

## Just Released: Freedom in the World 2026

ENGLISH 繁體中文



## FREEDOM ON THE NET 2024

## Taiwan

FREE

79  
/100

A. <u>Obstacles to Access</u>	24/25
B. <u>Limits on Content</u>	29/35
C. <u>Violations of User Rights</u>	26/40

## LAST YEAR'S SCORE &amp; STATUS

78 /100 Free

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

# Key Developments, June 1, 2023– May 31, 2024

Taiwan hosts one of the freest online environments in Asia, though concerns about overbroad and nontransparent website blocking have emerged in recent years. The information landscape is characterized by affordable internet access, diverse content, and a lack of internet shutdowns. Civil society, the technology sector, and the government have taken innovative action to counteract the impact of disinformation campaigns originating from China. However, concerns over disproportionate surveillance and a lack of transparency around website blocks threaten internet freedom.

- The telecommunication industry underwent drastic mergers that enabled three major providers to dominate the market, though the impact on Taiwanese internet subscribers is not yet clear (see A4).
- Government agencies relied on a nontransparent website blocking mechanism known as the DNS Response Policy Zone (DNS RPZ); WordPress-hosted sites were briefly blocked during the coverage period, likely because of the DNS RPZ, alongside a localized restriction on Telegram (see B1 and B3).
- The number of content removal requests from the government to Google and Meta surged tremendously, according to the companies' transparency reports (see B2).
- Ahead of Taiwan's January 2024 election, influence operations sought to distort views on politics and hackers launched cyberattacks, some of which were linked to Chinese state-affiliated actors (see B5 and C8).
- The government considered an amendment to the Communication Security and Surveillance Act that would expand authorities' access to network traffic records and expanded the range of crimes for which prosecutors could authorize surveillance without prior approval from a court; it passed after the coverage period (see C5).

# Political Overview

Taiwan's vibrant and competitive democratic system has allowed three peaceful transfers of power between rival parties since 2000, and protections for civil liberties are generally robust. Ongoing concerns include the Chinese government's efforts to influence policymaking, the media, and democratic infrastructure in Taiwan. In the January 2024 election, voters selected Vice President Lai Ching-te of the Democratic Progressive Party (DPP) to assume the presidency, while the opposition Kuomintang (KMT) secured a plurality of seats in the Legislative Yuan.

## A. Obstacles to Access

**A1** 0-6 pts

**Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?**

**6/6**

In general, there are no infrastructural limitations to internet access in Taiwan and the country boasts high rates of internet access. DataReportal's *Digital 2024* report placed Taiwan's internet penetration rate at 90.7 percent and counted 21.71 million internet users. <sup>1</sup> The Taiwan Network Information Center (TWNIC) reported a penetration rate of 84.67 percent for people over the age of 18 in 2023. <sup>2</sup>

Users can get online via a variety of connection standards: Fixed-line broadband options include fiber-optic and digital subscriber line (DSL) connections, while mobile users rely on 4G and 5G technology. Free public Wi-Fi services are also available, with nearly 10,000 free hotspots across the country. <sup>3</sup> According to the National Communications Commission (NCC), 6.76 million people, including more than 4.25 million fiber-optic users, were subscribed to fixed-line broadband networks in December 2023, and there were more than 30 million subscribers to mobile networks. <sup>4</sup> According to the TWNIC's report, the penetration rate for fixed-line broadband users was 65.41 percent and the penetration rate for mobile broadband users was 81.76 percent. <sup>5</sup>

In February 2023, the two submarine cables connecting Taiwan and the Matsu Islands, a Taiwan-governed archipelago off the coast of the mainland, were severed by Chinese civilian vessels. **6** The approximately 14,000 residents of the Matsu Islands lost high-speed internet until late March, when one of the cables was repaired, though Chunghwa Telecom—Taiwan’s largest telecommunications company—deployed low-bandwidth internet services in the interim. **7** Though an NCC investigation reportedly found no direct evidence that the incidents were deliberate, the cable cuts were widely understood as a national security risk. **8** More minor cable cuts are common. According to one tally, illegal sand-pumping vessels have cut the Taiwan-Matsu cables almost 30 times over the past six years. **9**

Several efforts to strengthen the resilience of Taiwanese internet infrastructure are underway. In November 2023, Chunghwa Telecom commissioned a new submarine cable for outlying islands. **10** The construction of a satellite internet network operated by the Taiwanese government and private sector remained under development during the coverage period. **11**

The government is dedicated to upgrading mobile services to 5G. **12** Telecommunications companies stopped offering 3G contracts in 2018. **13** Major service providers, such as Chunghwa Telecom, Taiwan Mobile, and FET, began providing 5G service in major cities and several other areas in 2020. **14** The number of 5G service users reached about 8.39 million in December 2023, according to the NCC, and 5G service users accounted for 26.77 percent of all users of mobile internet, according to the TWNIC. **15**

Taiwanese internet users enjoy fast internet speeds. In May 2024, Ookla’s Speedtest Global Index reported Taiwan’s median mobile download and upload speeds as 81.93 megabits per second (Mbps) and 14.91 Mbps, respectively. Fixed-line broadband download and upload speeds were reported at a median 190.01 Mbps and 94.20 Mbps. **16**

