Freedom House

FREEDOM ON THE NET 2018

Thailand

NOT FREE

35 /100

A. Obstacles to Access	16 /25
B. Limits on Content	11 /35
C. Violations of User Rights	8 /40

LAST YEAR'S SCORE & STATUS

33 /100 Not Free

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

Key Developments, June 1, 2017 - May 31, 2018

- A Ministry of Digital Economy and Society decree introduced clearer procedures for content removal, but continues to hold intermediaries and content owners criminally liable (see Content Removal).
- At least two internet users were sentenced under the *lèse majesté* law for more than a decade each in prison (see Prosecutions and Detentions for Online Activities).
- A concerning new regulation requires users to provide biometric data in order to register a SIM card, and the National Reform Steering Assembly has endorsed new invasive surveillance measures (see Surveillance, Privacy, and Anonymity).
- As part of plans to expand broadband access, the government set up two new companies, the National Broadband Network and the National Gateway and Data Centre, thereby increasing its control over Thailand's telecommunication infrastructure (see Restrictions on Connectivity).

Introduction

Despite remaining "Not Free" for the fifth year in a row, internet freedom improved slightly in Thailand due to increased access and less direct violence against online journalists and other ICT users.

Thailand entered its fourth year under military leadership, led by General Prayuth Chan-ocha. In May 2014, high-ranking military officers effected a *coup d'etat* and instituted themselves as the National Council for Peace and Order (NCPO). In August 2016, a national referendum on a new constitution was held under a law which effectively prohibited campaigning against it. That constitution came into effect on

April 6, 2017, retaining the NCPO's absolute authority to make important government appointments and issue directives without oversight.

The junta continued to consolidate its control over telecommunication infrastructure despite increased internet access for Thais. The state-controlled National Broadband Network Co Ltd and the National Gateway and Data Centre Co Ltd were both established during the reporting period. The junta also suspended the selection process for the National Broadcasting and Telecommunication Commission and extended the current commissioners' terms indefinitely.

The amended Computer Related Crimes Act (CCA) became effective in May 2017, despite significant opposition from internet freedom activists. A notice-and-takedown procedure for internet intermediaries could encourage more widespread content removals. The law also grants the authorities more powers to block and remove offending content.

Intermediary liability was again modified during the reporting period with the implementation of a new decree that provides a clearer set of procedures for content removal. While the new rules are expected to relieve some burden, both content owners and intermediaries can still be held criminally liable, thus incentivizing self-censorship.

Activists, journalists, and internet users continued to be silenced and often prosecuted under both the criminal code and the amended CCA, with at least two users being sentenced to prison for over a decade. However, in a welcoming development, the judiciary dismissed charges in two cases under the CCA amendments that no longer criminalize importing false information into the computer system.

There were troubling developments regarding the government's surveillance apparatuses during the reporting period. In a blow to online anonymity, users must now provide biometric data when registering a SIM card. The National Reform Steering Assembly (NRSA) has also endorsed invasive surveillance policies, including a centralized social media watch center and the purchase of enhanced surveillance technology. Additionally, after a March 2018 public hearing, a new cybersecurity law is

expected to be enacted in the next year, which would give the government even more power to surveil internet users under the guise of national security.

A. Obstacles to Access

Internet access is considered affordable, but faces an increasing tendency of tighter control by the government. During the reporting period, the junta government has shown a continuing commitment to devise various technologies and means to control online activities of Thais.

Availability and Ease of Access

Internet penetration steadily increased during the reporting period. By the end of 2017, 93.7 percent of internet users accessed the internet through their mobile phone compared to 90 percent in 2016. 45.4 percent of users, down from 50 percent the previous year, accessed the internet through desktop computers. [1]

The internet continues to become more affordable. The average price for one Kbps of mobile data decreased from THB 0.07 in 2015 to THB 0.02 in 2017. About 42.2 percent of internet users spend THB 200-399 (US$6-12) per month to access the internet, compared to 40 percent in 2016; 21.2 percent pay under THB 200 (US$6) per month, 14.8 percent pay THB 400-599 (US$12-18) per month; another almost 11 percent access the internet through free programs. [2]

