Freedom House

FREEDOM ON THE NET 2021

Thailand

NOT FREE

36 /100

A. Obstacles to Access	16 /25
B. Limits on Content	13 /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. Authorities responded to youth-led antigovernment protests—which started in July 2020 and continued throughout the coverage period—by arresting and harassing internet users and prodemocracy leaders who criticized the monarchy. In one of the most draconian cases, a former public servant was sentenced to 43 years in prison. The government also continued to enforce a repressive emergency declaration issued in response to the COVID-19 pandemic, which imposed further constraints on freedom of expression. Intimidation and harassment by authorities targeting individuals for their online activities continued. In a positive development, Thai courts, on several occasions, rejected government requests to restrict content and shut down platforms, and ruled in favor of individuals who faced criminal charges in relation to their online content.

Following five years of military dictatorship, Thailand transitioned to a military-dominated, semi-elected government in 2019. In 2020 and 2021, the combination of democratic deterioration and frustrations over the role of the monarchy provoked the country's largest antigovernment demonstrations in a decade. In response to these youth-led protests, the regime resorted to familiar authoritarian tactics, including arbitrary arrests, intimidation, lèse-majesté charges, and harassment of activists. Freedom of the press is constrained, due process is not guaranteed, and there is impunity for crimes committed against activists.

Key Developments, June 1, 2020 - May 31, 2021

- In October 2020, amid youth-led antigovernment demonstrations, the government ordered the blocking of Change.org after the site hosted a petition calling for the king to be declared a persona non grata in Germany, where he frequently vacationed. Leaked documents also revealed the government's

unrealized plan to block Telegram, a platform widely used by activists to organize protests and mobilize supporters (see B1 and B8).

- Also in October 2020, the Criminal Court rejected the government's request to shut down four online news platforms—Voice TV, the Standard, the Reporters, and Prachatai— and the online accounts of Free Youth, a youth-led prodemocracy group, for violating the Emergency Decree on Public Administration in Emergency Situations, and the Computer-Related Crime Act (CCA). In February 2021, the court had rejected a government request to block a video clip in which the former leader of the now disbanded Future Forward Party criticized the government's COVID-19 vaccination policy (see B2 and B3).
- Internet users were arrested, criminally charged, or subjected to targeted harassment for sharing a range of content, including unverified information about the pandemic and criticism of the government's response. In one of the most draconian sentences imposed in Thailand in recent memory, a former revenue officer received a reduced sentence of 43 and a half years in prison for uploading to YouTube radio clips that were critical of the monarchy (see C3 and C7).
- There were no reported cases within Thailand of enforced disappearances of and physical violence against users in retaliation for their online activities, though a Thai activist was forcibly disappeared in Cambodia. Extralegal intimidation of prodemocracy activists and critics of the monarchy continued (see C7).

A. Obstacles to Access

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 an increasing number of users go online via mobile phones. According to the Digital 2021 Report, developed by creative agency We Are Social and the social media management platform Hootsuite, as of January 2021 Thailand's internet penetration rate was at 69.5 percent, and there

were 49 million internet users, a 7.4 percent increase from January 2020. [1] The Inclusive Internet Index 2021, a project of the *Economist,* ranks Thailand 30 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 2021, 97.7 percent of internet users accessed the internet using a mobile phone, compared with 97 percent in 2020. [3] In contrast, 37.4 percent of users in December 2020 accessed the internet through laptop and desktop computers, according to available statistics —a decrease from 53.6 percent in December of the previous year. [4]

Thailand's international bandwidth usage amounted to 14,274 gigabits per second (Gbps) in January 2021, and domestic bandwidth amounted to 9,233 Gbps, [5] about 31 percent and 12 percent higher than the same month in 2020, respectively.

In February 2020, three private mobile service providers and two state-owned telecommunications firms submitted bids totaling 100 billion baht ($3.3 billion) for spectrum required to set up fifth-generation (5G) mobile service infrastructure. [6] After being the first mobile service provider to launch its 5G network, [7] Advanced Info Service (AIS) had 100,000 subscribers sign up by the end of 2020, and was operating 3,000 5G base stations running across all 77 provinces of Thailand by the end of January 2021. [8]

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. As of 2018, 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. As of 2018, nearly 11 percent of the population accessed the internet through free programs. [9] Some

observers expected the rollout of 5G service to increase internet accessibility due to lower costs; [10] 5G spectrum licenses, however, are more expensive than anticipated, [11] and these costs could be transferred to internet users. [12]

Government programs have sought to reduce the persistent digital divide between urban and rural areas. [13] 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. Although 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, [14] several specifications in the contract were not met. [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 to be completed by March 2020. [18] The program also includes recruiting and training of people to work with villagers to develop information and communication technology (ICT) skills. [19]

