Freedom House

FREEDOM ON THE NET 2022

Thailand

NOT FREE

39 /100

A. Obstacles to Access	16 /25
B. Limits on Content	14 /35
C. Violations of User Rights	9 /40

LAST YEAR'S SCORE & STATUS

36 /100 Not Free

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

Overview

The internet is severely restricted in Thailand. A wide-ranging crackdown on online expression was carried out by the military-led regime in response to prodemocracy protests that started in July 2020 and continued throughout the coverage period. Authorities significantly increased the use of lèse-majesté law and sedition, charging and imprisoning individuals for online expression. Prodemocracy activists face heavy prison sentences. State-sponsored attacks, intimidation, and harassment targeting individuals for their online activities also continued. The government repeatedly extended the enforcement of a repressive emergency declaration issued in response to the COVID-19 pandemic, imposing further constraints on fundamental freedoms, though the courts found some measures unconstitutional.

Following five years of military dictatorship, Thailand transitioned to a military-dominated, semielected government in 2019. The combination of democratic deterioration and frustrations over the role of the monarchy in Thailand's governance has since triggered massive demonstrations. In response, the regime continues to employ authoritarian tactics, including arbitrary arrests, intimidation, lèse-majesté charges, and harassment of activists. Press freedom is constrained, due process is not guaranteed, and there is impunity for crimes committed against activists.

Key Developments, June 1, 2021 - May 31, 2022

- The merger of mobile service providers TRUE and Total Communication Access (DTAC) was announced in November 2021; the consolidation of the market may present affordability concerns, though the communications regulator indicated it may not have the authority to review the merger (see A2 and A4).
- Authorities sought to restrict access to content relating to criticism of the government, including by blocking a website mobilizing support to repeal the

lèse-majesté law in February 2022 (see B1, B2, and B8).
- The Constitutional Court held in November 2021 that speech calling for reform of the monarchy constitutes an attempt to overthrow the king, impacting online expression (see B4 and C1).
- Internet users were arrested and charged for speech calling for government reform, with authorities notably sentencing an activist to six years' imprisonment over Facebook posts during the coverage period. However, no multidecade prison sentences were issued, in contrast to the previous coverage period (see C3).
- According to a report released in July 2022, the Thai government likely deployed spyware against prodemocracy advocates, researchers, and politicians during the reporting period (see C5).
- There were no reported cases of direct violence in retaliation for peoples' online activities, though extralegal intimidation, online harassment, and doxing 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 DataReportal's *Digital 2022* report, Thailand's internet penetration rate was 77.8 percent and there were 54.5 million internet users as of January 2022, a 0.2 percent increase from January 2021. [1]

Mobile internet penetration is high. By January 2022, 96.2 percent of internet users used a mobile phone to connect, compared with 97.7 percent in 2021. [2] In contrast, 50.6 percent of users in the same period accessed the internet through laptop and desktop computers—a decrease from 64 percent in the previous year. [3]

According to Ookla's Speedtest Global Index, median mobile and fixed-line broadband download speeds stood at 33.7 megabits per second (Mbps) and 188.8 Mbps, respectively, as of May 2022. [4]

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. [5] After being the first mobile service provider to launch its 5G network, [6] Advanced Info Service (AIS) had signed 2.2 million subscribers by the end of 2021, [7] and is operating more than 18,700 5G base stations running across all 77 provinces of Thailand. [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. According to the National Statistics Office, about 56 percent of internet users spend 200 to 599 baht ($7 to $20) per month to access the internet as of 2018, the most recent available data, while 21 percent pay under 200 baht per month. [9] The 2021 Affordability Drivers Index estimates that 1 gigabyte (GB) of mobile broadband service costs 1 percent of Thailand's gross national income (GNI) per capita. [10] As of 2018, nearly 11 percent of the population accessed the internet through free programs. [11]

Some observers expected the rollout of 5G service to increase internet accessibility due to lower costs; [12] 5G spectrum licenses, however, are more expensive than anticipated, [13] and these costs could be transferred to internet users. [14] After mobile service providers TRUE and DTAC announced their merger plans in November 2021, [15] government officials raised concerns that the deal would lessen market competition, possibly leading to price hikes (see A4). [16]

Government programs have sought to reduce the persistent digital divide between urban and rural areas. [17] Initiated in early 2016, 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. The state-owned TOT Public Company Limited had installed Wi-Fi hotspots in 24,700 locations as of 2017, and the intended reach of this program was extended to an additional 15,732 villages in rural areas and 3,920 villages in border areas. [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. In early 2020, the 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 postpaid mobile phone users. [20] Additionally, in January 2021, the NBTC ordered all mobile and fixed-line 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 speeds 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 service providers, AIS, TRUE, and 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 fixed-line or mobile connections during the coverage period, though the government does have some capability to do so through technical control over internet infrastructure.