Government programs have sought to reduce a persistent digital divide between urban and rural areas. Under the "Return Happiness to the Thai People" program, the NCPO has successfully installed Wi-Fi hotspots in 18,000 villages as of January 2018, although many users have complained of connectivity issues, with the goal of reaching 24,700 villages in total by the end of 2018. [3] Initiated in early 2016 by the then Ministry of Information and Communication Technology (MICT) and the National Broadcasting and Telecommunication Committee (NBTC), the project aims to reduce the penetration gap between urban and rural Thais by providing broadband internet via wireless and fixed-line access points at reasonable costs. The Ministry of Digital Economy and Society (MDES) in January 2018 also announced

plans to hire at least 1,000 people who could work with villagers to develop ICT skills. [4]

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, though the state is extending control of the infrastructure with the establishment of the new National Broadband Network Co Ltd and the National Gateway and Data Centre Co Ltd.

Out of 10 National Internet Exchanges that connect to international networks, the government-run Communication Authority of Thailand (CAT) Telecom operates the country's largest. Access to the international internet gateway was previously limited to CAT until it opened to competitors in 2006. [5]

Within a week of the May 2014 coup, an MICT government official announced plans to establish a "national digital internet gateway" through CAT Telecom, TOT Telecom, and six other ISPs, enabling the ministry to interrupt access. [6] 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." [7] Internet users and experts attacked the plan as a Chinese "Great Firewall," enabling censorship and personal data collection, while undermining speed and security. [8] After intense public opposition, Deputy Prime Minister Somkid Jatusripitak said the plan had been halted. [9]

In 2015, *TelecomAsia*, a telecom news website, received leaked documents that suggested that returning to a centralized gateway model, better known as "Single Gateway," had been a military priority since 2006 in order to tighten control over information in the country. [10] In January 2017, the government approved 5 billion baht to develop an internet gateway, which has been promoted as an infrastructure development to make Thailand the "digital hub" of Southeast Asia. [11] Although the ICT Ministry has denied that the project is the controversial Single Gateway, [12] critics suspect that it is indeed that. [13]

Under the government's plan to consolidate and spearhead the expansion of broadband access, the government set up the National Broadband Network Co Ltd (NBN Co) in August 2017 and the National Gateway and Data Centre Co Ltd (NGDC Co) in November 2017, primarily through the government-run CAT Telecom. [14] This has been seen as part of the government's plan to consolidate its control over telecommunication infrastructure in the country.

Thailand's international bandwidth usage amounted to 5,032 Gbps in December 2017, and domestic bandwidth amounted to 5,249 Gbps, [15] about 42 percent and about 29 percent higher than the same month in 2016 respectively. Bandwidth usage consistently increased every month in 2017 at an average of 3 percent (domestic) and 2.5 percent (international) per month.

ICT Market

High-speed internet is concentrated in a handful of large providers, and the trend points toward more concentration. Though many are privately owned, "successive Thai governments over the past few decades have maintained close relationships with private telecommunication companies and ISPs through appointments which starkly exemplify the revolving door between the government and the private telecommunications sector," according to a UK-based Privacy International research report published in 2017. [16]

Although 20 ISPs have licenses to operate in Thailand, the three biggest operators in 2017 control almost 89 shares of the market. TRUE online continued to dominate the market during the reporting period with the highest market share of 37.9 percent toward the end of 2017. Jasmin followed with 33.4 percent and TOT, a state-owned enterprise, retained third place despite having its market share fall to 17.3 percent. [17] Advanced Info Service (AIS), Thailand's number one mobile service provider, entered the fixed-line broadband market in 2015 and accounted for more than three percent. It is expanding the fiber-optic network and is expected to increase competition in the sector. [18]

For the mobile market, AIS saw an increase of one percent in its market share, from 44.3 at the end of 2016 to 47 percent toward the end of 2017, followed by Norwegian-

controlled DTAC at 26.7 percent, and TRUE at 26.2 percent. [19] AIS and DTAC operate some spectrum under concessions from state-owned TOT and CAT Telecom, an allocation system that does not entirely enable free-market competition.

Regulatory Bodies

The NBTC, the former regulator of radio, TV, and telecommunications, was stripped of its authority, revenue, and independence when the National Legislative Assembly (NLA) passed the NBTC Act in June 2017. It endures as a government agency 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 NBTC Act was part of a contentious set of bills called "digital economy" laws, [20] which were aimed at tightening control of the country's telecommunication. Two legislative changes from this set of bills passed during the previous reporting period were the amendments to the 2007 Computer-Related Crime Act (CCA) and the Digital Development for Economy and Society Act.