With the increased reliance on the internet by those in lockdown amid the COVID-19 pandemic, the government made various attempts to support increased internet usage. The National Broadcasting and Telecommunications Commission (NBTC) redirected 3 billion baht ($99.2 million) from its research fund to provide a one-time assistance of 10 GB internet usage to all prepaid and post-paid mobile phone users. [20] Additionally, in January 2021, the NBTC ordered all mobile and broadband operators to increase their speed and capacity to support those working from home. [21] Shortly after, low-cost mobile packages were introduced, allowing for unlimited data usage and broadband internet packages with increased speed without an increase in costs. [22] However, these benefits leave behind those without any access to the internet or electronic devices at home. [23]

Three mobile operators, AIS, TRUE, and Total Communication Access (DTAC) all offer free access to online content through zero-rating services; with the latter two part of

the Free Basics by Facebook project in Thailand. The program grants free access to entertainment content and social media platforms, including Facebook, Messenger, and Wikipedia, on mobile phones. [24]

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 capability to do so through technical control over internet infrastructure.

CAT Telecom, a state telecommunications provider, operates international telecommunications infrastructure, including international gateways and connections to submarine cable networks and satellites. [25] Access to the international internet gateway was limited to CAT until it opened to competitors in 2006. [26]

A merger of CAT and TOT, both of which are owned by the state, received regulatory approval in May 2019 [27] and took place in January 2020. The new entity is the National Telecom. While the merger was intended to help the public firms compete with private telecommunications companies, [28] it was also seen as part of the government's plan to consolidate 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. [29] 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. [30]

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. [31] 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. [32] 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. [33]

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. [34] 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. [35]

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 offered by only 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." [36]

Although 20 ISPs have licenses to operate in Thailand, the largest three controlled almost 85 percent of the market in 2020. TRUE Online led the sector with 36.5 percent toward the end of 2020. Jasmin followed with 30.46 percent, and state-owned TOT retained third place despite seeing its market share rise to 18 percent. [37] AIS, Thailand's top mobile service provider, which entered the fixed-line broadband market in 2015, accounted for 11 percent. [38]

The purchase and distribution of 48 5G spectrum licenses in February 2020 could also alter market shares (see A1). Given that AIS and TRUE hold the majority of 5G licenses—23 and 17 respectively—they may see market share increase in the future. [39]

For the mobile sector, AIS held a market share of about 44 percent toward the end of the third quarter of 2020. TRUE held 33 percent, and Norwegian-controlled DTAC followed with 20 percent. [40] 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 NBTC's nomination committee is composed of seven people holding various bureaucratic and judicial positions affiliated with the government. Out of 14 candidates shortlisted by the selection committee, 7 candidates are selected, vetted by the Senate secretariat, and endorsed by the unelected Senate. A new NBTC Act approved in February 2021 shortens the selection and removes requirements that candidates have specific experience in telecommunications, broadcasting, or other relevant fields. [41] The Senate specifically rejected amending Section 5(3), which

allows for selection to be based on the rank of individuals 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 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]

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). [45]

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). [46] Chaired by the prime minister, the CDES is composed of government ministers and no more than eight qualified experts. [47] 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.

In 2020 and 2021, additional bodies to operationalize Thailand's Cybersecurity Act and Personal Data Protection Act (PDPA) were established. The Cybersecurity Act created 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). [48] The NCSC develops policy, guidelines, and a code of practice, while the CRC with the support of the CMO administers these policy products. [49] 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. [50] In January 2020, the expert members of the committees were selected in order to prepare for the implementation of the Cybersecurity Act. [51]

In May 2020, ten members were selected and approved by the cabinet to form a Personal Data Protection Committee (PDPC) for the implementation of the PDPA, which is expected to occur in June 2022 (see C6). [52] However, in September 2020, the Cabinet revised the selection process following complaints that those selected lacked the necessary qualifications. [53] 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. [54] 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

B1 0-6 pts	
Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?	**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, and for hosting unauthorized virtual private network (VPN) services. [55]

In October 2020, a leaked secret order of the Ministry of Digital Economy and Society (MDES) was discovered that directed internet and mobile service providers to block four IP addresses linked to Telegram, a messaging app used by protesters to communicate and organize (see B8). [56] In the same month, the government ordered the blocking of Change.org in Thailand, after a petition calling for the king to be declared persona non grata in Germany was shared extensively on Twitter. [57] In November 2020, the MDES blocked 1,457 URLs related to gambling and blocked 190 websites, including Pornhub, for the sharing of pornographic content. [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]

Some blocks affect entire websites, not just the URLs for individual articles or posts. Websites offering tools for online anonymity and circumvention of censorship, as well as VPNs, have been blocked by more than one ISP. [60] The website of the VPN Hotspot Shield, [61] for example, used to be blocked by the ISP TRUE, while Ultrasurf, another VPN, was blocked by DTAC, AIS, and 3BB as of February 2021.

