kiri Khan province to honor past Thai kings. 66 Thanakorn was held at an undisclosed location for seven days, raising fears over his disappearance, 67 then charged with violating the CCA and Clause 116 of the penal code. He was additionally accused of committing lese majeste for "liking" a Facebook page deemed to contain lese majeste content, and for posting a sarcastic comment under an image of the royal dog. 68 He was released on THB 500,000 bail in March 2016, after 86 days in custody. His case is pending trial in the military court, and marks Thailand's first prosecution for "liking" content on Facebook. 69 Separately, Jaem (pseudonym) was arrested in November 2015 for violating the CCA and Clause 116 of the penal code, for alleging on Facebook that several high-ranking

- members of the NCPO are implicated in the Rajabhakti Park corruption scandal. She was released from custody on THB 100,000 bail. In mid-2016, a military prosecutor was still considering whether to bring the case to trial. **70**
- Theerawan Charoensuk, 57, was arrested in Chiang Mai on March 29, 2016 under Clause 116 of the penal code. Theerawan had shared a photo of herself on Facebook, holding a red water bowl and a Thai New Year poster from former Prime Ministers Thaksin and Yingluck Shinawatra. The photo was also printed in the daily *Thai Rath*. Theerawan said she found the poster and bowl in a temple where she was participating in a religious ceremony. She was released on THB 100,000 bail pending military trial in mid-2016.
- Patnaree Chankij, the mother of a prominent student activist, was charged with lese majeste for "failing to criticize or take action against lese majeste comments" made by a friend of her son in a private exchange on Facebook Messenger. The military court granted THB 500,000 bail, and her case was pending trial in mid-2016.

Internet users were also sentenced during the coverage period:

- On August 7, 2015, military courts in Bangkok and Chiang Mai sentenced a man and a woman to 30 and 28 years in prison respectively, in separate cases involving Facebook posts deemed critical of the monarchy. The sentences were reduced from 60 and 56 years after the defendants pleaded guilty. The court sentenced Pongsak (pseudonym) to 10 years in prison for each of 6 Facebook posts, 73 while Sasivimol (pseudonym) was convicted to 8 years in prison for 7 posts. 74 The Office of the United Nations High Commissioner for Human Rights called them the highest sentences imposed for *lese majeste* since they began documenting them in 2006. 75 Police also arrested Chayo (pseudonym), an individual in Pongsak's Facebook Messenger contacts, on the same charge based on private statements and photos deemed *lese majeste*. 76 In December 2015, the military court in Srakaew province sentenced him to 18 years in prison, reduced to 9 years after he entered a guilty plea.
- In July 2015, a Bangkok military court sentenced each of the eight alleged members of an online "antimonarchy network" to five years in prison. Two other people who were deemed sympathizers got three-year sentences. 77 In

early 2015, the Department of Special Investigations, which is tasked with identifying and tracking down anonymous online authors of content deemed *lese majeste*, announced that it had broken up the so-called "Banpot Network", which they accused of distributing hundreds of podcasts with information and political commentary critical of the royal family over the past three years, including its alleged founder, Hassadin "Banpot" Uraipraiwan.

- Thanes (pseudonym) has been in custody since July 2014 for allegedly sending a link to *lese majeste* content to a foreigner by email in 2010. In June 2015, a criminal court sentenced him to 5 years in prison, reduced to 3 years and 4 months for offering useful testimony. **78**
- Piya (pseudonym) was accused of publishing lese majeste content on a
 Facebook account in December 2014, though he denied operating the account.
 In January 2016, a criminal court sentenced him to 9 years in prison, reduced to 6 years for offering useful testimony.

Besides *lese majeste* and political speech, libel is a longstanding problem in Thailand. Clause 14(1) of the CCA criminalizes "bringing false computer information into the system." Suing people under this clause concurrently with the charge of libel has become the norm. Attorney generals and judges have shown no understanding of the differences between the two laws, nor the fact that "false computer information" means technical crimes such as hacking, not the veracity of online speech. The vast majority of plaintiffs in these cases are government officials or large corporations.

During the reporting period, at least one court demonstrated an improved understanding of the Computer-related Crimes Act, acquitting a *Phuketwan* editor and journalist sued by the Royal Thai Navy for re-publishing a Pulitzer prize-winning Reuters article accusing Navy officials of profiting from a refugee smuggling ring. Editor Alan Morison and reporter Chutima Sidasathian were charged with criminal defamation and an offence under the CCA. On September 1, 2015, the court acquitted both accused on all counts, ruling that the CCA was not intended to be used in defamation cases. The website shut down in 2015 because of the uncertainty during the trial, 80 and in May 2016 had not been restored.