One regulative authority in Thailand is the Ministry of Digital Economy (MDES), which was established in June 2016 by the NLA. MDES replaced the Ministry of Information and Communication Technology (MICT) and is responsible for implementing policy and enforcing the CCA. [21]

http://www.khaosodenglish.com/politics/2016/06/04/thailand-to-welcome-n....

The Commission for Digital Economy and Society (CDES) is another official body that provides directives to MDES and is responsible for formulating policy under the Digital Development for Economy and Society Act (DDA), which came into effect in January 2017. [22] Chaired by the prime minister, the commission is comprised of government ministers and no more than eight qualified experts. [23] It is stipulated as a legal entity, not a government body, absolving it of accountability under laws that govern 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 Act mandates that the NBTC transfer revenue to that office "as appropriate."

The DDA redirects up to THB five billion of NBTC licensing revenue toward a new Fund for Developing Digital for Economy and Society, a broad legal entity 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 a similarly broad 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. [24]

The number of NBTC commissioners was reduced from 11 to seven, and their eligible age range narrowed from 35-70 to 40-70 years old. Candidates are selected based on their rank in the government, military, or police, rather than their expertise. The nomination committee, previously comprised of 15 people from related professions, was reduced to seven people holding various bureaucratic and judicial positions affiliated with the government. Candidates are vetted by the senate secretariat and endorsed by the senate, which is effectively appointed by the junta for the first five years under the new constitution.

In April 2018, the NLA rejected all 14 candidates that the NBTC nomination committee proposed. [25] 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. As of July 2018, the selection of commissioners is still pending. [26]

In July 2017, the NBTC backtracked on its April 2017 decision to classify over-the-top (OTT) content as broadcasters, subject to licensing and content regulation. It has since started conducting a thorough study on OTT regulation before issuing a new policy. Popular paid OTT operators in Thailand include Netflix, Ifix, Primetime, Advanced Info Service's AIS Play, and TrueVisions. In response to NBTC's April decision, Asia Internet Coalition (AIC), a coalition of transnational IT companies such as Facebook, Google, and Paypal, submitted an open letter to the NBTC urging a review of its policy and a need to consult with relevant stakeholders and the public. [27]

https://www.aicasia.org/2017/06/30/aic-responds-nbtc/. AIC stated that the NBTC's April decision regarding OTT would limit users' ability to access quality international content and would result in other major global and domestic repercussions.

B. Limits on Content

The government has continued to restrict critical content online by blocking webpages and VPNs and by compelling platforms like Google and Facebook to remove content. A new decree implemented during the reporting period addressed intermediary liability and built off the 2017 amendments to the 2007 Computer-related Crimes Act (CCA). While both this decree and the CCA amendments included some small positive developments, intermediaries still experience a climate of fear and continue to self-censor content.

Blocking and Filtering

Website blocking of antiroyal content is widespread and lacks transparency, particularly since the coup. During the reporting period, more websites were blocked for hosting what the government deems as illegal content, while a new decree expanded on Section 20 of the amended CCA, which relates to the ways in which service providers block websites.

Thailand has never publicly revealed the number of URLs blocked by court orders. Often, the public learns that a URL is blocked when they are denied access to that website. In May 2017, the Thai Internet Service Providers Association (TISPA) said its members blocked access to over 6,300 URLs pursuant to NBTC orders for threatening national security, which includes *lèse majesté* content, hosting pornography, and facilitating gambling, among other issues. [28] The prohibition on criticizing royalty extends to related content: In October 2016, several ISPs blocked a *Phnom Penh Post* article reporting that Cambodian authorities received a request to extradite three people suspected of *lèse majesté* to Thailand. [29]

Some blocks affect entire websites, not just 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. [30] At least one news website, the

UK *Daily Mail,* was blocked at the domain level by TOT and 3BB. Websites offering tools for anonymity and circumventing censorship, as well as VPNs, are also blocked on more than one network. [31] The study revealed significant inconsistencies across ISPs, suggesting some providers may implement discretionary restrictions without prior authorization. The website of the *New York Post,* for example, was blocked by mobile phone operator DTAC in February 2017 but otherwise available.