The Center of Operational Policing for Thailand against Intellectual Property Violations and Crimes on the Internet Suppression (COPTICS) was established in 2018. [62] As of January 2019, it had received requests to block 1,080 URLs alleged to violate intellectual property rights, but only 89 were successfully blocked. [63] The NBTC said it was unable to block certain URLs because they were encrypted under the HTTPS protocol and made inaccessible by foreign-based content generators or platform hosts. [64]

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, particularly material that is protected by international human rights standards?	**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 2020, Facebook restricted access to 1,765 posts, of which 1,764 posts allegedly violated Section 112 of the criminal code on lèse-majesté and one which the MDES reported to be illegal hate speech. [65] According to Google's transparency report, the government sent 147 requests from July to December 2020 to remove 1,888 items across various Google services, including YouTube. [66] Of 147 requests, all but 6 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. In January 2021, the government ordered YouTube to restrict access to a music video uploaded by Thai activist rap group, Rap Against Dictatorship. In the music video, the rappers called for royal reforms and showcased images of the 2020 antigovernment youth-led protests. [67] In August 2020, 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, upon request of the MDES. [68] The group had more than a million users and featured discussions about the king. Facebook announced that it would legally challenge the order. [69]

The MDES announced it had obtained a court order to shut down Voice TV, as well as three other online media services: the Reporters, the Standards, and Prachatai in October 2020. According to MDES, the news outlet's coverage of prodemocracy protests in Bangkok violated the Emergency Decree on Public Administration in

Emergency Situations and the Computer-Related Crime Act (CCA). Prior to shutting down Voice TV, the government had asked satellite service providers to stop broadcasting its content. Authorities also obtained a court order to suspend the online activities of Free Youth, a youth-led prodemocracy group. The Ratchada Criminal Court later reversed its order to shut down the outlets and suspend the online activities of Free Youth (see B3). [70]

In June 2021, after the coverage period, courts issued order to Facebook and internet service providers to block or remove 8 Facebook accounts for allegedly spreading "fake news." The accounts are run by activists, journalists, and organizations that have been critical of the Thai monarchy. The accounts remained accessible four days after the MDES urged ISPs to comply with the court order within 24 hours. [71]

The government pressures and intimidates users, publishers, and content hosts to remove content. In May 2021,12 social media users were ordered to remove content that related the government's response to the COVID-19 pandemic or coronavirus vaccines, or face legal consequences. [72] In September 2020, the Thai government filed police complaints against Facebook and Twitter after both companies failed to fully comply with orders from the MDES to take down unspecified content. Google, however, avoided legal action because its video platform, YouTube, removed the requested content. [73] 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 punishment for posting the video. [74]

In November 2020, after announcing a protest march to the royal palace in 2 days, three Twitter accounts belonging to Free Youth and its leaders—Tatthep Ruangprapaikitseri, also known as Ford, and Panumas Singprom, also known as James —were suspended. While Twitter claimed the accounts were suspended for violating their platform manipulation and spam policy, cybersecurity experts suggested that this could have been a coordinated online attack in which government supporters reported the accounts at a rate high enough to trigger their automatic suspension. [75]

Under Section 15 of the CCA, social media companies and other content hosts may be penalized if they fail to comply with a government or court order to take down content that is defamatory, harms national security, causes public panic, or otherwise violates the criminal code. [76] Failing to comply with order is punishable with a fine of 200,000 baht ($6,500) and an additional daily fine of 5,000 baht ($160) until the order is complied with.

B3 0-4 pts	
Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**1** / 4

Score Change: The score improved from 0 to 1 because the Criminal Court twice rejected Thai authorities' requests to restrict critical online content, suggesting that the judiciary will in limited circumstances resist the government's censorial demands.

