Freedom House

FREEDOM ON THE NET 2020

Thailand

NOT FREE

35 /100

A. Obstacles to Access	16 /25
B. Limits on Content	12 /35
C. Violations of User Rights	7 /40

LAST YEAR'S SCORE & STATUS

35 /100 Not Free

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

Overview

The internet is severely restricted in Thailand. A repressive emergency declaration issued in response to the COVID-19 pandemic imposed further constraints on freedom of expression, and the authorities arrested and criminally charged internet users who criticized the government's public health policies. Meanwhile, physical violence and enforced disappearances targeting prodemocracy and antimonarchy activists, as well as human rights defenders, continued during the coverage period. Many people nevertheless defied the country's strict lèse-majesté laws by openly criticizing the monarchy online in 2019, and such speech persisted in the context of prodemocracy street protests in 2020.

In March 2019, Thailand held elections for the first time since a 2014 military coup overthrew its democratically elected government. The election process was widely considered to have been designed to prolong and legitimize the military's dominant role in Thailand's governance. The new, nominally civilian government, again headed by Prime Minister Prayut Chan-o-cha, the former army chief and coup leader, took office in July 2019 and continues to restrict civil and political rights and suppress dissent.

Key Developments, June 1, 2019 – May 31, 2020

- The government continued compelling social media platforms to remove content that criticized the monarchy; it also directly pressured social media users to delete their posts (see B2).
- In a rare development, a group of internet users publicly criticized the monarchy on social media in 2019, foreshadowing 2020 protests calling for democratic change and reform to the monarchy (see B4 and B8).
- In November 2019, the Ministry of Digital Economy and Society established an Anti-Fake News Center to combat what the government considers to be false

and misleading information that violates the repressive Computer Crime Act (see B5, C3, and C5).

- In response to the COVID-19 pandemic, the government activated an Emergency Decree on Public Administration in a State of Emergency, restricting both online free expression and press freedom and providing state officials with broader power to arrest and prosecute users (see C1 and C2).
- Internet users were arrested, criminally charged, or subjected to targeted harassment for sharing a range of content, from unverified information about the pandemic to commentary criticizing the government's response (see C3 and C7).
- Enforced disappearances and physical violence aimed at prodemocracy and antimonarchy online activists remained a major concern during the coverage period (see C7).

A. Obstacles to Access

Internet access is considered affordable. While penetration has been steadily increasing, there remains a significant urban-rural divide. The government has worked to install free Wi-Fi access points in underserved areas, but their reach remains limited. The political leadership has continued efforts to tighten control over technical infrastructure as well as telecommunications regulatory bodies. A handful of large providers dominate the telecommunications and internet service markets, and all are either government controlled or thought to have close links with the authorities.

A1 0-6 pts	
Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**5**/6

Internet access is improving in Thailand, particularly as increasing numbers of users go online via mobile phones. According to the Digital 2020 Report, developed by creative agency We Are Social and the social media management platform Hootsuite, as of January 2020 Thailand's internet penetration rate was at 75 percent with 52

million users, a 2 percent increase in the number of users from January 2019. [1] The Inclusive Internet Index 2020, a project of the *Economist,* ranks Thailand 29 out of 100 countries in terms of availability, determined by quality and breadth of available infrastructure. [2]

Mobile internet penetration continues to steadily increase. By January 2020, 97 percent of internet users accessed the internet using a mobile phone, compared with 94.7 percent in 2018. [3] In contrast, 53.6 percent of users in December 2019, down from 56 percent in December of the previous year, accessed the internet through laptop and desktop computers, according to available statistics. [4]

Thailand's international bandwidth usage amounted to 10,988 Gbps in February 2020, and domestic bandwidth amounted to 8,126 Gbps, [5] about 39 percent and 13 percent higher than the same month in 2019, respectively.

In February 2020, three private mobile service providers and two state-owned telecommunications firms offered bids worth a total of 100 billion baht ($3.3 billion) for spectrum required to set up fifth-generation (5G) mobile service infrastructure. [6] Following a successful bid, Advanced Info Service (AIS) was the first mobile service provider to launch its 5G network. [7]

A2 0-3 pts	
Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**2**/3

Disparities in internet access persist, largely based on socioeconomic class and geographical location.

However, the cost of access has continued to decrease. About 56 percent of internet users spend 200 to 599 baht ($7 to $20) per month to access the internet, while 21 percent pay under 200 baht per month. Nearly 11 percent of the population access the internet through free programs. [8] Some observers expected the rollout of 5G service to increase internet accessibility due to lower costs, [9] but the 5G spectrum

licenses cost the bidding companies more than anticipated, [10] and it remains to be seen whether this cost will be transferred to internet users. [11]

Government programs have sought to reduce the persistent digital divide between urban and rural areas. [12] Initiated in early 2016 by the then Ministry of Information and Communication Technology (MICT) and the National Broadcasting and Telecommunications Commission (NBTC), the Return Happiness to the Thai People program aimed to provide broadband internet via wireless and fixed-line access points in rural areas at reasonable costs. As of December 2017, the Ministry of Digital Economy and Society (MDES) and the state-owned TOT Public Company Limited had installed Wi-Fi hotspots in 24,700 villages. [13] However, several specifications in the contract were not met, including through the use of Chinese instead of Thai fiber-optic lines, discrepancies in mandated download speeds, [14] and requests for a significantly higher budget than anticipated. [15]

In February 2020, the MDES informed TOT that it had to resolve the problems within three months or risk losing the contract to the private sector. [16] Meanwhile, the intended reach of this program had been extended by the NBTC to an additional 15,732 villages in rural areas and 3,920 villages in border areas, [17] with the new work scheduled for completion by March 2020, though there were no updates by the end of the coverage period. [18] The program also includes recruiting and training of people to work with villagers to develop information and communication technology (ICT) skills. [19]

A3 0-6 pts	
Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**5**/6

There were no reports of the state blocking or throttling internet or mobile connections during the coverage period, though the government does have some technical control over the internet infrastructure.

CAT Telecom, a state telecommunications provider, operates international telecommunications infrastructure, including international gateways and connections

to submarine cable networks and satellites. [20] Access to the international internet gateway was limited to CAT until it opened to competitors in 2006. [21]

Authorities continued with a plan to merge CAT and TOT, both of which are owned by the state. The merger received regulatory approval in May 2019, [22] and the new entity, National Telecom, was set to launch in July 2020 after the proposal was approved by the cabinet in January 2020; this could be delayed, however, due to friction between the management teams at CAT and TOT. [23] While the merger was intended to help the public firms compete with private telecommunications companies, [24] it was also seen as part of the government's plan to consolidate its control over the country's telecommunication infrastructure.

Since 2006, the military has prioritized a "national internet gateway" that would allow Thai authorities to interrupt internet access and the flow of information at any time. [25] With the Thai military having handed power to a nominally civilian government following the March 2019 elections, it is unclear whether this controversial "single gateway" will be implemented. [26]

The National Cybersecurity Act of Thailand centralizes authority over public and private service providers in the hands of government entities (see C5). This law classifies information technology and telecommunications companies as Critical Information Infrastructure (CII) under Section 49, and also grants the National Cybersecurity Committee (NCSC) the ability to identify additional companies or organizations as CIIs. [27] Various committees established under the act, consisting primarily of government representatives, are given broad powers over CIIs to address perceived threats to national security and public order, terms which remain undefined. [28] Although restricting connectivity is not explicitly mentioned, the law makes it easier for authorities to compel service providers to comply with their orders in relation to what those authorities could broadly consider to be a risk to national security, among other provisions. [29]

The law does not provide transparency concerning government decisions and lacks an effective system of accountability if connectivity restrictions were to be implemented. For example, if the government defines a threat as "crisis level," the

highest level as defined by the act, a court would only need to be informed after authorities take any action that they deem necessary in response. [30] There are no clearly defined criteria to guide the government's determination of what could be a crisis-level threat, and there is no independent monitoring of or publicly available reporting on the law's implementation. [31]