Amendments to the CCA, which became effective in May 2017, may empower more bodies to assess 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 contravenes public morals or public order. [32] The 2017 amendments established a nine-member ministry-appointed "computer information screening committee" which may also authorize officials to apply for court orders to block content. Three 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 threaten public order or morals even if the content does not actually violate any law, meaning courts could be asked to issue orders to block even legal content at the discretion of a committee that is not accountable to the public. [33]

In July 2017, a decree expanding on the amended Section 20 was enacted. The decree states that service providers must abide by court orders to block access to websites using technical measures. [34] The final draft of the decree was an improvement from an earlier draft, which said ISPs are required to take a proactive role in censorship and use "whichever means necessary" to block content.

Content Removal

Like blocking and filtering, content removal continued under the tight control of the junta government. A July 2017 decree, which builds off of the 2017 CCA amendments, modified intermediary liability, and the military leadership continued to pressure intermediaries to censor political information, with some success.

Between May 1 and July 16, 2017, Facebook complied with a Thai court order and removed more than 1,000 links while YouTube removed nearly 800 links for illegal

content. [35] NBTC claimed that the court had ordered the removal of 3,726 webpages by August 7, the majority of which were housed on Facebook and YouTube. In response to Facebook and YouTube not removing all the links prior to the deadline, in August 2017 the MDES publicly threatened ISPs to block a remaining 1,786 webpages or risk prosecution or losing their license. [36] A few days later, however, it was reported that these additional links were not actually ordered to be removed and instead there were "coordination errors among government agencies." [37]

According to Google's transparency report, the government sent 141 requests to Google from July to December 2017 to remove 3,348 items. [38] 97 percent, or a total of 137 requests, were for criticizing the government. Two requests were for unidentified reasons. One request was for privacy and security concerns, while an additional request was due to causing religious offense. According to Facebook's transparency report, 139 items were restricted on the platform between July and December 2017. [39] 138 were restricted for allegedly violating *lèse-majesté* laws, while one item was restricted on defamation grounds.

Content providers or intermediaries have complied with removal requests in the past because they were subject to possible prosecution under the 2007 CCA for allowing the dissemination of content considered harmful to national security or public order. [40] The amendments to the CCA, effective in May 2017, provides some protection for intermediaries through a notice-and-takedown system. It also implements rules and procedures for takedown requests and clearly grants 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 it 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 if they fail to destroy it. [41] Analysts feared 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 May 2017.

In July 2017, a new MDES decree further modified intermediary liability. [42] The decree 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 twenty-four 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, who has final authority over the decision. Both companies and content owners who do not comply face imprisonment of up to five years.

Despite some welcomed developments in the new decree, the twenty-four hour window requirement to remove national security-related content disregards a Supreme Court ruling. In a case against Prachatai director Chiranuch Premchaiporn, the court decided that 11 days is an acceptable amount of time for removing content relating to national security. [43] Additionally, 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.

Media, Diversity, and Content Manipulation

Social networks and digital media provide opportunities for sharing information when traditional media is subject to restrictions, but the authorities have also issued laws and directives to control online discussions of sensitive topics. The most popular social media and communications apps in 2017 were Facebook (49 million users), followed by the Japanese messaging service LINE (41 million users), Instagram (13.6 million users), and Twitter (12 million users). [44]

Traditional media controls may increasingly be felt online as the sectors converge. TV channels already stream content online or on YouTube, and many began broadcasting on Facebook in 2017. [45] More than a dozen of print magazines ceased to publish in 2017, including Men's Health, Marie Claire, Health&Cuisine, Elle Men, and Nation Weekly. Meanwhile, the internet has become a central platform for media startups, competing to offer news and analysis to readers.

While the online market remains dynamic, the diversity of viewpoints available online has been limited due to a number of factors. One is economic: Media outlets almost universally use Facebook "likes" and similar indicators when seeking revenue. As the advertising model moves away from banner ads that support independent websites, sites are more likely to privilege popular entertainment content over complex or underrepresented information.