Restrictions on online content lack transparency and are not proportionate. 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]

In a positive development, in February 2021, the Criminal Court reversed a lower court ruling that a video of Thanathorn Juangroongruangkit, leader of the now-dissolved Thai Future party, criticizing the government's COVID-19 vaccine policy be restricted on three platforms for violating the Computer Crimes Act and threatening national security. [78] In October 2020, the Criminal Court overturned an MDES order to shut down Voice TV, which had been broadcasting the student-led protests (see B2 and B8). The court also rejected the government's request to close down three online news sites: the Standard, the Reporters, and Prachatai, shut down a Facebook page run by antigovernment activists, and restrict the online activities of Free Youth. [79]

Amendments to the CCA that took legal effect in May 2017 could empower the MDES and other bodies to advance blocking requests and could expand the kind of content subject to blocking. [80] However, members to a nine-seat, ministry-appointed screening committee tasked with reviewing content-blocking requests has yet to be

announced. [81] A separate 2017 decree stated that service providers must abide by court orders to block access to websites using technical measures—a somewhat more moderate directive than a draft that had required ISPs to censor content using "whichever means necessary." [82]

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. [83] 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. [84] 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. [85] 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. [86] 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.

In September 2020, the MDES filed a legal complaint against Twitter and Facebook for not complying with takedown requests (see B2). [87] The MDES also stated it would only withdraw the complaints if future compliance of takedown requests were adhered to by the social media companies.

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. [88] Users who express dissenting views have faced online harassment and intimidation or had their personal information shared and private lives scrutinized, including from ultra-royalists (see C7).

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, and 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 COVID-19 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 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 progovernment campaigns to proceed with impunity.

In February 2021, Facebook stated it had removed 77 accounts, 72 pages, 18 groups, and 18 Instagram accounts for violating the company's government interference policy after an investigation revealed these accounts were linked to the Internal Security Operations Command (ISOC), the political arm of the Thai military. [92] In October 2020, Twitter removed 926 accounts linked to the Royal Thai Army for violating the platform's manipulation policies by spreading state-sponsored disinformation and progovernment messages and targeting opposition activists. [93] Several internal documents leaked in November 2020 suggested that the army employed 17,000 individuals to create and share disinformation and trained personnel in how to avoid being banned by Twitter. The army verified that the

documents were real but claimed they were intended to teach how to use social media effectively. [94]

Manipulated, false, or misleading online content proliferated during the 2019 election period. Most of this content aimed to discredit opposition parties and prominent figures, like the leader of the progressive Future Forward Party (FWP) and its candidate for prime minister. 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), [95] whose previous chairman was a member of the NCPO. A September 2019 report from the Oxford Internet Institute identified Thailand as having coordinated "cybertroop" teams whose full-time staff members are employed and formally trained to manipulate the information space on behalf of the government or political parties. [96]

In February 2020, the opposition Move Forward Party—which became a successor to the FWP after the latter was dissolved by the Constitutional Court—accused the government of running a malicious online campaign funded by ISOC. [97] Accounts suspected of being associated with the campaign harassed and defamed the opposition, human rights defenders, and activists, including those involved in the peace process in the country's south, and attempted to stoke division between text conversations in which participants discussed deploying fabricated social media accounts to target government critics. [98] ISOC said the documents were authentic, but that they merely described a public relations exercise meant to address fake news. [99]

The Anti-Fake News Center, established by the MDES in November 2019 to combat false and misleading information that violates the CCA, [100] continued to identify alleged fake news, particularly news related to COVID-19. 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." [101] The center also includes staff from state-owned telecommunications firms. [102] 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. [103] In May 2021, a new Fake News center was established under the Department of Special Investigation (DSI) of the Ministry of Justice to investigate information about the COVID-19 pandemic deemed to be false and undermining the government's efforts in mitigating the pandemic. [104]

Some observers, including leaders of the FWP, have noted that the government does not work to combat disinformation targeting opposition parties. [105] Instead the Anti-Fake News Center has targeted users who post content that is critical of those in power (see C3). The center has also mislabeled content. During the previous coverage period, for example, the Anti-Fake News Center labelled a Khaosod news story discussing the government's COVID-19 quarantine policy as fake, but later clarified the article was incorrectly labelled due to a procedural error. [106]

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; [107] the bill was forwarded to the House of Representatives in October 2020. [108] This law would create a national professional media council tasked with issuing codes of conduct to journalists and media outlets. [109] 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. [110]

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, [111] as well as their use of the network infrastructure of telecommunications companies. 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. [112]

Similarly, the MDES discussed the development of regulatory guidelines for over-the-top (OTT) businesses in Association of Southeast Asian Nations (ASEAN) member states at the 2019 ASEAN Telecommunication Regulators' Council (ATRC). [113] The guidelines, which were expected to be completed in 2020, [114] could include revenue collection in all ASEAN countries and a new center to supervise and filter content. [115]

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

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 2021 Report by Hootsuite and We Are Social, there were about 55 million social media users in Thailand in January 2021. The most popular platforms were YouTube, followed by Facebook, LINE, and Instagram. [116] 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. [117]

The Chinese state-run Xinhua News Agency leverages 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) to share translated Chinese state news reports, thus broadening their reach. [118] However, the actual degree of influence this material has among Thai news consumers remains unclear. In December 2020, Thai news media Khaosod English decided not to renew its partnership with Xinhua. [119]

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

Most 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). The Clubhouse App is increasingly used for users to engage in political discussions related to the monarchy, the government, and democracy in the country.