A4 0-6 pts	
Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**4**/6

High-speed internet packages are concentrated among a handful of large providers. Though many are privately owned, a 2017 report by the United Kingdom–based organization Privacy International found that authorities have long held "close relationships with private telecommunication companies and ISPs [internet service providers] through appointments which starkly exemplify the revolving door between the government and the private telecommunications sector." [32]

Although 20 ISPs have licenses to operate in Thailand, the largest three controlled almost 86 percent of the market in 2019. TRUE Online led the sector with 37.5 percent toward the end of 2018. Jasmin followed with 32.4 percent, and state-owned TOT retained third place despite seeing its market share fall to 16.1 percent. [33] AIS, Thailand's top mobile service provider, which entered the fixed-line broadband market in 2015, accounted for 9.5 percent. [34]

Two developments during the coverage period could shake up ISPs' market positions. First, the Bangkok Metropolitan Administration (BMA) reportedly provided TRUE Corporation with a sole 30-year concession for moving overhead telecom and television cables underground within two years, a move that some have argued could greatly benefit TRUE in the telecom industry. [35] However, in September 2019, the NBTC reportedly asked the BMA to open a new request for proposals, citing a misunderstanding in the original process. [36] The second development, the purchase and distribution of 48 5G spectrum licenses in February 2020, could also alter market shares (see A1). AIS and TRUE purchased 23 and 17 licenses, respectively, with TOT

purchasing four, and Total Access Communication (DTAC) and CAT both purchasing two. [37]

For the mobile sector, AIS held a market share of about 43.5 percent toward the end of the third quarter of 2019. TRUE held 32 percent, and Norwegian-controlled DTAC followed with 21.7 percent. [38] AIS and DTAC operate some spectrum under concessions from state-owned TOT and CAT—an allocation system that does not entirely enable free-market competition.

A5 0-4 pts	
Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**0** / 4

Following the 2014 coup, the military junta—known as the National Council for Peace and Order (NCPO)—implemented reforms to the regulatory bodies overseeing service providers and digital technology that reduced their independence, transparency, and accountability.

The NBTC, the former regulator of radio, television, and telecommunications, was stripped of its authority, revenue, and independence when the junta-appointed National Legislative Assembly (NLA) passed the NBTC Act in 2017. It endures as a government agency at half its original size, authorized to implement policy set by a commission led by the prime minister and other new entities with overlapping functions.

The MDES was established by the NLA in 2016 to replace the MICT and is responsible for implementing policy and enforcing the Computer Crime Act (CCA) (see C2). [39]

The Commission for Digital Economy and Society (CDES) provides directives to the MDES and is responsible for formulating policy under the 2017 Digital Development for Economy and Society Act (DDA). [40] Chaired by the prime minister, the CDES is composed of government ministers and no more than eight qualified experts. [41] It is stipulated as a legal entity, not a government body, absolving it of accountability under laws that regulate government agencies, though it has authority over the MDES and the NBTC. The commission operates through the Office of the National

Digital Economy and Society Commission. Section 25 of the DDA calls for the NBTC to transfer revenue to the office "as appropriate."

The DDA redirects up to 5 billion baht ($165 million) of NBTC licensing revenue toward a new Digital Economy and Society Development Fund, a legal entity broadly authorized to regulate policy and receive profits from business joint ventures or its own operations. The act also effectively replaced a public body, the Software Industry Promotion Agency, with another broadly empowered entity, the Office of Digital Economy Promotion (ODEP). Like the CDES, neither the fund nor the ODEP is classified as a government body accountable to the public, leading to serious concerns about transparency and conflicts of interest.

The NBTC's nomination committee is composed of seven people holding various bureaucratic and judicial positions affiliated with the government. Candidates are vetted by the Senate secretariat and endorsed by the unelected Senate. Candidates are no longer required to have specific expertise in telecommunications, broadcasting, or other relevant fields per a January 2019 decision by the junta, though in effect they were already selected based on their rank in the government, military, or police, rather than relevant professional experience. NBTC commissioners are paid extremely well and have significant influence over the multibillion-baht telecom business. [42]

The government in turn has significant influence over the decisions of the NBTC. For example, the NBTC temporarily suspended the media broadcaster Voice TV in 2014, 2017, and most recently in February 2019, and then required it to comply with restrictions on reporting critical information about the government. [43] In response to the 2019 ban, the Administrative Court declared the suspension invalid and called on the NBTC to be politically neutral and respect free expression. [44]

In April 2018, the NLA rejected all 14 candidates proposed by the NBTC nomination committee. [45] Following the vote, the head of the NCPO suspended the nomination process under Section 44 of the interim constitution, which is not subject to appeal, mandating that the previous commissioners continue in their roles. It was expected

that the NBTC Act would be amended in July 2020, after which new commissioners would be selected. [46]

In 2019 and 2020, additional bodies have been or will be established to operationalize Thailand's Cybersecurity Act and Personal Data Protection Act (PDPA). The Cybersecurity Act established the NCSC, the Cybersecurity Regulating Committee (CRC), the Office of the National Cybersecurity Committee, and the Committee Managing the Office of the National Cybersecurity Committee (CMO). [47] The NCSC develops policy, guidelines, and a code of practice, while the CRC with the support of the CMO administers these policy products. [48] More than half of the members that make up these committees are government officials, with individuals from the same government bodies or authorities occupying positions in all of them, effectively limiting checks and balances and restricting opportunities to ensure accountability and independence. [49] In January 2020, the expert members of the committees were selected in order to prepare for the implementation of the Cybersecurity Act. [50]

In 2020, the Personal Data Protection Committee will be established to implement the PDPA, which is expected to come into force in 2021 (see C6). [51] The 16-member committee allows for the selection of nine honorary directors and one chairperson based on their expertise, while the remaining members are government officials. [52] The act calls for the selection of committee members to be carried out in a fair and transparent manner, but it does not explicitly guarantee that the committee's decisions are taken independently or subject to independent oversight.

B. Limits on Content

The government restricts critical content online by blocking webpages and virtual private networks (VPNs), and by requesting that major companies like Google, Twitter, and Facebook remove content from their platforms on the grounds that it violates the country's restrictive laws. Progovernment disinformation continues to proliferate online, and users self-censor on various topics. However, after the coverage period in the summer of 2020, protesters used social media to organize street demonstrations that included rare calls to reform the monarchy.

B1 0-6 pts	
Does the state block or filter, or compel service providers to block or filter, internet content?	**3**/6

The blocking of content deemed critical of the monarchy is widespread, but a lack of transparency means that the full extent of this blocking is unclear. Websites have also been blocked on grounds of national security, for gambling content, for alleged violations of intellectual property rights (IPR), and for hosting unauthorized VPN services. [53]

In December 2018, the police's Technology Crime Suppression Division (TCSD) reported that it had asked the MDES to block more than 1,500 websites that year, in most cases for gambling or IPR violations. [54] Also that month, the NBTC and the Royal Thai Police established the Center of Operational Policing for Thailand against Intellectual Property Violations and Crimes on the Internet Suppression (COPTICS) to streamline the process of blocking websites found to have violated IPR. [55] As of January 2019, COPTICS had received requests to block 1,080 URLs with IPR violations alleged against them. Only 89 were successfully blocked, with 991 URLs remaining unblocked. [56] The NBTC's secretary general explained that it was not successful in blocking certain URLs because they were encrypted under the HTTPS protocol and were made inaccessible by foreign-based content generators or platform hosts. [57] The same official reported that the commission sought assistance from the United States and Japan to help block 788 encrypted URLs based in those countries. [58]

Thailand has never publicly revealed the number of URLs blocked by court orders. Members of the public often learn that a URL is blocked when they are denied access to the website. For example, in September 2019 users reported that Somsakwork.blogspot.com, a blog written by prominent Thai historian and exiled activist Somsak Jeamteerasakul, was unavailable due to "improper or illegal content in breach of the Computer Crime Act 2017." The blog was later accessible for some but not all users. [59] In May 2017, the Thai Internet Service Providers Association (TISPA) said its members blocked access to over 6,300 URLs pursuant to NBTC

orders citing threats to national security, a category that can include lèse-majesté content, pornography, and gambling, among other types of material. [60]

Some blocks affect entire websites, not just the URLs for individual articles or posts. Researchers tested 1,525 URLs on six ISPs between November 2016 and February 2017, and found 13 websites completely blocked. [61] At least one news website, the United Kingdom's *Daily Mail*, was blocked at the domain level by TOT and 3BB. Websites offering tools for online anonymity and circumvention of censorship, as well as VPNs, are also blocked by more than one ISP. [62] The study revealed significant inconsistencies across providers, suggesting that some may implement discretionary restrictions without prior authorization. The website of the VPN Hotspot Shield, [63] for example, was blocked by the ISP TRUE but otherwise available, while Ultrasurf, another VPN, was blocked by DTAC, AIS, and 3BB as of June 2020.