In January 2020, National Telecom was formed through a merger of CAT Telecom and TOT, both of which are owned by the state. CAT Telecom previously operated 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 Telecom until it opened to competitors in 2006. [26] While the merger of CAT Telecom and TOT was intended to help the public firms compete with private telecommunications companies, [27] 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. [28] Although it was unclear whether this controversial "single gateway" would be implemented in subsequent years, [29] Chaiwut Thanakamanusorn, who heads the Ministry of Digital Economy and Society (MDES), said in February 2022 that he was considering the idea, citing the need to deter cybercrime and other criminal activity. [30]

The Cybersecurity Act centralizes authority over public and private service providers in the hands of government entities (see C6). 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. [31]

The law does not provide transparency concerning government decisions and lacks an effective system of accountability if connectivity restrictions were to be implemented. [32]

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

Although 20 ISPs have licenses to operate in Thailand, the largest three controlled almost 85 percent of the market during the coverage period. According to an NBTC

report released in December 2021, TRUE Online led the sector with 36.1 percent, followed by Jasmine with 29.9 percent and state-owned TOT with 18.8 percent. AIS, Thailand's top mobile service provider, which entered the fixed-line broadband market in 2015, accounted for 11.5 percent. [33]

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—their future market shares may increase. [34]

In the mobile sector, AIS held a market share of 44 percent as of first quarter of 2021. TRUE held 32.3 percent, and Norwegian-controlled DTAC followed with almost 20 percent. [35] 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. In November 2021, TRUE and DTAC announced their plans to merge. The announcement prompted concerns about negative implications for consumers stemming from a mobile-service duopoly. [36] As of August 2022, the NBTC commission was reportedly split on whether the regulator had the authority to approve or deny the merger. [37]

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 through appointments which starkly exemplify the revolving door between the government and the private telecommunications sector." [38]

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 commissioners are selected in a process that is highly controlled by the government. After receiving Senate approval in December 2021, new NBTC commissioners were appointed only in April 2022. [39] The delay was allegedly caused by the government's intention to retain the former commissioners. [40] The February 2021 NBTC Act further removed requirements that candidates have experience in relevant spheres. [41] NBTC commissioners are paid extremely well and have significant influence over the multibillion-baht telecommunications sector. [42]

The government in turn has significant influence over the decisions of the NBTC. For example, the NBTC temporarily suspended the media broadcaster Voice TV in 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 Ministry of Information and Communication Technology 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. [46] Chaired by the prime minister, the CDES is composed of government ministers and no more than eight qualified experts. [47] It is not a government body and therefore not accountable to laws that regulate government agencies, though it has authority over the MDES and NBTC. Other bodies that influence policy include the Digital Economy and Society Development Fund and the Office of Digital Economy Promotion.

In 2020 and 2021, additional bodies to operationalize the Cybersecurity Act were established. The Cybersecurity Act created the National Cybersecurity Committee

(NCSC), the Cybersecurity Regulating Committee (CRC), the Office of the NCSC, and the Committee Managing the Office of the NCSC (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 January 2022, the committee tasked with implementing the Personal Data Protection Act (PDPA) was established, with mainly government officials as members. [52]

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. [53]

In November 2021, the MDES received court authorization to block 71 URLs related to illegal gambling and 9 URLs for national security reasons. [54] In the first half of 2022, the MDES sought court orders to block illegal websites and, as of June 2022, 2,630 URLs were blocked in total: 1,231 URLs for allegedly insulting the monarchy, 876 URLs related to online gambling, and 312 related to content deemed unethical. [55] In February 2022, MDES blocked no112.org, which hosted an online petition calling for the repeal of the lèse-majesté law, due to its alleged violation of the CCA and the

Gambling Act. [56] Access was restored that month; nevertheless, the website was inaccessible at times between February and May 2022. [57]

In the previous coverage period, the MDES blocked 1,457 URLs related to gambling and other 190 websites, including Pornhub, for the sharing of pornographic content. [58] In October 2020, a secret MDES order was discovered; it directed internet service providers (ISPs) and mobile service providers to block four internet protocol (IP) addresses linked to Telegram, a messaging app used by protesters to communicate and organize. [59] 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. [60]

The government has never publicly revealed the number of URLs blocked by court orders. However, MDES reported that throughout the second half of 2020 it obtained court orders to block roughly 8,440 URLs containing allegedly offensive content to the monarchy; the URLs were mainly on Facebook, YouTube, and Twitter. As of the end of 2020, only 5,025 of them were blocked. [61]

Websites offering tools for online anonymity and circumvention of censorship, as well as VPNs, have been blocked by more than one ISP. [62] The website of the VPN Hotspot Shield, [63] for example, used to be blocked by TRUE, while Ultrasurf, another VPN, was blocked by DTAC, AIS, and 3BB as of February 2021.

Since 2017, courts have issued orders to block or disable access to URLs over copyright infringement; more than 1,500 URLs were blocked as of October 2021. [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?	**1** / 4

Score Change: The score improved from 0 to 1 because while the MDES and service providers continued to engage in large-scale blocking activities, fewer reports of

individual internet users facing forced content removals appeared during the coverage period.