Nationwide protests calling for the reform of the monarchy surged in February 2020, after the Future Forward Party was dissolved. Though online discussions and digital activism on issues related to the monarchy are typically quite rare (see B4), during the 2020 protests, activists used social media to share information and spark discussions. 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. [120] In October 2020, prodemocracy activists used hashtags such as #WhatsHappeninginThailand to share information on the protests in English and other languages in order to gain international support. [121]

The government blocked or attempted to block platforms used during these protests. In October 2020, the government ordered the blocking of Change.org after

the website hosted a petition calling for the German government to revoke the king's diplomatic immunity (see B1). In the same month, leaked government documents outlined the government's plan to block the Telegram messaging app, which activists used to quickly organize protests (see B1). The police also reportedly ordered MDES to restrict the Free Youth group, which played a prominent role in organizing protests, on Telegram. [122]

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 (see C7). [123]

Free Youth and its leaders used Twitter to organize protest marches to the palace; [124] shortly after announcing the details of the march, the accounts of the group and its leaders were suddenly suspended (see B2).

During the campaign period leading up to the March 2019 elections, vague and restrictive rules imposed by the Electoral Commission of Thailand (ECT) limited the use of digital tools for political activism. [125] The rules required parties to notify ECT of what content they would publish and when. Furthermore, only candidates' names, photos, party affiliations, party logos, policy platforms, slogans, and biographical information could be posted on social media. 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. [126] Some candidates, such as the Pheu Thai Party's prime ministerial candidate, Sudarat Keyuraphan, resorted to deactivating their Facebook pages to avoid potential punishment. [127]

C. Violations of User Rights

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

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. [128]

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, from 2014–19, the NCPO-appointed government passed a number of laws to consolidate its power. Many 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. After activating the decree in March 2020 in response to the COVID-19 pandemic, the government passed regulations which provided 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." [129] The regulations impose criminal penalties and allow authorities to order journalists, news outlets, and media groups to "correct" reporting that authorities deem incorrect (see C2). After the coverage period, in August 2021, the Thai Civil Court prohibited the government from enforcing a new regulation issued under the decree and promulgated in July 2021. The new decree repeated the same prohibitions on disseminating any content that causes misunderstanding or instigates fear. [130] Civil society organizations voiced concerns the new regulation would allow the government to target content that was

not considered to be false information. Following the court's ruling, the prime minister revoked the regulation. [131]

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. The Constitutional Court has summoned users for posting critical content, though the courts have also rejected government requests to block content deemed to be threatening to national security or critical of the monarchy and, at times, ruled in favor of free expression in criminal cases brought against individuals (see B3 and C3). [132] However, the judiciary still suffers from a general lack of independence, as demonstrated by the Constitutional Court's disbanding of the opposition FWP in February 2020. [133]

C2 0-4 pts	
Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?	**0** / 4

A number of laws impose heavy criminal and civil penalties for online activities.

Section 14(1) of the original 2007 CCA banned introducing false information into a computer system; experts understood this to refer to technical crimes such as hacking. [134] 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. [135] However, the revised law introduced in 2017 retained the problematic term "false" computer information, and added another: "distorted" computer information. As a result, the broader 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. [136]

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 beginning in March 2020. [137] During the coverage period the cabinet repeatedly extended the state of emergency, and, as of July 2021, it was set to end in September 2021. [138] Regulations issued under the state of emergency criminalized the presentation or dissemination of news about the virus deemed false, to intentionally misrepresent the state-of-emergency provisions, or to harm public morals or public order. [139] 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). [140] 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 sent to the House of Representatives in October 2020 but has not been included in the agenda for the November 2021 legislative session (see B6).

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). [141]

C3 0-6 pts	
Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	**0** / 6

Score Change: The score declined from 1 to 0 due to the sentencing of a former revenue officer to 43 and a half years in prison for uploading radio clips critical of the monarchy on YouTube.