B2 0-4 pts	
Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?	**0** / 4

Like blocking and filtering, content removal continued under the tight control of the government during the coverage period. Users are often pressured by authorities to remove content, while content providers or intermediaries often comply with removal requests to avoid criminal liability (see B3).

Between July and December 2019, Facebook restricted access to 958 posts after receiving reports from the MDES alleging that the content violated Section 112 of the criminal code on lèse-majesté and Section 14(3) of the CCA on threats to national security. [64] According to Google's transparency report, the government sent 25 requests from July to December 2019 to remove 1,238 items across various Google services, including YouTube. [65] All of the requests were related to criticism of the government or the monarchy.

Content targeted for removal or blocking by social media platforms includes speech on political, cultural, historical, and social topics. After the coverage period in August 2020, amid a series of prodemocracy protests, Facebook blocked Thai-based users'

access to the Royalist Marketplace, a group created on the platform in April by the self-exiled academic and monarchy critic Pavin Chachavalpongpun, after receiving a legal demand from the MDES. [66] The group had more than a million users and featured discussions about the country's king. After blocking domestic users' access to the content, Facebook announced that it would legally challenge the order. [67]

In another example, a June 2019 Facebook post that was shared by Somsak Jeamteerasakul, a historian living in exile who also discusses the monarchy, and that included a historical document discussing Queen Sirikit, the current king's mother, was evidently blocked only for users in Thailand. [68]

Users, publishers, and content hosts are pressured and intimidated to remove content. In June 2019, a French satirist living in Bangkok was pressured to remove a music video mocking the NCPO's anthem from his social media accounts. Police officers visited his house and ordered him to sign a memorandum stating that such content was "improper" and damaged Thailand and its people. [69] During the same month, a comedian and a group of high school students were also pressured by authorities to remove or apologize for social media content that criticized or joked about the junta.

In November 2019, a Twitter user was arrested after she posted using the hashtag #royalmotoracade to criticize the royal family's motorcade for blocking traffic (see B4). [70] Police interrogated her about her posts, including content shared by other prodemocracy student activists. Officers made her delete previous posts and sign an agreement stating that she would not post about the monarchy (see C7). [71] In March 2020, a policeman was forced to remove a parody TikTok video mocking Prime Minister Prayut Chan-o-cha and was placed in solitary confinement as a punishment. [72]

Ahead of the March 2019 general elections, the Election Commission of Thailand (ECT) set up a special unit to monitor for online posts that it deemed to be spreading misinformation and inflammatory content. When such content was found, the ECT would call on those involved to remove it, or ask platforms such as Facebook, Google, and the messaging app LINE to do so within two days. [73] Under Sections 73(5) and

159 of the Organic Law on the Election of Members of Parliament and the ECT's Election Campaign Regulation, respectively, authors of such content can also be punished with prison terms of up to 10 years and banned from politics for 20 years. [74] While these provisions were only used to file petitions against members of opposition parties, the ECT ordered the removal of content from both pro- and anti-NCPO parties, most of which was deemed to be false information about parties or candidates. [75]

B3 0-4 pts	
Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**0** / 4

Restrictions on online content lack transparency, and those penalized do not have access to an independent appeals process. While authorities do ask courts to block content, the judiciary in practice grants requests without scrutiny. [76] In addition, both the Anti-Fake News Center and the COVID-19-specific emergency declaration allow authorities to issue correction notices for online content (see B5 and C1). [77]

Amendments to the CCA that took effect in May 2017 could empower more bodies to advance blocking requests and could expand the kind of content subject to blocking. Section 20 of the CCA authorized MDES officials to request court orders to block content that is deemed a threat to national security or found to contravene public morals or public order. The 2017 amendments established a nine-member, ministry-appointed "computer data screening committee" that may also authorize officials to apply for court orders to block content. Three of its members must be from the media, human rights, and information technology sectors. Section 20(3) appears to authorize the committee to order restrictions on content that threatens public order or morals even if the content does not actually violate any law, meaning courts could be asked to issue orders to block legal content at the discretion of a committee that is not accountable to the public. [78] In August 2019, a meeting was organized for the selection of committee members, [79] but the conclusion of this meeting and details on the selection process have not been made publicly available. [80]

In July 2017, a decree expanding on the amended Section 20 was enacted. It states that service providers must abide by court orders to block access to websites using technical measures. [81] The final draft of the decree was an improvement from an earlier draft, which had said that ISPs are required to take a proactive role in censorship and use "whichever means necessary" to block content.

Under the 2007 CCA, providers or intermediaries are subject to prosecution for allowing the dissemination of content considered harmful to national security or public order. [82] The 2017 amendments provide some protection for intermediaries through a notice-and-takedown system. They also require rules and procedures for takedown requests and clearly grant immunity to "mere conduits" and cache operators.

Despite these positive developments, the amendments still contain considerable scope for abuse. The amended CCA appears to hold individuals responsible for erasing banned content on personal devices, though how this rule might be enforced remains unclear. Section 16(2) states that any person knowingly in possession of data that a court has found to be illegal and ordered to be destroyed could be subject to criminal penalties. [83] Analysts argued that the language could lead to the destruction of archival data, but there was no clear case of the provision being enforced since the law became effective in 2017.

Another MDES decree in July 2017 further modified intermediary liability. [84] It established a complaints system for users to report banned content and also incentivized intermediaries to act on every complaint to avoid liability. After receiving notice, intermediaries must remove flagged content within seven days for alleged false or distorted information, within three days for alleged pornographic content, and within 24 hours for an alleged national security threat. There are no procedures for intermediaries to independently assess complaints. There is also an onerous burden on content owners: to contest removal, owners must first file a complaint with police and then submit that complaint to the intermediary, which has final authority over the decision. Both companies and content owners who do not comply face imprisonment of up to five years.

The decree's 24-hour window to remove national security–related content disregards a 2013 court ruling that 11 days is an acceptable amount of time for removing content relating to national security. [85] In addition, the decree requires that intermediaries determine the legality of content, which could cause intermediaries to ultimately remove any content they think could result in a lawsuit—prioritizing protecting themselves over the public's right to know. Some feedback from intermediaries regarding the MDES decree has been cautiously optimistic, particularly relating to the clear set of procedures and the relief of some burden to proactively monitor and remove content. However, there have been no cases on the decree's implementation as of yet.

In September 2020, after the coverage period, the MDES filed a legal complaint against Twitter and Facebook for not complying with takedown requests. [86]

B4 0-4 pts	
Do online journalists, commentators, and ordinary users practice self-censorship?	**1** / 4

Thailand's restrictive political environment encourages self-censorship online. Legal sanctions for activity such as criticizing the government or businesses on Facebook and Twitter are frequently imposed (see C3). The government has also made it known that it monitors social media to control political expression, [87] issuing repeated threats on the consequences of sharing such information. For example, in 2020 authorities threatened prison time for sharing information deemed false about COVID-19, including on April Fools' Day. [88] Users who express dissenting views have faced online harassment and intimidation or had their personal information shared and private lives scrutinized (see C7). Such reprisals can have a chilling effect, contributing to self-censorship online.