Another case also saw a more positive outcome, though still based on a misinterpretation of the false information clause. Maitree, a citizen journalist of Lahu ethnic descent, was sued by the military for violating Clause 14(1) of the CCA. On January 1, 2015, he videotaped an incident in his village in which a villager was slapped by a soldier, then shared the footage on his personal Facebook account. The military alleged that he violated Clause 14 because the content of the video clip was "false information" that damaged the reputations of the soldiers involved. On March 9, 2016, a criminal court in Chiang Mai acquitted Maitree, saying he posted the video clip because he believed it was true; his action would be an offense under Clause 14(1) only if "he was aware that the information he posted were false."

However, these two court verdicts remain a minority in the overall trend of courts handing out guilty verdicts under the CCA for supposedly libelous online content. For example, Natural Fruit, a canned fruit company, sued migrant labor rights activist Andy Hall over dissemination of research reports that allege violations of labor rights in the company's plants. The company sued him in three separate cases, one of which uses the computer-related crimes law because the report was disseminated online. The cases were being tried in a criminal court during the reporting period; ⁸² in September 2016, Hall was sentenced to a suspended three-year prison term and a THB 150,000 fine. ⁸³

As in past years, a number of computer crimes charges filed against journalists or public persons for alleged libel were dropped or dismissed, suggesting they lacked merit, but were filed to intimidate the defendant. In August 2015, a criminal court in Mae Sot indicted Suraphan Rujichaiwat, a community-based human rights defender from Loei Province, on charges of criminal defamation and violating Clause 14(1) of the CCA. Suraphan was sued by Tungkhum, a mining company in dispute with the community about its environmental impact. The plaintiff dropped the charge in March 2016. 84 In December 2015, the same company sued Wanpen Khunna, a 15-year-old student in Loei province who had helped document the mine's impact on villages for ThaiPBS, Thailand's public broadcaster. 85 In mid-2016, the case was pending trial.

Surveillance, Privacy, and Anonymity

A number of NCPO decrees and orders specifically mandate surveillance of online media. NCPO order no. 26/2014 mandated surveillance and monitoring of social media by military agencies. 86 Pending draft laws also include provisions that will grant police and other agencies overbroad surveillance powers (see Legal Environment).

Thai government officials frequently announce that they are monitoring private communication on chat applications such as LINE, **87** and actively seeking cooperation from social media platforms such as Facebook. In 2015, Facebook reported that it received three user requests from the junta government, but produced no data in response. **88** In May 2016, following the arrests of eight Facebook page administrators (see Violation of Users Rights), Facebook reiterated that it had not shared users' private communications with the junta. **89**

Internet users and journalists have reported that the Department of Special Investigations is pursuing an aggressive surveillance policy, joining private chat groups on the social messaging service LINE, creating Facebook accounts in order identify the authors of "illegal" messages, and even "baiting" some people to criticize the monarchy or the junta in order to arrest them. **90** In several cases where individuals were summoned or arrested, the authorities confiscated smartphones to peruse personal information and photos, or check for potential links to other people.

In June 2014, Somyot Poompanmuang, Deputy Commissioner of the Royal Thai Police, publicly invited Thai people to "serve as eyes and ears" of the state by submitting images of anti-coup symbols displayed in public and online to police. He offered a monetary reward of THB 500 for photos that result in an arrest. He also urged the public to inform the police via the *Jah Hook* ("Owl Sergeant") Facebook page. 91 The Cyber Scout program, which began in 2011 under the ICT and education ministries, trains students to monitor and report online behavior they deem a danger to national security. In 2015, there were over 120,000 cyber scouts nationwide, spanning 88 schools. The curriculum stresses recruiting new members and training cyber scout leaders. 92

During the reporting period, several revelations shed more light on the inner workings of Thailand's technical surveillance apparatus. In July 2015, leaked internal

documents belonging to Milan-based Hacking Team revealed that a number of government agencies in Thailand bought spyware from them between 2012 and 2014. Those agencies included the Royal Thai Police, the National Security Council, the Royal Thai Army, and the Department of Corrections under the Ministry of Justice. Correspondence between National Security Council and Hacking Team revealed that the Thai intelligence wanted the ability to eavesdrop on popular messaging programs, especially Line, Skype, and WhatsApp. 93 Police spokesman Pol. Lt. General Prawut Thawornsiri said reports of the 2012 deal with Hacking Team were "groundless" because "surveillance on citizens was illegal and ran counter to national police agency policy." 94 General Prayut Chan-ocha, who was head of the Royal Thai Army at the time the procurement was approved, also denied the reports. According to emails documented in the leak, the Royal Thai Army was in the process of buying spyware worth EUR 360,000 as of December 2014. 95 The company's Remote Control System software would give the junta the ability to intercept communications, remotely activate a mobile phone's microphone and camera, and access all of the phone's content including contacts and messages without the user's knowledge. 96