The second is the restrictive political environment, which encourages self-censorship online. Legal sanctions for online activity such as criticizing the government on Facebook are prevalent (see Prosecutions and Detentions for Online Activity). The junta government has let it known that it monitors social media to control political expression. [46] On October 14, 2016, *VoiceTV*, a critical news outlet owned by former Prime Minister Thaksin Shinawatra, temporarily suspended its Facebook page to avoid breaking the law. [47] Several news outlets deleted online articles stating a regent would assume royal responsibilities instead of the crown prince without publishing a correction. [48] The *Khaosod English* news website republished an edited version, saying the original had been censored on the instruction of its parent company. [49]

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. There was also an increased use of social media by state agencies to propagate progovernment information. For example, in April 2018 the Office of the Prime Minister's Secretariat announced a new LINE account to reach citizens directly. [50] In the past, officials have offered financial incentives to citizens to monitor one another online (see Surveillance, Privacy, and Anonymity),

and many have organized informally to harass the junta's opponents (see Intimidation and Violence).

Digital Activism

Social media, chat applications, and online petition sites such as Change.org are essential tools for digital activism under the junta government. For example, one recent petition calling for an independent investigation into a student's death at a military school collected thousands of signatures. [51]

Since the coup, many bloggers, activists, and human rights lawyers have formed coalitions such as Thai Lawyers for Human Rights to monitor the situation and document human rights violations by the junta. Anonymously operated Facebook pages have become a crucial space for individuals to share their opinions and hold the junta accountable.

A remarkable example is CSI LA, which is a Facebook page run anonymously by a citizen journalist. The page has attracted more than 810K followers because it offers sensationalist investigations into scandals and crimes unsolved by the police and the traditional media. In January 2017, the page successfully influenced the government's anti-corruption agency when it investigated the irregular wealth of junta leader General Prawit Wongsuwan, particularly in relation to his luxurious watch collections. In response to the Facebook page's coverage, traditional media followed suit in investigating and questioning Prawit. This was one of the scandals that forced General Prawit Wongsuwan to publicly announce that if the National Anti-Corruption Commission probe found him guilty of corruption, he would voluntarily resign. A Change.org petition was made during the reporting period where over 80,000 people have called for General Prawit to resign. [52]

C. Violations of User Rights

As the proposed timeline for a general election approaches, civil society and political parties have unsuccessfully called for the junta to lift political bans and restrictions on fundamental rights. Internet users continued to be charged and imprisoned for their online activity during the reporting period, some for more than a decade. New

government policies restricted anonymity online, and more concerning surveillance measures are expected to be implemented in the future.

Legal Environment

A new constitution went into effect on April 6, 2017 after it was accepted in a national referendum. It replaced an interim constitution introduced after the coup d'etat in 2014. However, Section 44 of the interim constittion is still in effect, which authorizes the NCPO to issue any legislative, executive, or judicial order without accountability, and dozens of so-called "absolute power" orders have been issued. [53] Some of these orders have internet freedom implications, such as giving authorities the power to surveil internet users and order ISPs to cooperate with the authorities in removing content.

The new constitution followed historical norms by enshrining 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 threaten national security, public order, public morals, or any other person's rights and freedoms.

The NCPO-appointed government, made up of the NRSA and the NLA, has passed 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 revised CCA was adopted on December 16, 2016, sparking widespread outcry from internet users. Section 14(1) of the original 2007 law banned introducing false information into a computer system, which experts understand to refer to technical crimes such as hacking. [54] Judges, however, have shown limited understanding of this application, and the clause has been widely used in conjunction with libel charges to prosecute speech. Observers say this provided grounds for Strategic Lawsuits Against Public Participation (SLAPP), allowing government officials and large corporations to file charges in order to intimidate and silence their critics.

Lawmakers sought to limit this abuse by adding new language, "in which the perpetration is not a defamation offense under the Criminal Code." [55] Yet the law retains the problematic term "false" computer information, and adds 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 Prosecutions and Detention for Online Activities). Other problematic sections of the CCA also went unchanged, including Section 14(3), which criminalizes online content deemed to "affect national security" and is frequently used in conjunction with *lèse majesté* charges. The revised CCA also extended the scope of online censorship (see Blocking and Filtering) and altered the legal framework for intermediary liability (see Content Removal).