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).

The government pressures and intimidates users, publishers, and content hosts to remove content. Some of the 2,630 URLs restricted by the MDES in the first half of 2022 included content removed from social media platforms; in June 2022, the MDES publicly thanked YouTube and TikTok for assisting the Thai government, with both platforms complying with 100 percent of its orders. [65] In May 2022, the MDES sought court orders to remove 42 YouTube, Twitter, and Facebook pages that allegedly defamed the monarchy by sharing an ad from the online shopping platform Lazada. [66] In May 2021, during the previous coverage period, the government ordered 12 social media users to remove content related to the COVID-19 pandemic or face legal consequences. [67]

Between July and December 2021, Facebook restricted access to 77 posts allegedly violating Section 112 of the criminal code on lèse-majesté and 1,754 posts in response to reports submitted by the Thailand Food and Drug Administration. [68] According to Google's transparency report for the same period, the government sent 162 requests to remove 436 items across various Google services, 70 percent of which were removed. [69] Some 96 percent of the requests were related to criticism of the government. During the same period, Twitter received 50 legal demands to remove content in relation to 130 accounts, complying with 12 percent. [70]

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, which called for royal reforms and showcased images of the 2020 antigovernment youth-led protests. [71] In August 2020, the government ordered Facebook to block Thai-based users' access to a popular Facebook group

created by a prominent critic of the monarchy, which featured discussions about the king. [72] Facebook complied but announced that it would legally challenge the order. [73]

In June 2021, courts ordered Facebook and ISPs 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, [74] and are still accessible as of June 2022.

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. [75] Failing to comply with order is punishable with a fine of 200,000 baht ($5,900) and an additional daily fine of 5,000 baht ($148) until the order is complied with.

In September 2020, the MDES filed a legal complaint against Twitter and Facebook for not complying with takedown requests. [76] Although the MDES initially stated it would only withdraw the complaints if social media companies complied with future orders, it dropped them in April 2021. [77]

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

Restrictions on online content lack transparency and are not proportionate. Both the Anti-Fake News Centre and the COVID-19-specific emergency declaration allow authorities to issue correction notices for online content (see C1). [78]

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 CCA and threatening national security. [79] In October 2020, the Criminal Court overturned an MDES order to shut down

Voice TV, which had been broadcasting student-led protests. The court also rejected the government's request to close down the Standard, the Reporters, and Prachatai news sites, shut down a Facebook page run by antigovernment activists, and restrict the online activities of Free Youth. [80]

The 2007 CCA, which subjects providers or intermediaries to prosecution for allowing the dissemination of content considered harmful to national security or public order, was amended in May 2017. [81] The amendments could empower the MDES and other bodies to advance blocking requests and could expand the kind of content subject to blocking. [82] However, members to a ministry-appointed screening committee tasked with reviewing content-blocking requests has yet to be announced as of the end of the coverage period. [83] The amendments provide some protection for intermediaries through a notice-and-takedown system. Still, certain sections of the amendments appear to hold individuals responsible for erasing banned content on personal devices, though how this rule might be enforced remains unclear. [84]

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." [85]

Another MDES decree from July 2017 established a complaints system for users to report banned content and incentivized intermediaries to act on every complaint to avoid liability. [86] 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 such content. [87] 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.

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 ultraroyalists (see C7).

Most Thai internet users and journalists self-censor on public platforms when discussing the monarchy because of the country's severe lèse-majesté laws (see C2). This was particularly true after the Constitutional Court ruled that protesters' calls for reform of the monarchy amounted to an attempt to overthrow it (see C1). In the wake of the said ruling, the NBTC warned the media against covering prodemocracy protests calling for reform of the monarchy and that noncompliant outlets risk criminal prosecution; [89] this led to increased self-censorship by media and ordinary users.

However, since late 2019, several hashtags questioning the government and the monarchy went viral on Twitter, [90] including one which highlighted the absence of moral and financial support from the king while the country was overwhelmed with

the COVID-19 pandemic; this hashtag was shared over 1.2 million times within 24 hours. MDES did not directly address the hashtag but warned people against breaking the law online. [91] In May 2021, internet users criticizing the government's harsh response to protests and its handling of the coronavirus pandemic used the #**ย้ายประเทศกันเถอะ** ("Let's move countries") hashtag, which was prevalent across multiple social media platforms at the time and featured in a Facebook group with the same name. [92] The MDES instructed its staff to review the content of the Facebook group and take legal action if any illegal content was found; [93] the group's name changed to **ข่าวทั่วไป** ("general news") later that month. [94]

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 (HRDs), and certain segments of the population. Official efforts to combat disinformation are allegedly selective, allowing progovernment campaigns to proceed with impunity.