Most Thai internet users self-censor on public platforms when discussing the monarchy because of the country's severe lèse-majesté laws (see C2). In February 2019, news circulated that the opposition Thai Raksa Chart Party would nominate Princess Ubol Ratana, the older sister of King Maha Vajiralongkorn, as its candidate for prime minister ahead of the elections. Users only discussed the development in

private online conversations, such as in closed Facebook and LINE groups, and not on public platforms; Thai news outlets and journalists also refrained from reporting on it. Local outlets only began covering the story after Ubol Ratana's candidacy was officially announced, presumably to avoid committing lèse-majesté. [89]

However, between late 2019 and early 2020, several hashtags questioning the monarchy went viral on Twitter, [90] including one that criticized the blocking of traffic by a royal motorcade. Another reacted to the absence of moral and financial support from the king while the country was overwhelmed with the pandemic; it was shared over 1.2 million times within 24 hours. In response, while not directly addressing it, Minister of Digital Economy and Society Buddhipongse Punnakanta warned people against breaking the law online, issuing a Twitter post that included an image of handcuffs. [91]

B5 0-4 pts	
Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	**1** / 4

Online propaganda, disinformation, and content manipulation are relatively common in Thailand. State entities and some political parties are believed to engage in such practices using a variety of means to target the opposition, human rights defenders, and certain segments of the population. Official efforts to combat disinformation are allegedly selective, allowing pro-government campaigns to proceed with impunity.

Manipulated, false, or misleading online content proliferated during the 2019 election period. Most such content aimed to discredit opposition parties and prominent figures like Thanathorn Juangroongruangkit, then the leader of the progressive Future Forward Party (FFP) and its candidate for prime minister. A September 2019 report from the Oxford Internet Institute identified Thailand as having coordinated "cybertroop" teams whose full-time staff members are employed to manipulate the information space on behalf of the government or political parties. [92] The report found evidence that such teams have undergone formal training and work to support preferred messaging, attack political opponents, and suppress critical content.

Fake accounts in Thailand, which may be either automated or run by humans, most often manipulate content on Facebook and Twitter. Some of the websites, Facebook pages, and news outlets putting out false content and doctored files around the 2019 elections linked back to the News Network Corporation (NNC), [93] whose previous chairman was a member of the NCPO. A few days before the vote, a dubious audio recording was circulated on social media, purportedly indicating that Thanathorn had conspired with the self-exiled former prime minister Thaksin Shinawatra. Internet users proved that the clip was doctored after it was aired by Nation TV Channel, a pro-NCPO outlet under NNC. [94]

In February 2020, the opposition Move Forward Party—which became a successor to the FFP after the latter was dissolved by the Constitutional Court that month—accused the government of running an online information operation, pulling funds from the budget of the Internal Security Operations Command (ISOC), the political arm of the Thai military with the prime minister as its chair. [95] The campaign was reported to feature online accounts that harassed and defamed the opposition, human rights defenders, and activists, including those involved in the peace process in the country's south. Reporting also highlighted a suspicious online blog that shared information intended to increase hate between Buddhists and Muslims. [96] Evidence of the campaign included official ISOC documents, a video interview with an alleged former officer, and records of conversations from a LINE group in which participants discussed deploying fabricated social media accounts to target government critics. [97] ISOC admitted that the documents supporting the allegations were authentic, but claimed that the operation was merely a public relations exercise meant to address fake news. [98]

In November 2019, the MDES established the Anti-Fake News Center to combat false and misleading information that violates the CCA, particularly Sections 14(2) and 14(3) (see C2). [99] The center is staffed by 30 officials and has a broad mandate to review information, including that which relates to natural disasters, the economy, health products, illicit goods, government policies, and any other content affecting "peace and order, good morals, and national security." [100] The center also includes staff from the state-owned telecommunications firms TOT and CAT. [101] In addition to identifying content deemed to be misleading or damaging to the country's image, the

center disseminates what it deems to be "corrections" through its website, social media accounts (including an official LINE account), and various news outlets. [102]

Some observers, including leaders of the FFP, have noted that the government does not work to combat disinformation targeting opposition parties. [103] Instead the Anti-Fake News Center has targeted users who post content that is critical of those in power (see C3). The coverage period saw examples of incorrect labelling of false or misleading information. In February 2020, the Anti-Fake News Center labelled a Khaosod news story as fake. The article discussed the government's quarantine policy for those returning from the United Kingdom amid the COVID-19 pandemic, citing information obtained from the Facebook page of the Thai embassy in London. [104] The center later clarified that the article was incorrectly labelled as false due to a procedural error.

B6 0-3 pts	
Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**2**/3

Many outlets struggle to earn enough in advertising revenue to sustain themselves, limiting their ability to publish diverse content. A draft bill circulated during the coverage period could allow the imposition of large fines for ethics violations, which would further limit outlets' resources; the bill also contains language that would incentivize a wide variety of outlets to register with authorities.

The draft legislation in question, the Bill on the Promotion of Media Ethics and Professional Standards, originally proposed as the Media Reform Law, was approved by the cabinet in December 2018; [105] it was pending before the Senate as of January 2020, [106] and had yet to pass at the end of the coverage period. It would create a national professional media council tasked with issuing codes of conduct to journalists and media outlets. [107] The council would also rule on complaints and could impose fines of at least 1,000 baht ($33) per day on a legal media entity or at least 100 baht ($3) per day on a journalist. The bill includes a vague definition of media that can be interpreted to include social media pages and anyone routinely

publishing to a wide audience. [108] The draft gives the prime minister authority over its implementation, including through the issuance of ministerial regulations.

The NBTC has previously signaled its intent to scrutinize the amount of advertising revenue digital media receive in comparison to traditional broadcasters, [109] as well as their use of the network infrastructure of telecommunications companies. In April 2019, in the face of criticism from users and experts, the NBTC scrapped a plan to tax over-the-top (OTT) service providers by imposing a surcharge based on the amount of bandwidth used. [110] Instead, a bill proposed in parliament in June 2020 would require foreign digital service providers to pay a value-added tax of 7 percent on sales, if they earn more than 1.8 million baht ($59,500) annually. [111]

Similarly, the MDES discussed the development of regulatory guidelines for OTT businesses in Association of Southeast Asian Nations (ASEAN) member states at the 2019 ASEAN Telecommunication Regulators' Council. [112] The guidelines, expected to be completed in 2020, [113] could include revenue collection in all ASEAN countries and a new center to supervise and filter content. [114]

B7 0-4 pts	
Does the online information landscape lack diversity?	**2** / 4

Score Change: The score improved from 1 to 2 due to a modest increase in the diversity of content in recent years, including from news outlets and across social media.

The diversity of viewpoints available online has been limited by the enforcement of restrictive laws, policies, and practices, including those specifically aimed at controlling online content, as well as by content removals, economic restrictions, and self-censorship (see B2, B4, B6, and C3). Nevertheless, social networks and digital media provide opportunities for sharing information that would typically be restricted in traditional media, and Thailand has a relatively vibrant social media environment.

According to the Digital 2020 Report by Hootsuite and We Are Social, there were about 52 million social media users in Thailand by the end of 2019. The most popular platform that year was Facebook, followed by YouTube, LINE, and Instagram. [115] Given the offline restrictions on free expression and freedoms of assembly and association, civil society groups, activists, and politically engaged younger netizens have turned to social media to express opinions and garner support for democracy and human rights. [116]

The Chinese state-run Xinhua News Agency has news-sharing partnerships with various Thai media groups, such as Voice Online, Manager Online, Sanook, the Matichon Group, and the state broadcasting agency, National Broadcasting Services of Thailand (NBT). Xinhua translates articles into Thai to be shared on the websites of partner organizations, thus broadening the reach of Chinese state news reports and potentially limiting diversity of content. [117] However, the actual degree of influence this material has among Thai news consumers remains unclear.