Pending legislation includes a draft media reform law, which could limit both press freedom and online speech, though it was tempered following public opposition and there were no updates to it during the reporting period. The NRSA media reform committee proposed establishing a national media council, including two high-ranking government representatives, to register and license "professional" journalists broadly defined as anyone routinely engaged in publishing to a wide audience for direct or indirect profit. The draft law would punish working without a license with prison sentences, [56] and gave the council authority to levy fines, [57] both deterrents to online and citizen journalists. Facing nearly universal opposition, the NRSA removed the criminal and financial penalties before approving the draft. [58] In May 2017 the National Legislative Assembly chairman conceded that it will be an uphill battle to pass it. [59]

A controversial draft cybersecurity act was also widely criticized when it was introduced in 2015 for clauses that would invade privacy and enable surveillance. A public hearing on the cybersecurity bill was held in March 2018.

A revised criminal procedural law pending in mid-2018 would separately grant 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 broad categories like "complex" crimes. [60]

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. Creating and distributing such information would be punishable by one to seven years in prison with 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 five-year jail term and THB 500,000 fine. [61] The draft was still pending at the end of reporting period.

Prosecutions and Detentions for Online Activities

Criminal prosecution is one of the junta's main strategies to combat opposition, despite talk of reconciliation and reform. Police and the Attorney General's office continue to pursue charges which clearly infringe on basic rights. The burden of deciding for or against regime critics is therefore passed to the court, resulting in an unprecedented number of prosecutions for online speech.

In a positive development, courts dismissed a few charges for false information and defamation under Article 14 (1) of the CCA due to the 2017 amendments. Cases affected by these changes included the June 2017 sentencing of Wichai and the May 2018 acquittal of British human rights defender Andy Hall.

Nevertheless, at least two cases resulted in prison sentences lasting over a decade:

- In June 2017, a man named Wichai was sentenced to 35 years [62] in jail under the *lèse majesté* law for posting ten messages on a fraudulent Facebook account with another individual's name and photo. Originally Wichai was also charged under Article 14 (1) of the CCA, but the court later dismissed this charge due to the 2017 amendments to the law. [63]

- In August 2017, a 61-year-old man was sentenced to 18 years in prison for posting six Facebook videos that the court determined insulted the monarchy. He was convicted under both Thailand's computer crime law and Article 112 of the Criminal Code. Because he was arrested when the martial law was imposed,

his case was tried in a military court in Bangkok with no opportunity to appeal. [64]

Activists, former politicians, and ordinary internet users were newly charged for criticizing the monarchy or the NCPO leadership. There were also important development on cases from previous reporting periods.

- In August 2017, Jatuphat Boonpattaraksa, a student pro-democracy activist, was sentenced [65] to two and a half years in prison after pleading guilty to *lèse majesté* and violating the CCA [66] for sharing a BBC Thai profile of King Rama X on Facebook. [67]

- In August 2017, former energy minister Pichai Naripthapahan was put under investigation for violating CCA. The investigation was on Pichai's July 2017 Facebook post criticizing the junta's Thailand 20 Year Strategic Plan. [68]

- In August 2017, Pravit Rojanaphruk, a *Khaosod English* journalist, was charged under Section 14 of the CCA and with sedition under Article 116 of the Criminal Code for multiple Facebook posts criticizing the junta in February 2016 and July 2017. [69]

- In August 2017, Junta critic and former Pheu Thai politician Watana Muangsook was charged with sedition under Article 116 of the Criminal Code and for violating Section 14 of the CCA for Facebook posts critiquing the government and urging support for former Prime Minister Yingluck Shinawatra. [70] Also in August 2017, Wattana was twice given suspended jail sentences for contempt of court after he broadcast court proceedings on social media. [71]

- In December 2017, human rights lawyer Anon Nampa was accused of contempt of court and for "importing false information into a computer system" under Article 14 of the CCA for a November Facebook post questioning the fairness of a court verdict. [72]

- In January 2018, Chanoknan Ruamsap, pro-democracy activist, fled Thailand after she was charged for *lèse majesté* under Article 112 of the Criminal Code for posting a BBC profile of King Vajiralongkorn on Facebook. [73]

- In January 2018, historian and pro-democracy activist Charnvit Kasetsiri was accused of violating Article 14 of the CCA for sharing a false news report about the wife of the head of the NCPO. [74]

- In March 2018, pro-democracy activist Ekkachai Hongkanwan was accused of violating Article 14 of the CCA for a Facebook post that was published almost a year before his arrest. The charge was brought against Ekkachai shortly after his corruption campaign against the NCPO deputy-chairman gained popularity. [75]