Social media companies have removed accounts that were linked to the Thai military. [95] [96] Several internal documents leaked in November 2020 suggested that the army employed 17,000 individuals to create and share disinformation and trained personnel on how to avoid being banned by Twitter. The army verified the documents' veracity but claimed they were intended to teach how to use social media effectively. [97]

Manipulated, false, or misleading online content proliferated during the 2019 election period, with most of this content aimed at discrediting opposition parties and prominent figures. 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, [98] whose previous chairman was a member of the NCPO.

In February 2020, the opposition Move Forward Party (MFP)—which became a successor to the Future Forward Party (FFP) after the latter was dissolved by the Constitutional Court—accused the government of running a malicious online campaign funded by the Internal Security Operations Command (ISOC), the political arm of the Thai military. [99] Accounts suspected of being associated with the campaign harassed and defamed the opposition, HRDs, and activists, including those involved in the peace process in the country's south, and attempted to stoke division; participants discussed deploying fabricated social media accounts to target government critics via text conversations. [100] The ISOC said the documents were authentic, but that they merely described a public relations exercise meant to address news deemed false. [101]

In August 2021, an MFP parliamentarian shared documents detailing the structure of the Thai army's network of commentators, which includes soldiers designated to spread progovernment sentiments, respond to criticism of the government, and target political opposition figures online. The politician also criticized the ISOC's budget request for 361 million baht ($10.6 million) for information operations. [102] In 2021, the military allegedly signed contracts with public relations companies to enhance the quality of their campaigns, [103] and signs of a "cyber army" spreading online disinformation have been growing.

In May 2022, the Bangkok Civil Court held initial hearings in a case against the government brought by women HRDs Angkhana Neelapaijit and Anchana Heemina, who alleged that ISOC violated rules on official conduct by disseminating disinformation to manipulate public opinion about them. [104]

The government has invested in efforts to purportedly fight misinformation. The Anti-Fake News Centre, established by the MDES in November 2019 to combat false and misleading information that violates the CCA, [105] continued to identify news considered false, particularly related to COVID-19, and release "corrections." In May 2021, a new center was established under the Department of Special Investigation of

the Ministry of Justice to investigate pandemic-related information deemed to be false and undermining the government's efforts in mitigating the pandemic. [106] The establishment of three levels of centers to combat disinformation on social media is stipulated in the Draft Regulation on Prevention, Suppression and Solving Problems of Fake News Dissemination on Social Media, which the cabinet approved in February 2022. [107]

Some observers, including leaders of the FFP, have noted that the government does not work to combat disinformation targeting opposition parties. [108] The Anti-Fake News Centre has instead targeted users who post content that is critical of those in power (see C3). While the government's crackdown on expression has been heavily criticized, Prime Minister Prayuth Chan-ocha exalted the authorities for their success in the campaign against "fake news" in a September 2021 statement. [109] The Anti-Fake News Centre detected more than one million such items posted online between November 2019 and the end of 2021. [110]

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 cabinet approved the Draft Media Ethics and Professional Standards Promotion Act in January 2022. The draft law would require media organizations to register with the new government-appointed Media Council, which would oversee their activities and set ethical standards for reporting. Upon any failure to align their activities with those standards, media outlets risk having their licenses revoked and hefty fines, further limiting their resources. [111]

The NBTC has previously signaled its intent to scrutinize the amount of advertising revenue digital media receive in comparison to traditional broadcasters, [112] as well as their use of the network infrastructure of telecommunications companies. New value-added tax (VAT) rules that came into effect in September 2021 require foreign digital service providers to pay a 7 percent VAT on sales if they earn more than 1.8 million baht ($53,300) annually. [113]

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. [114] The guidelines, which were expected to be completed in 2020 [115] and had not been issued at the end of the coverage period, could include revenue collection in all ASEAN countries and a new center to supervise and filter content. [116]

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 DataReportal's Digital 2022 report, there were 56.9 million social media users in Thailand in January 2022. The most popular platforms were Facebook, LINE, TikTok, and Instagram. [117] Given the offline restrictions on expression, assembly, and association, civil society groups, activists, and politically engaged youths have turned to social media, particularly Twitter, to express opinions and garner support for democracy and human rights. [118]

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, to share translated Chinese state news reports, thus broadening their reach. [119] In December 2020, Thai outlet Khaosod English decided not to renew its partnership with Xinhua. [120]

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).

Nationwide protests calling for the reform of the monarchy surged in February 2020, after the FFP was dissolved. Though online discussions and digital activism on issues related to the monarchy are typically quite rare (see B4), activists used social media to share information and spark discussions during the 2020–22 protests. For example, a hashtag that translates as "If politics were good" trended on Twitter, spurring discussion about the potential dimensions of Thai politics under a more democratic structure. [121] Since August 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, and its use escalated that October. [122] In 2021, the top four hashtags were #Mob18July, #Mob1August, #Mob7August, and #Mob10August—all referring to protest mobilization—which accounted for 38.1 million mentions. [123]

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). The online petition platform no112.org was blocked or was otherwise inaccessible on several occasions during the coverage period (see B1). [124] The government also charged individuals for launching online campaigns against

the monarchy. Tiwakorn Withiton was charged with sedition in March 2022 for running a campaign on Change.org that called for a referendum on abolishing the royal institution (see C7). [125]

The Draft Act on the Operations of Not-for-Profit Organizations may have a wide-ranging impact on online organizing. Originally approved by cabinet in February 2021, the latest draft, dated January 2022, contains numerous provisions that would subject not-for-profit organizations (NPOs), which are broadly defined, and its members to excessively restrictive measures. As the draft law's language is very vague, almost any act may violate the law. [126] The bill is yet to enter into force.