B8 0-6 pts	
Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**3** / 6

Social media, chat applications, and online petition sites are available and serve as essential tools for digital activism, though the risk of criminal charges and targeted harassment or violence has discouraged such activism in practice (see C3 and C7).

Online discussions and digital activism on issues related to the monarchy are typically quite rare (see B4). However, beginning in February and into August 2020, after the coverage period, protests that included student leaders called for reform of the monarchy. Social media platforms were fundamental to the organization and mobilization of these demonstrations (see B2). [118] For example, a hashtag that translates as "If politics were good" trended across Twitter, spurring discussion about what politics could look like in the country if the political situation were more stable and democratic. [119]

The June 2020 disappearance of Thai activist Wanchalearm Satsaksit in Cambodia contributed to the growth in online activism, particularly among the younger generation, with the hashtag #SaveWanchalearm remaining popular more than a month later. [120]

Users are also quite active on Change.org. In early 2019, over 70,000 people signed a petition calling for the Thai government to reject the Bahraini government's request for the repatriation of Hakeem al-Araibi, a Bahraini soccer player and political refugee with residency in Australia. [121]

During the campaign period leading up to the March 2019 elections, vague and restrictive rules imposed by ECT limited the use of digital tools for political activism. [122] The rules required parties to notify ECT of what content they would publish and when. They also restricted the type of content that can be posted on social media, allowing only candidates' names, photos, party affiliations, party logos, policy platforms, slogans, and biographical information. Parties and candidates could not "like" or share content about other candidates that was deemed defamatory or false. Violations could draw up to six months in jail, a fine of up to 10,000 baht ($330), or both. [123] Some candidates, such as the Pheu Thai Party's prime ministerial candidate, Sudarat Keyuraphan, resorted to deactivating their Facebook pages to avoid potential punishment. [124] After the elections, in April 2019, the ECT sued seven activists for defamation pertaining to a Change.org petition. [125] The page accused the commission of cheating and questioned the actions of some commissioners, ultimately garnering 865,000 signatures. [126]

C. Violations of User Rights

Forced disappearances of Thai prodemocracy and antimonarchy activists in neighboring countries continued to be reported, while people inside Thailand faced physical violence and intimidation as a result of their online activities. Internet users were also charged and imprisoned for their online speech during the coverage period. COVID-19 emergency provisions restricted free expression and were used to arrest several people for their social media posts.

C1 0-6 pts	
Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	**0** / 6

Score Change: The score declined from 1 to 0 due to pandemic-related restrictions on free expression and press freedom online under the Emergency Decree on Public Administration in a State of Emergency, as well as the judiciary's continued lack of independence.

The constitution drafted by the military government following the 2014 coup went into effect in April 2017, months after it was approved in a tightly controlled national referendum. It replaced an interim constitution, also introduced by the junta. However, Section 44 of the interim constitution, which gave the NCPO unchecked powers to issue any legislative, executive, or judicial order without accountability, remained in force until the new government—headed by incumbent prime minister Prayut Chan-o-cha—took office in July 2019, following the elections that March. [127]

The 2017 constitution enshrined basic rights, but Section 25 stipulates that all rights and freedoms are guaranteed "insofar as they are not prohibited elsewhere in the constitution or other laws," and that the exercise of those rights must not threaten national security, public order, public morals, or any other person's rights and freedoms.

During its four-and-a-half-year term, the NCPO-appointed government passed a number of laws to consolidate its power. Many have reduced the efficiency and transparency of independent regulators and government agencies in the name of "reforming" bureaucracy and the media.

The 2005 Emergency Decree on Public Administration in a State of Emergency restricts both online free expression and press freedom. The decree, which was activated in March 2020 in response to the COVID-19 pandemic, provides officials with broader power to take action against users who spread online content that is deemed to be a threat to state security, peace and order, or public morality, as well as

content that amounts to "deliberate distortion of information which causes misunderstanding." [128] The law imposes criminal penalties and allows authorities to order journalists, news outlets, and media groups to "correct" reporting that authorities deem incorrect (see C2).

Thailand's judiciary is independent under the constitution, but in practice the courts suffer from politicization and corruption, and they often fail to protect freedom of expression. For example, the Constitutional Court has summoned users for posting critical content about the judiciary online (see C3). [129] In an important indicator of the judiciary's general lack of independence, the Constitutional Court disbanded the opposition FFP in February 2020. [130]

C2 0-4 pts	
Are there laws that assign criminal penalties or civil liability for online activities?	**0** / 4

A number of laws impose heavy criminal and civil penalties for online activities, and police and the attorney general's office continued to pursue criminal charges that clearly infringed on basic rights during the coverage period.

A revised CCA was adopted in December 2016 and took effect in May 2017. Among other changes, it altered Section 14(1) of the original 2007 law, which banned introducing false information into a computer system; experts understood this to refer to technical crimes such as hacking. [131] Judges, however, showed limited understanding of this application, and the clause was widely used in conjunction with libel charges to prosecute speech. Observers say this interpretation enabled strategic lawsuits against public participation (SLAPPs), in which government officials and large corporations initiated cases in order to intimidate and silence their critics. Lawmakers sought to curb this abuse by adding new language that excluded the measure's application in conjunction with defamation offenses. [132] Nevertheless, the revised law retained the problematic term "false" computer information, and added another, "distorted" computer information. As a result, the incorrect interpretation of the law persists, and individuals continue to face charges for publishing allegedly false content on the internet (see C3). A study by the Human Rights Lawyers' Association

concluded that between 1997 and May 2019, about 25.47 percent of SLAPP cases related to online speech. [133]

The revised CCA also extended the scope of online censorship and altered the legal framework for intermediary liability (see B3). Other problematic sections of the original CCA went unchanged, including Section 14(3), which criminalizes online content deemed to "affect national security."

The country's criminal code imposes additional penalties for legitimate online activities (see C3). Sedition is covered under Section 116, and lèse-majesté is covered in Section 112, for example.

In response to the COVID-19 pandemic, the prime minister declared a state of emergency from March 26, 2020. [134] Regulations issued under the state of emergency criminalized the presentation or dissemination of news "through any media featuring content on the communicable disease Coronavirus 2019 (COVID-19) which is false or may instigate fear among the people, or to intentionally distort information which causes misunderstanding of the emergency situation to the extent of affecting the public order or good moral of the people." [135] Those in violation can be charged under the CCA or under Section 18 of the 2005 Emergency Decree, which stipulates that any person convicted would face up to two years in prison with a fine of less than 40,000 baht ($1,300). [136] Several individuals have since been arrested and charged using the provision (see C3).

Legislation that was pending during the coverage period included the Bill on the Promotion of Media Ethics and Professional Standards, which could limit both press freedom and online speech by imposing fines of up to 50,000 baht ($1,700) for any outlet deemed to have violated media ethics. The draft was the subject of a public consultation with the Senate in early 2020 (see B6). [137]

Under a separate draft law for the prevention and suppression of materials that incite "dangerous behavior," creating and distributing information deemed to provoke behavior such as certain sexual acts, child molestation, or terrorism would be punishable by one to seven years in prison and fines of up to 700,000 baht ($23,000). [138] The draft was still pending at the end of the coverage period.