Authorities continued to exploit Section 14 of the CCA, the criminal code, and other broadly worded mandates 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 September 2020, the CyberCrime Investigation Bureau (CCIB) was established under the Royal Thai Police to crack down on computer crimes, particularly those related to national security and "fake news'." It has seven separate divisions to handle various cybercrimes. [142]

Users also faced charges and were arrested under the Criminal Code's Section 112 on lèse-majesté & Section 116 on sedition as well as the Computer Crimes Act, for social media activities associated with the prodemocracy protests in 2020 and 2021 (see B8). Following the growing criticism of the monarchy, the government in November 2020 reversed its earlier decision to avoid filing charges and pursuing cases under Section 112. [143] Between July 2020 and February 2021, at least 234 people were charged for their political activities online and offline with at least 358 people charged in 198 cases under Section 112 and 116 of the Criminal Code. [144]

In the most draconian sentence in recent years, Anchan Preelert, a 63-year old former revenue officer, was sentenced in January 2021 by the Appeal Court to 87 years in prison—reduced to 43 years after she plead guilty to violating Section 112 of the Criminal Code and the Computer Crime Act (CCA). [145] Anchan was sentenced for uploading to YouTube 29 audio clips of "Banpot," a radio host critical of the Thai

monarchy. Her bail was denied on the basis that her offence was serious and caused trauma to those loyal to the monarchy. [146]

In March 2021, Thai courts sentenced 21-year-old Supakorn Pinijbuth to four years and five months in jail for violating the lèse-majesté law by using different Facebook accounts to post photoshopped pictures of the king. [147]

The MDES filed a cybercrime complaint against Pavin Chachavalpongpun, the exiled academic and creator of the Facebook group Royalist Marketplace in August 2020 (see B2). [148] Members of the group have reportedly been targeted with additional CCA complaints as well as intimidation and harassment (see C7). [149]

A netizen named Narin was arrested in September 2020 on charges of violating Sections 14 (2), (3), and (5) of the Computer Crime Act for running a Facebook page called "GuKult" that produces political memes involving the monarchy, and his electronic devices were confiscated. [150] He was released in September 2020 for a bail of 100,000 baht ($3,300).

Kitti Pantapak, a reporter for Prachatai was arrested while reporting, via Facebook live, on a police crackdown of protests in October 2020. [151] He was released a few hours later after being fined for violating the Emergency Decree, which prohibits publishing or broadcasting information that threatens the country's stability.

Prodemocracy activist Karn Pongpraphapan 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 August 2020, he was out on bail of 100,000 baht ($3,300) and awaiting trial; [152] his hearing was scheduled for September 2020. [153] If convicted, he faces up to five years in prison.

In another case, the Twitter user known as 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). [154] In June 2020, the prosecutor decided not to move forward with

the case, [155] but days later Niranam was charged with more offenses under the CCA and summoned for interrogation. If convicted, he faces up to 40 years in prison. [156]

A number of users were arrested under the March 2020 emergency decree and the CCA for sharing information about COVID-19 or the government's response to the pandemic. [157] In February 2021, the Minister of Digital Economy and Society revealed that arrest warrants have been issued against 35 people for posting information that purportedly caused public panic during the pandemic. [158]

In January 2021, the MDES filed charges against Thanathorn Juangroongruangkit under Section 112 of Criminal Code for his criticism of monopoly over the COVID-19 vaccine production by Siam Bioscience, funded by the King. [159] The complaint was filed over a 30-minute Facebook Live video that was also uploaded to YouTube, in which Thanathorn shared his opinion. After the coverage period, in August 2021, Thanathorn received two additional lèse majesté charges for his statements. [160]

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. [161] If convicted, he faces up to five years in prison. In a July 2020 trial, prosecutors requested he receive the maximum possible sentence. [162] There were no apparent developments in the case during the coverage period.

Private companies and individuals often file defamation cases against human rights defenders, activists, and journalists for their online activities. In December 2019, the Thai poultry company Thammakaset Co. Ltd, filed a defamation case against former Voice TV reporter Suchanee Rungmuanporn after she wrote a Twitter post discussing a complaint against the company filed with the National Human Rights Commission by migrant workers. She was sentenced to two years in prison for criminal defamation under Section 328 of the criminal code [163] and later released on bail of 75,000 baht ($2,500) pending an appeal against the judgment. [164] In October 2020, the Court of Appeals reversed her sentencing, recognizing her right to investigate and give her opinion as a member of the press. [165]

In June 2020, Thammakaset filed two new criminal defamation charges against former National Human Rights Commission member Angkhana Neelapaijit; [166] the company had previously initiated a case against Neelapaijit after she shared two Twitter posts in support of women human rights defenders facing defamation charges filed by the company. [167] The case commenced in November 2020. [168] After the coverage period, a criminal court set the first hearing for October 2021 and granted Neelapaijit bail. [169]

There have been some positive developments in cases regarding online speech in recent years. In June 2020, 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. [170] Thanet was released after spending three years and 10 months in prison. [171]