- In May 2018, eight prominent Pheu Thai Party members, including Watana Muangsook, were charged with violating the ban on political gatherings, at least three of which were also charged with sedition and importing false information into a computer system under Article 14 of the CCA. The charges stemmed from a press conference live streamed on Facebook in which the party members critiqued the junta in light of the upcoming anniversary of the 2014 coup. [76]

- In a positive development in May 2018, a Court of Appeal acquitted British human rights defender Andy Hall of violating Section 14 of the CCA. [77] On September 20, 2016, a court in South Bangkok found Hall guilty of bringing false computer information into the system via an online report for Finland-based NGO Finnwatch which accused the Thai canning company Natural Fruit of labor rights abuses. Hall refused to present his sources as witnesses, and the court ruled that he could not prove the allegations were true. He was separately found guilty of defamation for distributing the same allegations in print, and sentenced to a total three-year suspended prison term and a THB 150,000 fine. [78] The Supreme Court dismissed a separate case involving the same charges on November 3, 2016, due to investigative irregularities, among other issues. [79]

- In June 2018, after the end of the coverage period, human rights lawyer Prawet Praphanukul was convicted of three sedition charges under Article 116 of the Criminal Code and sentenced to 16 months in prison. [80] Prawet was arrested in 2017 for Facebook posts on the country's 1932 revolution. Prawet was originally also charged with *lèse majesté*, but these were later dropped.

Nonstate actors also pursue criminal charges for online speech. Although the CCA was amended during the previous reporting period, companies and officials can still abuse the law to launch burdensome prosecutions—often repeatedly—in order to deter rights defenders, environmental activists, and investigative journalists who publish in any online forum (see Legal Environment).

- In October 2017, the Electricity Generating Authority of Thailand (EGAT) filed a libel suit and a charge under the CCA against environmental activist Prasithchai Noonuan. [81] The charges stemmed from Prasithchai's critical Facebook posts of EGAT's plan to build a coal power plant in the Krabi Province.

- In September 2016, Preeyanan Lorsermvattana, a patient's right activist, critiqued Thailand's Medical Council and called for its reform on Facebook. The Council accused her of violating Article 14 of the CCA and for defamation under Section 328 of the Penal Code. The court accepted the case in August 2017, and it is at trial as of mid-2018. [82]

Surveillance, Privacy, and Anonymity

The junta government actively monitors social media and private communications. A complex set of policies are aimed at controlling online communication, but the country lacks a legal framework establishing accountability and transparency mechanisms for government surveillance.

There were new troubling developments during the reporting period affecting anonymity and surveillance. In July 2017, the NRSA endorsed a set of policies that would systematize and increase the efficiency of government surveillance and its censorship apparatuses. [83] The proposed measures included three new updates to government surveillance. First, a centralized social media watch center would review and determine whether social media content is "inappropriate." Second, telecommunication technology would be upgraded in order to more efficiently surveil internet communications. Finally, anonymity would be restricted by mandating the collection of biometric data when registering new SIM cards.

In February 2018, the NBTC implemented the NRSA policy affecting the anonymous use of the internet. The new regulation requires mobile operators to collect fingerprints or face scans from SIM card registrants. The data must then be sent to a central repository at NBTC. [84]

It is unclear whether the other two NRSA measures, the social media watch center and upgraded surveillance technology, have been implemented. However, the new National Reform Plan setting policy direction for all ministries in the upcoming years states that between 2018 and 2019 a central social media watch system will be established to monitor and remove "inappropriate or illegal content which impacts securities." [85] The reform plan also states that the government will establish an official point of contact for domestic and foreign online media companies, develop a central database of mobile user data, and more efficiently combat illegal online content.

Instead of clear procedures, surveillance is facilitated by "the Thai government's control of the internet infrastructure [and] a close relationship with internet service providers." [86] CCA amendments allow officials to instruct service providers to retain computer traffic data for up to two years, up from one year in the 2007 version. Providers must otherwise retain data for at least 90 days under the law. Though official requests to access that data 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, so 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.

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 secret chat groups, even baiting users to criticize the monarchy or the junta. [87] In several cases in which individuals were summoned or

arrested, the authorities also confiscated smartphones to access social media accounts.