From August 2015 onwards, users of pre-paid mobile phone cards and free Wi-Fi nationwide in Thailand must be registered pursuant to a February 2015 Cabinet resolution. Every user must supply their full name and ID or passport number, or lose service. Partly as a result of this blow to online anonymity, the number of mobile numbers in Thailand declined during the reporting period (see Availability and Ease of Access). **97**

Intimidation and Violence

In addition to charging internet users, the NCPO uses extrajudicial measures to intimidate its opponents. In one prominent 2016 case, Sarawut Bamrungkittikhun, administrator of the Facebook page *Peod Praden* ("Open Issue"), which is critical of the junta government, was abducted from his residence in Surat Thani province, his laptop and mobile confiscated, transported to Bangkok and held in an undisclosed military barracks for seven days. 98 Sarawut subsequently terminated his Facebook page.

After the May 2014 coup, the NCPO summoned hundreds of people for questioning in order to suppress potential dissent, often through public announcements in the media. Summons to "attitude adjustment" at military barracks continued in 2015 and 2016, but were made via phone calls or by post. The NCPO also diversified their intimidation methods, making repeated home visits unannounced, threatening family members, or issuing mandatory "invitations" for coffee or meals. During interrogations, individuals reported being required to sign written agreements promising not to voice political opinions or criticize the NCPO. A number of people were ordered to reveal their Facebook passwords. 99

In 2015, at least 234 people were summoned or visited by the military. Watana Muangsook, a politician with the Pheu Thai party of former Prime Ministers Thaksin and Yingluck Shinawatra, was summoned multiple times without charge after expressing disagreements with the junta on Facebook, including over the draft constitution.

Alleged violations of national security or *lese majeste* laws prompted persecution from fellow internet users as well as the state. Ultra-royalist groups increasingly organize online to track down people they deem to have insulted the monarchy, often filing criminal charges against them. "Rubbish Collection Organization," a group of ultra-royalists led by Maj. Gen. Rientong Nan-nah, wages witch-hunt campaigns on Facebook; its targets are often ostracized socially and lose their jobs. The organization asks Thais based abroad to help track down "fugitives," and post their addresses online to facilitate further harassment, and has threatened to sue Facebook for allowing *lese majeste* content. 102

Technical Attacks

There have been sporadic reports of hacking attacks on online news outlets in Thailand in the past. None were documented during the coverage period of this report, though hackers did target government sites. In October 2015, the international hacking collective Anonymous hacked websites of several Thai government agencies, including the Royal Thai Police and CAT Telecom, to express their opposition to the junta's single gateway plan. 103

Footnotes

- International International Telecommunication Union, "Percentage of Individuals Using the internet, 2000-2015," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
- Telecommunications Data and Research Center, "Report on the Survey of Thai People's Telecom Behavior 2012-2013," (in Thai) The National Broadcasting and Telecommunication Commission, http://www.nbtc.go.th/wps/PA_WCMLocalRendering/jsp/html/NTC/download/NB....
- "Thailand Internet 8th Fastest in Asia," Bangkok Post, May 21, 2015, http://www.bangkokpost.com/tech/local-news/568859/thailand-internet-8th.... Akamai reported average connection speed was 10.8 Mbps and average peak connection speeds of 69.6 Mbps in 2016. http://akamai.me/2ewzRnD.
- 4 NBTC, "Telecommunications industry: 2015 Q3 summary overview" (The National Broadcasting and Telecommunications Commission, September 2015), http://bit.ly/2fvJnfp.
- NBTC, "Internet Market Report: Price/Kbps," http://www.nbtc.go.th/TTID/internet_market/price_kbps/.

More footnotes (+)





On Thailand

See all data, scores & information on this country or territory.

See More >

Country Facts

Global Freedom Score

36/100 • Partly Free

Internet Freedom Score

39/100 Not Free



Be the first to know what's happening.

Join the Freedom House weekly newsletter



ADDRESS

1850 M St. NW Floor 11 Washington, DC 20036 (202) 296-5101

@2024 FreedomHouse

GENERAL INQUIRIES info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org