Cases have also been decided in favor of those charged after trials moved from military to civilian courts. In December 2020, Patnaree Chankij, the mother of prodemocracy activist Sirawith Seritiwat, was found not guilty of violating Section 112 in connection with communications with her son's friend, who themselves had been charged with violating lèse majesté laws. [172] In January 2021, a former factory worker, Thanakorn (whose surname was withheld by Thai outlets), was acquitted of violating lèse majesté and computer crimes laws by mentioning the late king's dog, after the case moved to the civil court. [173] Also, in December 2020, former Deputy Prime Minister Chaturon Chaisingh was acquitted of charges under Section 116 on sedition and under CCA for holding a press conference in defiance of military coup leaders in May 2014, concluding a six-and-a-half-year legal battle. [174]

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. [175] 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. [176] 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, [177] and a number of phones were disconnected starting in April 2020. [178] 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. [179]

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. [180] 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). [181] The group also 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. [182]

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.

Sections 18 (1) to 18 (3) of the CCA allows the government to access user-related or traffic data without court order and compel ISPs to decode programmed data. [183]

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). [184]

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. [185] 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. [186]

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, at times even baiting users to criticize the monarchy or the junta. [187] In several cases in which individuals were summoned or arrested, the authorities also confiscated smartphones to access social media accounts (see C3).

Government agencies possess a variety of surveillance technologies. A 2020 report by CitizenLab identified Thailand as a likely customer of Circles technology. [188] Separately, some agencies bought spying software from the Milan-based company Hacking Team between 2012 and 2014, according to leaked documents; [189] Thailand has also obtained licenses to import telecommunications interception equipment from Switzerland and the United Kingdom. [190] 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.

Social media monitoring is also of concern in Thailand. The Anti-Fake News Center collects information through the use of artificial intelligence that is then reviewed by human content monitors (see B5). [191] 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. In February 2021, the MDES warned government employees that their activity on the Clubhouse app was being monitored, and those that distorted information or violated laws on the app would be punished. [192]

The 2019 National Intelligence Act 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. [193] The prime minister is in charge of the implementation of this act.

In response to COVID-19, the MDES initially introduced a mobile app to track and monitor people returning to Thailand from high-risk countries. This app requires submission of personal information and was made mandatory for all foreign arrivals. Although the information collected is reportedly only stored until the end of a person's self-quarantine, [194] the uncertainty about how and by whom information is used raise serious concerns about privacy rights. [195] These apps include MorChana, a mobile app that uses GPS, Bluetooth and QR Code to trace the location of a user to trace persons at risk; and ThaiChana, an online platform where users may register themselves while entering a public venue using a QR code to check in and check out. [196] The Digital Government Development Agency has access to personal data of MorChana users and shares it with the Department of Disease Control (DCD), who will delete the data only when the pandemic is deemed over. Check-in data from Thai Chana users is deleted every 60 days. MorChana has faced criticism because of the

gaps and lack of transparency in its privacy policy. [197] ThaiChana has no privacy policy at all.

C6 0-6 pts	
Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	**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 Computer Crime Act (CCA). This data would include information that allows the identification of users. Failing to retain this data could lead to a fine of up to 500,000 baht ($16,650), presenting an additional financial burden to service providers. [200]

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. [201] 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 2022. [202] The law outlines how businesses can collect, use, or disclose personal information. [203] 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. [204]

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 Defense (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. [205] The MOD denied the report, although it confirmed that it had met with major mobile service providers about tracking the virus. [206] 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 2020. Google received one request for data regarding two users or accounts but complied with none between January and July 2020. [207] LINE, the most popular chat application in Thailand, reported receiving one request from law enforcement for user data in the first six months of 2020 which it did not comply with. [208] Between

July and December 2020, Facebook received 103 requests for data regarding 136 users or accounts and provided 69 percent of the data requested. [209]

Service providers surrendering user data 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). [210]

C7 0-5 pts	
Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?	**1** / 5

Score Change: The score improved from a 0 to 1 because there were no reported cases of enforced disappearances of users for their online activities within Thailand during the coverage period.

Prodemocracy activists and individuals who criticize the monarchy have been subjected to extralegal intimidation and violence, in an apparent connection with their online actions. Although the whereabouts of previously forcibly disappeared activists remain unknown, there were no reported instances during the coverage period of enforced disappearances of people in Thailand.