The June 2020 disappearance of Thai activist Wanchalearm Satsaksit in Cambodia contributed to the growth in online activism, particularly among younger people, with the hashtag #SaveWanchalearm remaining popular more than a month later (see C7). [127] The hashtag #abolish112 was also tweeted many times following his disappearance and has been extensively used ever since. [128]

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 2017 constitution, drafted by the military government following the 2014 coup, 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.

The 2005 Emergency Decree on Public Administration in a State of Emergency restricts both online free expression and press freedom, and the government activated the decree in March 2020 in response to the COVID-19 pandemic. The cabinet has repeatedly extended the state of emergency, including through the end

of the coverage period. [129] As of September 2022, authorities announced that the state of emergency would lapse in October. [130] In July 2021, the government promulgated Regulation 29 using its decreed powers; the regulation would have authorized the suspension of internet services for those who share content that may "instigate fear," "mislead," or affect security. In August 2021, Prayuth revoked the regulation after the Civil Court suspended it. [131] Civil society voiced concerns the new regulation would allow government to target content that was not considered to be false information. Following the court's ruling, the prime minister revoked the regulation. [132]

The amended Communicable Diseases Act (CDA) is expected to become the primary legislation governing Thailand's COVID-19 response on the expiration of the state of emergency. Thai civil society groups and UN experts expressed their concern over the law's repressive provisions, which could similarly restrict freedom of expression, and the lack of transparency around amendments to the CDA approved by the cabinet in September 2021. [133]

Thailand's judiciary is independent under the constitution, but in practice the courts suffer from politicization and corruption [134] and often fail to protect freedom of expression. In November 2021, the Constitutional Court ruled that activists' call for royal reform constituted an attempt to overthrow the monarchy, setting a dangerous legal precedent for freedom of speech. [135]

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). [136]

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 revised CCA banned introducing false or distorted information into a computer system; experts understood this to refer to technical crimes such as hacking. [137] However, the clause has been broadly interpreted and used by the government to intimidate and silence critics. [138] 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.

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.

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 ($1,190). [140]

The Draft Media Ethics and Professional Standards Promotion Act, which was approved by the cabinet in 2022, would impose fines under a multitiered system; offending outlets could face fines of up to 10,000 baht ($296), at least 20,000 baht ($592), or at least 30,000 baht ($889). [141]

C3 0-6 pts	
Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	**1** / 6

Score Change: The score improved from 0 to 1 because extreme prison sentences were not imposed against internet users during the coverage period, though activists still face arrest and multiyear prison terms for their online activities.

Authorities continued to exploit Section 14 of the CCA, the criminal code, and other broadly worded mandates to silence opposition politicians, activists, HRDs, and civil society groups during the coverage period.

Users were arrested and charged under the CCA as well as Sections 112 (which addresses lèse-majesté) and 116 (sedition) of the criminal code for social media activities associated with the 2020–22 prodemocracy protests (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. [142] Between November 2020 and June 2022, at least 216 lèse-majesté lawsuits were documented against 201 people, including university students and minors, 107 of which stemmed from online commentary. [143]

Lèse-majesté defendants face multiple prosecutions, with some facing cumulative prison terms ranging from 120 to 300 years. Student activist Parit Chiwarak received bail for three months in February 2022, after being detained for over six months; Chiwarak faces numerous charges under the CCA, Section 112, and Section 116. Complaints were filed against him over two Facebook posts dating back to December 2020 about King Maha Vajiralongkorn's divorce from his ex-wife and the holding of funerals in Sanam Luang, a Bangkok park where police arrested volunteers. [144] Chiwarak could face a centuries-long sentence if convicted of all charges. [145]

Activist Tantawan "Tawan" Tuatulanon was arrested and charged with lèse-majesté and violating the CCA in March 2022 for live-streaming a royal procession and stating that demonstrators were removed from the street to allow the motorcade to pass. Tantawan was arrested by about 60 police officers and detained for two nights; she was released on bail of 100,00 baht ($2,960). [146] Tantawan's bail was revoked in April but she was later placed under house arrest after she engaged in a 36-day hunger strike and her health subsequently deteriorated. [147]

In March 2021, during the previous coverage period, 21-year-old Supakorn Pinijbuth received a four-year-five-month prison sentence for lèse-majesté by using different Facebook accounts to post photoshopped pictures of the king. [148] 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 CCA. [149] Anchan was sentenced for uploading audio clips of "Banpot," a radio host critical of the monarchy, to YouTube. Her bail was denied on the basis that her offense was serious and caused trauma to the monarchy's supporters. [150]