C3 0-6 pts	
Are individuals penalized for online activities?	**1** / 6

Authorities continued to exploit Section 14 of the CCA, the criminal code, and other broadly worded laws to silence opposition politicians, activists, human rights defenders, and civil society groups during the coverage period. Law enforcement agencies have also used the Anti-Fake News Center and the pandemic-related emergency declaration to arrest internet users. In May 2020, a new cyberpolice unit with 1,700 officers was approved to monitor for cybercrimes, including those related to "fake news." [139]

In December 2019, the internet user Nathee was sentenced to three years in prison, later reduced to two years. He was originally arrested in September 2018 under Sections 14(3) and 14(5) of the CCA and Section 116 of the criminal code for posting a picture of King Rama IX with a comment on Facebook. [140] Nathee died by suicide, on his third attempt, in April 2020; the court had rejected his argument that the case should be dismissed in light of his bipolar disorder. [141] In February 2020, 26 other individuals were informed of CCA charges against them for sharing a Facebook post that was critical of the prime minister and deputy prime minister Prawit Wongsuwan. [142]

There has been a surge in arrests for what authorities view as "fake news," particularly since the establishment of the Anti-Fake News Center (see B5). [143] Prodemocracy activist Karn Pongphrapan was arrested and charged under the CCA in October 2019 for sharing a Facebook post highlighting the violent fates suffered by various foreign monarchies. Karn later deleted the post and his social media account. As of July 2020, he was out on bail of 100,000 baht ($3,300) and awaiting trial. [144] If convicted, he faces up to five years in prison.

In another case, a Twitter user called Niranam was arrested in February 2020 for posts about the king. Arrested by 10 officers, both he and his parents were interrogated for six hours without being presented with a warrant or charges. He was

later charged under Section 14(3) of CCA and eventually released on bail of 200,000 baht ($6,600). [145] In June 2020, the prosecutor decided not to move forward with the case, [146] but days later Niranam was charged with more counts under the CCA and summoned for interrogation. If convicted, he faces up to 40 years in prison. [147]

A number of users were arrested and charged under the March 2020 emergency decree for sharing information about COVID-19 or the government's response to the pandemic. [148] At least six people were arrested and detained in February 2020, in some cases before an arrest warrant was issued, for sharing unverified information about the spread of COVID-19 in the country. [149] In March, the TCSD arrested two more people for sharing on Twitter that a person had died of COVID-19 in a Bangkok shopping mall. [150] In April, another three people were arrested and had their phones confiscated for claiming on Facebook that a 24-hour curfew was going to be imposed. [151]

In a case centered on criticism of the government's COVID-19 response, Thai artist Danai Ussama was arrested in March 2020 after stating on Facebook that he and other passengers arriving from Spain did not go through any screening process at Suvarnabhumi Airport. He was charged under Section 14(2) of CCA and released on bail; [152] the case was pending at the end of the coverage period. [153] Separately, police sought to question the administrator of the investigative Facebook page Queen of Spades about posts alleging corruption around a mask-hoarding scandal. [154] The businessman accused of hoarding the masks as well as a politician from the governing Palang Pracharath Party filed complaints against the page administrator. [155]

Users also faced arrest for social media activity associated with the pro-democracy protests in July and August 2020, after the coverage period (see B8). The MDES filed a cybercrime complaint against Pavin Chachavalpongpun, the exiled academic and creator of the Facebook group Royalist Marketplace (see B2). [156] Members of the group have reportedly been targeted with additional CCA complaints as well as intimidation and harassment (see C7). [157]

The judiciary in Thailand uses the threat of contempt of court charges to intimidate those who criticize its actions online. On August 2019, the Constitutional Court summoned professor Kovit Wongsuwarat for questioning after he posted disapproving comments about a court decision. [158] The court later decided not to proceed with contempt charges.

Private companies and individuals often file defamation cases against human rights defenders, activists, and journalists for their online activities. The Thai poultry company Thammakaset Co. Ltd. launched cases against several individuals in 2019 and 2020 for sharing allegations of labor rights violations or even expressing support for other defendants targeted by the company in defamation cases. In December 2019, former Voice TV reporter Suchanee Rungmuanporn was sentenced to two years in prison for criminal defamation under Section 328 of the criminal code. Thammakaset filed the case against her in response to a Twitter post that discussed a complaint filed with the National Human Rights Commission by migrant workers. [159] She was released on bail of 75,000 baht ($2,500) pending an appeal against the judgment. [160]

In October 2019, Thammakaset initiated a criminal defamation case against former National Human Rights Commission member Angkhana Neelapaijit for sharing two Twitter posts in support of women human rights defenders facing defamation charges filed by the company. [161] In June, Thammakaset filed two new criminal complaints against Angkhana Neelapaijit. [162] Hearings on the cases were expected later in 2020. [163]

In December 2019, a human rights researcher for Fortify Rights, Puttanee Kangkun, was charged with criminal defamation for sharing similar posts across Facebook and Twitter. [164] A former communications associate for Fortify Rights was also charged for sharing Twitter posts. [165] Both cases were ongoing at the end of the coverage period.

Ordinary voters and party candidates faced CCA charges during the 2019 election period. [166] Nine internet users were charged that March for sharing “false” information about the ECT, [167] with the police claiming that they had confessed. [168]

Three politicians from the opposition FFP—Thanathorn Juangroongruangkit, Klaikong Vaidhyakarn, and Jaruwan Saranket—were charged in February 2019 after criticizing the junta in a Facebook Live broadcast, though the charges were dropped in March 2020. [169] Pongsakorn Rodchompoo, another FFP politician, was charged for sharing a doctored photo aimed at discrediting junta member and deputy prime minister Prawit Wongsuwan. As of June 2020, the prosecutor had yet to bring official charges, and the case was still under investigation. Pongsakorn said he deleted the photo three minutes after posting when he realized it was fake. [170] The FFP party spokesperson, Pannika Wannich, faced charges in two separate cases under the CCA; one was filed in December 2019 over an altered image of the prime minister's Children's Day slogan, [171] and the second was filed in March 2020 for a 2013 Facebook post on the monarchy. [172]

There have been some positive developments in such cases in recent years. In March 2020, a prosecutor declined to pursue charges filed against academic Pinkaew Laungaramsri under Section 14 of the CCA. She was originally charged in June 2019 for sharing pictures of the military from a protest in Chiang Mai. [173] In May 2019, several people who had been convicted for their online activity were granted a royal pardon and an early release from prison. [174] Those released included student activist Jatupat Boonpattararaksa, who was sentenced for sharing a British Broadcasting Corporation (BBC) news biography of the king, [175] and singer Thanat Thanawatcharanond, who served half of his 10-year sentence for a speech he gave at a rally that was uploaded to YouTube. [176] In June 2020, after the coverage period, activist Thanet Anatawong was acquitted of sedition charges, with the court concluding that the five Facebook posts in which he had criticized the NCPO were political expression protected by the constitution. [177] Thanet was released after spending three years and 10 months in prison. [178]

C4 0-4 pts	
Does the government place restrictions on anonymous communication or encryption?	**2** / 4

The government has attempted to restrict encryption and has seen some success in limiting online anonymity.

In February 2018, the NBTC ordered all mobile service providers to collect fingerprints or face scans from SIM card registrants. This process was required of all new SIM card users, with the old SIM card users having to reregister. The data must be sent to a central repository at the NBTC. [179] In the southernmost provinces of Thailand, site of a long-running insurgency, this policy is enforced more strictly. New identification measures that employ facial scanning and biometrics came into force in October 2019 in the three provinces of Yala, Pattani, and Narathiwat, as well as in three districts of Songkhla Province. [180] According to this announcement, those who do not register their SIM cards with facial scans by the service providers AIS, TrueMove H, or DTAC will not be able to use mobile phone services, [181] with a number of phones disconnected starting in April 2020. [182] Civil society groups and human rights defenders have warned that the requirements could harm privacy, restrict other freedoms, and lead to profiling of the local ethnic Malay Muslim population. [183]

In early 2017, the government took steps to undermine encryption. Section 18(7) of the amended CCA enables officials to order individuals to "decode any person's computer data" without a court order. [184] While some companies may be unable to comply with such orders, the law could provide grounds to punish providers or individuals who fail to decrypt content on request. Privacy International has reported on other possible ways for Thai authorities to circumvent encryption, including impersonating secure websites to intercept communications and passwords, and conducting downgrade attacks, which force a user's communications with an email client through a port that is unencrypted by default (see C8). [185] The group challenged Microsoft for trusting Thai national root certificates, leaving them vulnerable to measures that would undermine security for users visiting certain websites; Microsoft said a trustworthy third party vets authorities that issue certificates before the company accepts them. [186]

C5 0-6 pts	
Does state surveillance of internet activities infringe on users' right to privacy?	**1** / 6

The government actively monitors social media and private communications with limited, if any, oversight. A complex set of policies aim to control online communication, but the country lacks a legal framework that establishes accountability and transparency mechanisms for government surveillance.