There have been several instances of Thai dissidents being abducted while abroad. In June 2020, Wanchalearm Satsaksit, a critic of the government and the monarchy, was forcibly disappeared from outside his home in Cambodia. [211] He faced pending charges under Section 112 and 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 February 2021. [212]

In May 2019, three antimonarchy activists who face lèse-majesté charges in Thailand —Siam Theerawut, Chucheep Chivasut, and Kritsana Thaptha—were forcibly disappeared in Vietnam after leaving Laos. Civil society groups reported that they were then handed to Thai authorities, a claim authorities deny. [213] Their whereabouts remain unknown. [214]

In December 2018, another three Thai prodemocracy and antimonarchy activists—Surachai Sae Dan, Kraidej Luelert, and Chatchan Buphawan—disappeared while living in Laos. [215] 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 Thai government has similarly denied any responsibility. [216]

Authorities are known to use intimidation tactics to pressure users to remove content or self-censor (see B2 and B4). Among the most extreme recent cases was that of Tiwakorn Withiton, who went viral in a July 2020 photo wearing a T-shirt reading "I lost faith in the monarchy." Police first summoned him to demand he stop wearing the shirt; [217] after refusing he was forcibly remanded to a psychiatric hospital, his computer and smart phone were seized, and his mother was forced to sign a document without being informed of its contents. Tiwakorn was eventually released, but was subject to surveillance and temporarily banned from seeing his family. [218] A Bangkok university student was visited by plainclothes police officers after he shared information on Tiwakorn's case, and another user was arrested and interrogated after he used a picture of Tiwakorn's T-shirt as his Facebook cover photo.

Prodemocracy activists who are vocal online were assaulted inside and outside Thailand during previous coverage periods. Student activist Sirawit Seritiwat was violently assaulted twice in June 2019, [219] with police offering him protection only if he gave up his activism. [220] Independent political activist Ekkachai Hongkangwan has been assaulted at least seven times since January 2018, [221] and scholar Pavin Chachavalpongpun, who lives in Japan, was attacked with chemicals in July 2019. [222] The Thai police have not conducted thorough investigations into the threats and attacks, and in some cases have even halted investigations, [223] instead blaming the activists for the attacks perpetrated against them. [224]

Individuals who expressed critical opinions about the monarchy received online and offline threats and intimidation (see B2 and C3). In November 2020, the information of a journalist who authored an article exposing government coordinated disinformation tactics was leaked on social media. [225] Some participants in the

Royalist Marketplace Facebook group have been doxed on social media, threatened by police, or threatened with the loss of their jobs. [226]

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. [227] 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. [228]

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, [229] identified a number of advanced persistent threats (APTs) that attacked Thai websites between 2018 and 2020, including those dubbed FunnyDream, Cycldek, and Zebrocy. [230] 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. Zebrocy is a Russian APT that targets Thai entities as well. [231] The Provincial Electricity Authority, which supplies electricity to all of Thailand except for Bangkok, experienced a ransomware attack in June 2020. [232]

Private sector entities and individuals were also subjected to technical attacks. The SilentFade malware, which hacks users' Facebook accounts to purchase ads for

fraudulent services, rapidly spread across Southeast Asia in January 2021, with 27 of 576 incidents taking place in Thailand. [233] In November 2020, e-commerce and communication companies including Lazada, Shopee, and Line suffered a data hack risking the personal and financial data of users. Over 13 million Thai users were compromised in the hack on Lazada. [234]

Hackers demanded 200,000 bitcoins (103 billion baht; $3.4 billion) in a September 2020 ransomware attack that left Saraburi Hospital's patient records damaged or inaccessible. [235] As a result, the Ministry of Public Health committed to investing 1.9 billion baht ($62 million) to install a data-protection system at state run hospitals. [236] It was also revealed that between January and November 2020 alone, there were 1,969 cyberattacks targeting agencies and organizations related to infrastructure, entertainment, finance and in the public health sector. [237]

A leading independent online news outlet, Prachatai, [238] was subject to distributed denial-of-service (DDoS) attacks in previous coverage periods.

The Cybersecurity Act came into force in May 2019. [239] The law aims to protect against, address, and mitigate cybersecurity threats. [240] 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. [241] 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. [242] Noncompliance can result in imprisonment and heavy fines.

• • •

Footnotes

1 Simon Kemp, "Digital 2021: Thailand," Datareportal February 11, 2021, https://datareportal.com/reports/digital-2021-thailand

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

3 Simon Kemp, "Digital 2021: Thailand," Datareportal February 11, 2021, https://datareportal.com/reports/digital-2021-thailand

4 Simon Kemp, "Digital 2021: Thailand," Datareportal February 11, 2021, https://datareportal.com/reports/digital-2021-thailand

5 Internet Information Research Network Technology Lab, "About Internet Bandwidth (Internet Bandwidth)," National Electronics and Computer Technology Center, Accessed September 2021, 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

Not 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 2021

Other Years

2023

Be the first to know what's happening.

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