The government has escalated its efforts to stifle public expression on other topics, imposing excessive penalties. In May 2022, prodemocracy activist Ekachai Hongkangwan received a one-year prison term for CCA violations stemming from internet posts discussing overcrowding and unsanitary conditions in a Bangkok prison. [151] Sombat Thongyoi, a former protest guard for the United Front for Democracy against Dictatorship, was sentenced to six years' imprisonment in May 2022 for royal defamation and violating the CCA; Sombat had authored Facebook comments on the king in 2020. [152]

In September 2021, student activist Panusaya Sithijirawattanakul was arrested and charged under Section 116 of the criminal code and Section 14 of the CCA for running the Facebook page of the United Front of Thammasat and Demonstration, a student-led prodemocracy group; Panusaya was accused of sedition according to a press report. She was received bail of 35,000 baht ($1,040). [153] Panusaya faces as many as 135 years in prison, if found guilty on all charges. [154]

Law enforcement agencies have used the Anti-Fake News Centre and the pandemic-related emergency declaration to arrest internet users. In September 2020, the Cybercrime Investigation Bureau 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. [155] The MDES revealed that at least 135 cases of "fake news" were prosecuted from January to September 2021. [156]

Internet users have been arrested under the March 2020 emergency decree, under the CCA, and on defamation charges for sharing information about COVID-19 or the government's response to the pandemic. [157] In July 2021, rapper Danupha "Milli" Kanateerakul was fined 2,000 baht ($60) for criticizing the government's slow pandemic response via Twitter. As more Thai celebrities began expressing their disaffection with the government, the MDES warned they could face prosecution under the CCA for "distorting information and inputting fake news onto social media." [158]

In January 2021, the MDES filed charges against Thanathorn Juangroongruangkit under Section 112 of the criminal code for criticizing Siam Bioscience's exclusive production of a COVID-19 vaccine; the company is effectively owned by the monarch. [159] The complaint was filed over a 30-minute Facebook Live video that was also uploaded to YouTube, in which Thanathorn shared his opinion. In August 2021, Thanathorn received two additional lèse-majesté charges for his statements. [160] In April 2022, Thanathorn was indicted for both charges, which carry a combined sentence of up to 20 years' imprisonment. He was released on bail. [161]

In June 2022, after the coverage period, an individual was sentenced to 12 years in prison over four messages he posted in the Royalist Marketplace Facebook group that allegedly defamed the king. The sentence was reduced to six years after he pled guilty to violating Section 112 of the criminal code and Section 14(3) of the CCA. [162] He was released on bail. Also in June 2022, three social media influencers were indicted for a video promotion for the Lazada e-commerce network in May 2022 which allegedly insulted the monarchy. [163] Piyabutr Saengkanokkul, a legal scholar and secretary general of the Progressive Movement, was charged under Section 112 in June 2022 over a Twitter post calling for democracy reforms. [164]

Cases from previous coverage periods remain ongoing. 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). [165] If convicted, he faces up to five years in prison. As of June 2022, the court has not issued a decision in this case.

In another case, a 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). [166] In June 2020, the prosecutor decided not to move forward with the case, [167] but days later Niranam was charged with more CCA-related offenses and summoned for interrogation. If convicted, he faces up to 40 years in prison. [168] The case remains ongoing as of the end of the coverage period.

Private companies and individuals often file defamation cases against HRDs, activists, and journalists for their online activities. In June 2020, Thammakaset, a poultry company, filed two criminal defamation charges against former National Human Rights Commission member Angkhana Neelapaijit; [169] the company had previous initiated a case against Neelapaijit after she shared two Twitter posts in support of women HRDs facing defamation charges filed by the company. [170] The two cases remain ongoing as of the end of the coverage period. [171]

There have been some positive developments in cases regarding online speech in recent years. In March 2022, a criminal court dismissed royal defamation charges against writer Harit Mahaton, who was originally accused of defaming the monarchy in a private Facebook chat in 2016. The claims were dismissed due to insufficient evidence in the complaint filed by a former NCPO legal office chief, whose testimony was deemed hearsay. [172] In June 2020, during the previous coverage period, activist Thanet Anatawong was acquitted of sedition charges; the court concluded that his Facebook posts were constitutionally protected examples of political expression. [173]

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 users of older cards having to reregister. The data must be sent to a central repository at the NBTC. [174] In the southernmost provinces of Thailand, site of a long-running insurgency, this policy is enforced more strictly. Identification measures that came into force in October 2019 in three provinces required individuals to register their SIM cards with facial scans, [175] and a number of phones were disconnected starting in April 2020. [176] Civil society groups and HRDs have warned that the requirements could harm privacy, restrict other freedoms, and lead to profiling of the local ethnic Malay Muslim population. [177]

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. [178] 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.