Section 4(2) of the PDPA exempts data collected under the Cybersecurity Act from privacy safeguards that are otherwise guaranteed under the data protection law (see C6). [187] The Cybersecurity Act fails to protect individual privacy and provides broad powers to the government to access personal information without judicial review or other forms of oversight. [188] For issues designated as "critical level threats," officials can access computer systems or data, and extract and maintain a copy of the information collected. No attempt is required to notify the persons affected by this information gathering, and there are no privacy protections to govern the handling of the information. [189]

There have been prosecutions in previous years in which private chat records were used as evidence against internet users. It is not clear how officials accessed chat records in these cases, though military and police authorities have created fake accounts in order to join chat groups, even baiting users to criticize the monarchy or the junta. [190] In several cases in which individuals were summoned or arrested, the authorities also confiscated smartphones to access social media accounts (see C3).

A number of draft laws would enable more government surveillance. For example, a revised criminal procedure law that was still pending in 2020 would grant surveillance powers to authorized police officials. The draft stipulates a wide range of suspected offenses for which surveillance is lawful; in addition to violations of national security and organized crime, it includes broad categories like "complex" crimes. [191] 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 behavior such as certain sexual acts, child molestation, or terrorism.

Government agencies possess a variety of surveillance technologies. Some bought spying software from the Milan-based company Hacking Team between 2012 and

2014, according to leaked documents; [192] Thailand has also obtained licenses to import telecommunications interception equipment from Switzerland and the United Kingdom. [193] According to Privacy International, the licenses indicate the probable acquisition of IMSI (international mobile subscriber identity) catchers—devices that intercept data from all phones in the immediate area regardless of whether they are the focus of an investigation.

The Anti-Fake News Center collects information through the use of artificial intelligence that is then reviewed by human content monitors (see B5). [194] The extensive monitoring, particularly of social media accounts, raises significant privacy concerns, and there is a lack of clearly drafted procedural guidelines and independent oversight to ensure that any data collected are protected.

The 2019 National Intelligence Act, which went into effect in April 2019, authorizes the National Intelligence Agency to obtain from government agencies or individuals any information that will have an impact on "national security," a term that remains undefined (see C6). If this information is not provided by a government agency or individual, the National Intelligence Agency may "use any means, including electronic, telecommunication devices or other technologies," to obtain it. [195] The prime minister is in charge of implementation of this act.

In response to COVID-19, the MDES introduced a mobile app to track and monitor people returning to Thailand from high-risk countries. This app requires submission of information such as one's name, address, phone number, and passport number, and it was made mandatory for all foreign arrivals. Although the information collected is reportedly only stored until the completion of the self-quarantine period of 14 days, [196] the collection of information and uncertainty about how it is used and by whom raise serious concerns about privacy and other basic rights. [197]

C6 0-6 pts	
Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	**1** / 6

Surveillance is facilitated by "the Thai government's control of the internet infrastructure [and] a close relationship with internet service providers," according to Privacy International. [198] Section 15 of the CCA places a masked obligation on service providers to monitor user information, as they can face penalties under Section 14 if they are found to have "intentionally supported or consented to" a given offense. [199] Failure to monitor what is being shared by a user, take down that information, or share the user's information with the government may be seen as support or consent for the activities in question. In addition, CCA amendments allow officials to instruct service providers to retain computer traffic data for up to two years, up from one year under the 2007 version. Providers must otherwise retain data for at least 90 days under Section 26 of the law. Failure to comply with court or government orders can result in a fine of up to 200,00 baht ($6,320), or a daily fine of 5,000 baht ($158) until compliance.

In October 2019, the MDES attempted to enforce the data retention provisions of the law more strictly, directing coffee shops, restaurants, and other venues that offer public Wi-Fi to retain the data of users, including names, browsing history, and log files, for at least 90 days. [200] The order was intended to preserve data for the Anti-Fake News Center and to combat the sharing of false content that is punishable under Section 14 of the CCA or any other law (see B5 and C2).

The PDPA of 2019 was scheduled to enter into force in May 2020, but certain aspects of the law's implementation were delayed until May 2021. [201] The law outlines how businesses can collect, use, or disclose personal information. [202] The law can apply to data controllers and data processes outside the country if they process the data of people in Thailand. However, the act provides exemptions for certain activities and authorities. Section 4 exempts any activity of a public authority that has a duty to maintain national security, ranging from financial security to cybersecurity. It also allows an exception for the House of Representatives, the Senate, or any committee appointed by them. [203]

Though official requests to access privately held data generally require a warrant, a 2012 cabinet directive placed several types of cases, including CCA violations, under the jurisdiction of the Department of Special Investigation (DSI). Under rules

regulating DSI operations, investigators can intercept internet communications and collect personal data without a court order, meaning internet users suspected of speech-related crimes are particularly exposed. Even where court orders are still required, Thai judges typically approve requests without serious deliberation.

The 2019 National Intelligence Act could allow the National Intelligence Agency to compel service providers to hand over information it requests, even if it includes sensitive or personal data (see C5).

During the COVID-19 pandemic, there were reports of increased data sharing between government agencies and telecommunications providers. In June 2020, a document leaked from a meeting between the Department of Disease Control (DDC), the MDES, the NBTC, and the Ministry of Defence (MOD) alleged that the government planned to use big-data tools to monitor the virus and would access location data from telecom service providers such as AIS, DTAC, TRUE, CAT, and TOT. [204] The MOD denied the report, although it confirmed that it had met with major mobile service providers about tracking the virus. [205] The NBTC and the MDES have reportedly been asked to manage the tracking of the movements of mobile phone users.

Facebook and Google reported a handful of government requests to access user data in the last six months of 2019. Google received one request for data regarding three users or accounts, but complied with none between July and December. [206] In the same time period, Facebook received 107 requests for data regarding 125 users or accounts and provided 71 percent of the data requested. [207] LINE, the most popular chat application in Thailand, reported receiving no requests from law enforcement for user data in the last six months of 2019. [208]

The surrender of user data by service providers to authorities has led to arrests and detentions. In a glaring misuse of its access to user data, TrueMove H provided the location and identity of a Twitter user called Niranam to the police. The user is now being prosecuted for posting content about the king and faces a heavy prison sentence if convicted (see C3). [209]

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	0 / 5

This coverage period featured instances of extralegal intimidation, enforced disappearances, and mysterious deaths of prodemocracy and antimonarchy activists as well as human rights defenders, including those based outside of Thailand, in apparent connection with their online and other actions.