Facebook and Google reported a handful of government requests to access user data between July and December 2017. Google received five requests for data regarding six users/accounts, but complied with none. [88] Facebook received six requests for data regarding seven users/accounts and provided some amount of data on 17 percent of the requests. [89] LINE, the most popular chat application in Thailand, reported receiving no requests from law enforcement for user data in 2017. [90]

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. [91] 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 reported other possible ways for Thai authorities to circumvent encryption, including impersonating secure websites to intercept communications and passwords, or conducting downgrade attacks, which force a user's communications with an email client through a port that is unencrypted by default. [92] 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. [93]

Government agencies also possess surveillance technologies. Some bought spyware from the Milan-based Hacking Team between 2012 and 2014, according to leaked documents; [94] and Thailand has also obtained licenses to export telecommunications interception equipment from Switzerland and the UK. [95] According to Privacy International, the licenses indicate the probable acquisition of IMSI (International Mobile Subscriber Identity) catchers, devices which intercept data from all phones in the immediate area regardless of whether they are the focus of investigation.

Government supporters have assisted in monitoring perceived opponents in the past, activity that intensified after the passing of King Rama IX in October 2016. The MDES

established a cybersecurity center based in state-owned telecommunications company TOT to monitor for inappropriate content (see Blocking and Filtering). [96] A cyber scout program, through which students and regular citizens can apply to receive training on monitoring and reporting inappropriate content, was functioning since before the coup. It is unclear whether the program is still operational.

Separately, a draft law to register and license journalists—including anyone routinely engaged in publishing to a wide audience for direct or indirect profit—was under consideration during the reporting period. [97]

Intimidation and Violence

During the reporting period, there were fewer reports of physical violence and extrajudicial intimidation against bloggers and ICT users compared to the previous year, which saw intensified violence in reprisal for online speech following the death of King Rama IX.

The government uses the controversial CCA to threaten internet users. In November 2017, Prime Minister General Prayut Chan-o-cha threatened to prosecute under CCA those disseminating information that damages the country's reputation or incites violence and hatred. [98] In October 2017, Lt General Sansern Kaewkamnerd, Secretary of the Office of Prime Minister, also threatened to prosecute internet users spreading rumors about flooding in Bangkok, claiming that the rumors cause public panic. [99] In March 2018, [100] the Chiangmai Governor threatened to sue Pim Kemasingki, the editor of a Chiang Mai lifestyle magazine, for violating the CCA for sharing on Facebook an image addressing the bad air quality in the area. The governor argued that the post hurt the city's reputation. [101]

In addition to threatening charges under CCA, the government personally targets those criticizing the government online. In December 2017, the NCPO arbitrarily detained Natchapon Supattana for a so-called "attitude adjustment" after he criticized the NCPO on social media. [102] Also it was reported in June 2017 that military officers went to the home of Surapot Tawesak, a philosopher and academic, to threaten him to stop criticizing the junta and using the word "dictatorship" on Facebook. [103]

https://prachatai.com/journal/2017/06/71922.

Technical Attacks

There have been sporadic reports of cyberattacks on online news outlets in Thailand in the past, though none were documented during the coverage period of this report. In January 2017, Privacy International reported that the authorities have the capability to use downgrade attacks or man-in-the-middle attacks to circumvent encryption.

Hackers targeted government sites in previous years, notably in protest when the NLA passed 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 control of the internet by imposing a single gateway; [104] others were brought offline by DDoS attacks. Several people suspected of involvement were subsequently arrested and interrogated at a military base, [105] including a 19-year-old. [106]

• • •

Footnotes

1 National Statistical Office.

2 National Statistical Office.

3 Ministry of Digital for Economics and Society, "MDES Minister announced the success of Pracharat Internet Project in Chaiyaphum:",. July 7, 2018, https://goo.gl/TrVre6; Apisitniran, L.

4 Apisitniran, L.

5 World Bank, "Telecommunications Sector," Thailand Infrastructure Annual Report 2008, World Bank, accessed May 1, 2012, http://siteresources.worldbank.org/INTTHAILAND/Resources/333200-1177475....

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**

In Other Reports

Freedom in the World 2018

Other Years

2023

Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe >

ADDRESS

GENERAL INQUIRIES
info@freedomhouse.org

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

PRESS & MEDIA
press@freedomhouse.org