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. [179]

Government agencies possess a variety of surveillance technologies. In July 2022, after the coverage period, an investigation from Citizen Lab, iLaw, and Digital Reach identified at least 30 Thai HRDs whose devices were infected with Pegasus spyware. The 30 people included prodemocracy protesters and monarchy reform activists, whose devices were targeted between October 2020 and November 2021. [180] The

investigation was prompted after Thai politicians, activists, and academics received emails from Apple in November 2021 notifying them that "state-sponsored attackers" may have targeted their iPhones. [181]

A 2020 report by Citizen Lab identified Thailand as a likely customer of Circles technology, [182] while a 2018 Citizen Lab report identified a Pegasus operator that was likely focusing on targets in Thailand. [183] Thailand has also obtained licenses to import telecommunications interception equipment from Switzerland and the United Kingdom. [184] 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. Government efforts to counter misinformation, including the Anti-Fake News Centres established in 2019 and 2021, collects information from social media, including through the use of artificial intelligence (AI) that is then reviewed by human content monitors (see B5). [185] The extensive monitoring, particularly of social media accounts, raises significant privacy concerns, and there is a lack of clearly drafted procedural guidelines or independent oversight to ensure that collected data are protected. [186] Activists and online journalists were listed on a police watchlist released in July 2022 along with their social media handles. [187] 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. [188]

The 2019 National Intelligence Act authorizes the National Intelligence Agency (NIA) 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 NIA may "use any means, including electronic, telecommunication devices or other technologies," to obtain it. [189]

In response to COVID-19, the MDES introduced MorChana and ThaiChana, mobile applications that track and trace infected persons, as part of the government's

coronavirus containment efforts. [190] The use of these apps, which collect personal information, was mandatory for all individuals arriving in Thailand from abroad. Although the information collected was reportedly only stored until the end of a person's self-quarantine, [191] the uncertainty surrounding the information's use raised serious concerns about privacy rights. [192] On June 1, 2022, MorChana was terminated, as it was no longer considered necessary. [193] The use of ThaiChana is no longer mandatory and is rarely used; however, there is no government order to deactivate it.

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

The Thai government's centralization of internet infrastructure and close relationship with ISPs facilitates government surveillance. [194]

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. [195] 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 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 ($14,820), presenting an additional financial burden for service providers. [196]

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. [197] The order was intended to preserve data for the Anti-Fake News Centre and to combat the sharing of purportedly false content that is punishable under Section 14 of the CCA or any other law (see B5 and C2).

The 2019 PDPA was scheduled to enter into force in May 2020, but certain aspects of the law's implementation were delayed until June 2022, after the coverage period. [198] The law outlines how businesses can collect, use, or disclose personal information. [199] The law can apply to data controllers and data processes outside the country if they process the data of people in Thailand. However, the PDPA provides exemptions for certain activities and authorities. Section 4 exempts any activity of a public authority that has national security responsibilities, ranging from financial security to cybersecurity. It also allows an exception for the House of Representatives, the Senate, or any committee appointed by them. [200] Under Section 26, the legal obligation to various public interest is considered a lawful basis to process sensitive personal data, including biometric data, without the data subject's explicit consent. [201] The PDPA lacks significant safeguards for the automated processing of personal data. Though the National AI Ethics Guidelines, approved by the cabinet in February 2021, require that automated systems processing personal data comply with the PDPA, the limits of the legal regime may be insufficient to protect privacy.

The Personal Data Protection Committee (PDPC), which is responsible for implementing the PDPA, was established in January 2022. [202] The PDPC has 16 members; most are current and former government officials, raising doubts about the PDPC's commitment to protecting user rights.

A warrant is normally required before government authorities can access privately held data. A 2012 cabinet decision, however, allowed investigators to intercept internet communications and collect personal data without a court order in certain cases, including those involving CCA violations. Even where court orders are still required, Thai judges typically approve requests without serious deliberation.

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. [203] 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 affected persons, and no privacy protections govern the handling of collected information. [204]

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, 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 service providers such as AIS, DTAC, TRUE, CAT Telecom, and TOT. [205] The MOD denied the report, although it confirmed that it had met with major mobile service providers about coronavirus tracking. [206] The NBTC and the MDES were reportedly asked to manage the tracking of mobile phone users' movements.

Facebook and Google reported a handful of government requests to access user data. From July to December 2021, Google received four requests for data regarding nine users or accounts but complied with none of them. [207] In the same period, Facebook received 179 requests for data regarding 221 users or accounts and provided data in 55 percent of the cases. [208] Twitter reported 24 information requests regarding 29 accounts; the company complied with none of them. [209]

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?	**2** / 5

Score Change: The score improved from 1 to 2 because there were no reports of internet users facing direct retaliation for their online activities during the coverage period, though online journalists experienced violence in the course of their reporting and targeted online harassment campaigns remain common.