After the coup in May 2014, more than a dozen Thai prodemocracy activists fled the country to continue their political engagement online, often criticizing and parodying the Thai monarchy and advocating for a republic. In May 2019, three antimonarchy activists—Siam Theerawut, Chucheep Chivasut, and Kritsana Thaptha—who face lèse-majesté charges in Thailand were forcibly disappeared in Vietnam after leaving Laos. Civil society groups reported that they were handed to Thai authorities, a claim Deputy Prime Minister Prawit Wongsuwan denied. [210] Their whereabouts remained unknown at the end of the coverage period. [211]

In December 2018, another three Thai prodemocracy and antimonarchy activists—Surachai Sae Dan, Kraidej Luelert, and Chatchan Buphawan—disappeared while living in Laos. [212] In January 2019, the bodies of Kraidej and Chatchan were found on the shore of the Mekong River at the border between Thailand and Laos. Surachai's whereabouts remained unknown. The United Nations and civil society organizations have expressed concern about these developments; [213] the Thai government has denied any responsibility. [214]

In June 2020, after the coverage period, Wanchalearm Satsaksit, a critic of the government and the monarchy, was forcibly disappeared from outside his home in Cambodia. [215] He faced pending charges under the CCA, and disappeared a day after he posted a video in which he criticized the Thai prime minister. Wanchalearm's whereabouts were unknown as of September 2020. [216]

Prodemocracy activists who are vocal online were assaulted inside and outside Thailand during the coverage period. Sirawit Seritiwat, for example, was violently assaulted twice in June 2019, [217] with police offering him protection only if he gave

up his activism. [218] Ekkachai Hongkangwan has been assaulted at least seven times since January 2018, [219] and Pavin Chachavalpongpun, who lives in Japan, was attacked with chemicals in July 2019. [220] The Thai police have not conducted thorough investigations into the threats and attacks, or have halted investigations, [221] instead blaming the activists for the attacks perpetrated against them. [222]

There have been a string of online threats against those who voice opinions that are critical of the monarchy or the government, encouraging self-censorship (see B4). Prodemocracy activist Parit Chiwarak received a call in June 2019 in which he was threatened with violence. [223] In October 2019, users sharing the viral hashtag #royalmotoracade on social media were subjected to online threats. For example, an anonymous Twitter user whose post was shared 10,400 times was targeted in a Facebook post that called the original post "fake news" and a result of a conspiracy, and claimed to contain pictures of the Twitter user. [224] Following the threats, the Twitter account and post were removed. An activist who commented on the same hashtag deleted his Facebook account after he received a message asking him to delete all his social media accounts for his own safety; the message was sent by someone claiming to belong to the royal household. [225] Starting in March 2020, student activist Sirin Mungcharoen received death threats, bullying, sexual harassment, and other attacks online, [226] after a video of her protest with a black flag went viral. She deactivated her social media accounts temporarily. [227]

Participants in the Royalist Marketplace Facebook group who expressed critical opinions on the monarchy received online and offline threats and intimidation (see B2 and C3). Some users have been doxed on social media, threatened by police, or threatened with the loss of their jobs. [228] In June 2020, a human rights lawyer petitioned the House Committee on Law, Justice, and Human Rights to investigate the harassment and intimidation.

During the COVID-19 pandemic and the subsequent lockdown, police officers have visited and questioned women human rights defenders after they shared videos on Facebook about their work. In May 2020, Katima Leeja, an ethnic Lisu activist, was visited and questioned by plainclothes military officers after she participated in a Facebook video criticizing physical violence amid a land dispute. [229] Also in May,

Sommai Harntecha, an activist with the Rak Ban Haeng environmental conservation group in Lampang, participated in a Facebook video calling for the government's COVID-19 emergency declaration to be revoked. Three plainclothes officers warned her not to discuss or engage in any activism related to the emergency decree. [230]

Authorities are known to intimidate and detain users to pressure them to remove content or self-censor (see B2 and B4). For example, one user reported in November 2019 that she was arrested and interrogated about posts that were shared by other prodemocracy student activists. During the interrogation, police reportedly asked her about her opinions, her personal life, and her family, friends, and classmates. They reportedly took photos of the internet protocol address of her mobile phone, her phone number, her Twitter log-in details, and other email and social media content. She was made to delete her previous posts and sign an agreement stating that the police could use her information, that she was not being intimidated by them, and that she would not post about the monarchy. [231] She was not presented with an arrest warrant or provided with the identities of the officers who questioned her.

C8 0-3 pts	
Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**2**/3

While there were a number of cyberattacks during the coverage period, civil society groups, journalists, and human rights defenders were not routinely affected by state-sponsored technical attacks in response to their work.

Kaspersky, a global cybersecurity company, [232] identified a number of advanced persistent threats (APTs) that attacked Thai websites between 2018 and 2020, including those dubbed FunnyDream, Cycldek, and Zebrocy. [233] FunnyDream, a Chinese APT actor, focused on high-level government organizations as well as political parties starting in mid-2018. Cycldek, another Chinese APT actor, stole information from the defense and energy sectors, with 3 percent of its targets based in Thailand. Zebrocy is a Russian APT that targets Thai entities as well. [234] The

Provincial Electricity Authority, which supplies electricity to all of Thailand except for Bangkok, was hit with a ransomware attack in June 2020. [235]

Private-sector entities and individuals were also subjected to technical attacks. Two people hijacked the accounts of private individuals on Facebook and LINE to fraudulently persuade friends of the users into sending money. They were arrested by the TCSD in June 2019 for the scheme, which yielded 4 million baht ($130,000). [236] In August 2019, online attackers broke into the computer systems of Thai Lion Air and Malindo Air and leaked the information of 35 million passengers, [237] including full names, home addresses, email addresses, dates of birth, telephone numbers, passport numbers and expiration dates. [238]

A leading independent online news outlet, *Prachatai*, [239] has been subjected to distributed denial-of-service (DDoS) attacks, though no major attacks were documented during the coverage period. The sites of prominent dissident rights groups, such as iLaw and Thai Lawyers for Human Rights, [240] also reported no attacks during this period. [241]

Hackers have targeted government agencies and websites in previous years, notably to protest government actions, such as the NLA's adoption of the CCA in December 2016. Websites operated by several government agencies were defaced by hackers, who displayed a symbol that was developed to oppose a plan to strengthen state control of the internet by imposing a single gateway; [242] other sites were brought offline by DDoS attacks. Several people suspected of involvement were subsequently arrested and interrogated at a military base, [243] including a 19-year-old. [244] Separately, the TCSD arrested 19-year-old Thiranat Mahatthanobol in October 2019 for allegedly launching a cyberattack against the registration website of a government cash handout program called Chim, Shop, Chai. [245] In December 2019, the internal security-camera feed from a cramped Thai prison in Chumphon Province was hacked, and real-time video was posted to YouTube to highlight the poor living conditions of those detained. [246]

In January 2017, Privacy International reported that the authorities have the capability to use downgrade attacks or machine-in-the-middle attacks to circumvent

encryption (see C4).

The Cybersecurity Act came into force with its publication in the government gazette in May 2019. [247] The law sets out measures to protect against, address, and mitigate cybersecurity threats. [248] However, the text fails to protect online freedom and privacy. CIIs, as defined in the law (see A3), have a number of requirements under Sections 54, 55, 57, 73, and 74 that can be challenging to comply with, especially for private companies. [249] For example, CIIs must monitor and report all threats to the government as they develop, which could include sharing confidential information. It can also be challenging to evaluate or identify threats until after the cyberattack has already taken place. [250] Noncompliance can result in imprisonment and heavy fines.

• • •

Footnotes

1 Digital 2020: Thailand, We are social and Hootsuite, https://datareportal.com/reports/digital-2020-thailand

2 "Availability rankings," The Inclusive Internet Index 2020, The Economist Intelligence Unit, https://theinclusiveinternet.eiu.com/explore/countries/TH/performance/i....

3 Digital 2020: Thailand, We are social and Hootsuite, https://datareportal.com/reports/digital-2020-thailand

4 Ibid.

5 Internet Information Research Network Technology Lab, "About Internet Bandwidth (Internet Bandwidth)," National Electronics and Computer Technology Center, http://internet.nectec.or.th/webstats/bandwidth.iir?Sec=bandwidth.

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

Freedom in the World Status

Partly Free

Networks Restricted

No

Social Media Blocked

No

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2020

Other Years

2023

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

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

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org