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

Several online journalists were injured while reporting on prodemocracy protests, which police often repressed with violence. [210] In July 2021, for example, Thanapong

Kengpaiboon, a journalist from the online magazine Plus Seven, was injured by a rubber bullet fired by police; Thanapong was covering clashes between protesters and the authorities. [211] As part of the authorities' effort to instill fear among dissidents and intimidate journalists, police questioned journalists who reported on antigovernment protests during the coverage period. For instance, Suramet Noyubon, a journalist with the Facebook outlet Friends Talk, and a pseudonymous reporter with the Facebook news group Live Real were visited in January 2022. [212]

Authorities intimidate users into removing content or self-censoring (see B2 and B4). In November 2021, authorities deported and blacklisted Yan Marchal, a French national and longtime resident of Thailand, likely for parodying the government and monarchy on Facebook and TikTok. [213]

An extreme case was documented during the previous coverage period. In July 2020, Tiwakorn Withiton received social media prominence after wearing a shirt reading, "I lost faith in the monarchy." Police summoned him and demanded he stop wearing the shirt. [214] After refusing, Tiwakorn was forcibly remanded to a psychiatric hospital, his computer and smartphone were seized, and his mother was forced to sign a document without being told of its contents. Tiwakorn was eventually released but was subject to surveillance and was temporarily banned from seeing his family. [215] Tiwakorn was charged with sedition in March 2022 for his involvement in a Change.org petition on abolishing the monarchy (see B8). [216]

Prodemocracy activists who are vocal online, including Sirawit Sertiwat, Ekkachai Hongkangwan, and Pavan Chachavalpongpun, have faced violent attacks inside and outside Thailand during previous coverage periods. [217] The Thai police have not conducted thorough investigations into these incidents and have sometimes halted investigations, [218] blaming the activists for the attacks perpetrated against them. [219]

Individuals who criticized the monarchy received online and offline threats and intimidation (see B2 and C3). 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. [220] Hundreds of critics of Thailand's monarchy were also doxed by royalists in June 2021. Promonarchy users created two Google Maps documents

containing the data of 500 perceived opponents, who they intended to report for engaging in lèse-majesté. [221]

Women HRDs and LGBT+ and gender-nonconforming activists experienced online attacks and harassment. Prodemocracy activist Panusaya Sithijirawattanakul faced gender-based discrimination on social media for strongly criticizing a promilitary politician. LGBT+ activists Sirisak Chaited and Chitsanupong Nithiwana reported experiencing online attacks aimed at their identities and appearances. [222] In previous years, police officers questioned HRD Katima Leeja after she participated in a Facebook video criticizing physical violence amid a land dispute. [223]

There have been several instances of Thai dissidents being abducted while abroad. In June 2020, during the previous coverage period, Wanchalearm Satsaksit, a critic of the government and the monarchy, was forcibly disappeared from outside his home in Cambodia. [224] He faced pending charges under Section 112 and the CCA and disappeared a day after posting a video in which he criticized the Thai prime minister. Wanchalearm's whereabouts remain unknown as of June 2022. [225]

In May 2019, three antimonarchy activists facing 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 they denied. [226] Their whereabouts remain unknown. [227] In December 2018, another three Thai prodemocracy and antimonarchy activists—Surachai Sae Dan, Kraidej Luelert, and Chatchan Buphawan—disappeared while living in Laos. [228] In January 2019, the bodies of Kraidej and Chatchan were found at the Thailand–Laos border. Surachai's whereabouts remain unknown. The Thai government has similarly denied any responsibility. [229]

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

Major organizations, including high-level government bodies, political parties, and defense and energy institutions, frequently face technical attacks, as do private-sector entities and individuals. [230] An NCSC board member has stated that cyberattacks will become widespread and hard to defend against. [231] Indeed, cyberattacks have more than doubled following the COVID-19 outbreak. [232] For instance, Bangkok Airways, the third-largest airline company in Thailand, faced a ransomware attack that month, suffering the theft of 200 GB of data. [233] Several high-profile cyberattacks were likewise reported in September 2021. About 16 million patient records from the Ministry of Public Health were allegedly hacked and put up for sale, [234] though authorities indicated that the data of only 10,000 patients was leaked. [235] In January 2022, a large data leak concerning Siriraj Hospital's records of 39 million patients was reported. [236]

The Cybersecurity Act came into force in May 2019. [237] The law aims to protect against, address, and mitigate cybersecurity threats. [238] However, the text fails to protect online freedom and privacy. For example, telecommunications and technology firms designated as operating critical information infrastructure must monitor and report all threats to the government as they develop, which could include sharing confidential information.

• • •

Footnotes

1 Digital 2022: Thailand, We are social and Kepios, https://datareportal.com/reports/digital-2022-thailand

2 Digital 2022: Thailand, We are social and Kepios, https://datareportal.com/reports/digital-2022-thailand

3 Ibid.

4 "Thailand," Ookla Speedtest Global Index, accessed September 11, 2022, https://www.speedtest.net/global-index/thailand.

5 "5G is about to be real," Bangkok Post, February 24, 2020, https://www.bangkokpost.com/tech/1864284/5g-is-about-to-be-real

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 2022

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