## **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**

**3/3**

reasons?	
----------	--

There are no significant digital divides in Taiwan, although slight disparities remain based on geographical area and age. Internet access, especially on mobile networks, is affordable. According to a 2020 TWNIC report, 95 to 97 percent of users spend less than 1 percent of their monthly income on mobile network access. **17** The Economist Intelligence Unit's Inclusive Internet Index 2022 noted improvements in the cost of internet access relative to income; for example, the price of a 1 gigabyte (GB) postpaid mobile phone accounted for 0.26 percent of monthly income on average in 2022, compared to 0.72 percent of monthly income in 2021. **18**

There is no significant gender-based digital divide, though digital divides based on geography, age, and education level persist. A 2023 TWNIC report found lower rates of internet penetration for people over the age of 70, people living in the east coast of Taiwan, and people with primary school education or below. **19** The age-based disparity in access is gradually improving. In 2020, the National Development Council (NDC) reported that 86.6 percent of people above the age of 12 accessed the internet, compared to 77.6 percent of people between the ages of 60 to 64 and 46.8 percent of people over the age of 65. **20**

Some other marginalized groups have experienced a boost in internet access in recent years. For example, as of 2020, 96 percent of immigrants used the internet, a sharp increase from 72 percent in 2014. **21** The government established the i-Tribe program to increase wireless broadband access for Indigenous communities. **22** The program has reportedly improved people's ability to access digital healthcare services and other information. **23** However, migrant fishers working on deep-water vessels still face limited internet access. **24** Advocates launched multiple campaigns during the coverage period to ensure migrant fishers' access to the internet while at sea. **25**

**A3** 0-6 pts

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

The government does not intentionally restrict connectivity, and the country's internet infrastructure is privately owned. However, the infrastructure is vulnerable to damage or interference (see A1).

The four major internet exchange points (IXPs)—TWIX, TPIX, EBIX, and TWNAP—are all operated by telecommunications companies, although TWNAP functions largely as a data center and not an exchange point. **26** A community-based IX, STUIX (Student & Technology United Internet Exchanges), was established in 2021 with the mission to provide a more affordable networking service. **27**

The submarine cables connecting international networks are privately owned. **28** Chunghwa Telecom, 35 percent of which is held by the Ministry of Transportation and Communications (MOTC), lays the majority of submarine cables. **29** Three new submarine cables are expected to be ready for service by 2026, including the TPU cable project exclusively owned by Google, and the Southeast Asia-Japan Cable (SJC2) project that was reportedly halted for over a year partly due to Beijing's objection. **30**

**A4** 0-6 pts

**Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?**

**5/6**

While people have a choice of service providers, certain companies dominate the market. The Telecommunications Management Act (TMA), **31** which was approved in June 2019 and came into effect in July 2020, replaced the Telecommunications Act (TA) and relaxed some of its rules. Under the TMA, service providers and intermediary telecommunications operators must register with the NCC. **32**

According to the TMA, direct foreign ownership of telecommunications services is limited to no more than 49 percent, and only 60 percent of shares may be owned indirectly or directly by foreigners. **33**

The TMA places some obligations on service providers that are not particularly onerous and are often meant to protect users. For example, telecommunications

operators are obligated to take appropriate and necessary measures to protect the confidentiality of communications, provide public and easily accessible information to consumers, separate telecommunications and service fees from unrelated ones, and provide channels for consumers to lodge complaints. **34**

During the coverage period, the telecom industry saw significant mergers that enabled three major providers to dominate the market: Chunghwa Telecom, New Taiwan Mobile (the result of a merger of Taiwan Mobile and Taiwan Star in December 2023), and Far EasTone (which merged with Asia Pacific Telecom, also in December).

**35** The NCC approved these mergers with conditions—including disposing of extra bandwidth acquired in the mergers, raising the coverage rates for 4G and 5G service, and addressing the digital divide—to maintain market competition and further strengthen internet connectivity. **36** The impact of the mergers on Taiwanese subscribers is not yet clear. Prior to the mergers in 2023, market-entry requirements and the high cost of developing infrastructure, among other factors, had already allowed only a small number of providers to dominate the fixed-line and mobile markets. **37**

As of December 2023, Chunghwa Telecom reported 13.14 million mobile subscribers and 4.4 million fixed-line broadband subscribers. **38** New Taiwan Mobile reported 10.28 million subscribers following the December 2023 merger. **39** In October 2023, Far EasTone said it expected to have 9.2 million subscribers following its merger. **40** Eighty-two companies offered fixed-line networking as of February 2020, most of them small businesses that only provide local services. **41**

**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?**

**4/4**

Regulatory bodies that oversee telecommunications and other internet-related issues in Taiwan are generally seen as free, fair, and independent.

Established in 2006, the NCC is an independent government body responsible for regulating telecommunications and broadcasting services, including overseeing the

telecommunications industry, managing domain names and internet protocol (IP) addresses, and processing and overseeing licenses; **42** it has additionally governed the TWNIC since 2017. The NCC's mission includes promoting sound policy, safeguarding users' rights, protecting consumer interests, and ensuring fair and effective competition in the market. **43** The body is composed of seven commissioners who serve four-year terms, all of whom are nominated by the prime minister and approved by the Legislative Yuan. The prime minister is tasked with appointing both the chairperson and vice chairperson, rather than elected by its commissioners, prompting questions about the body's independence. **44** According to a report released by the Taiwan Public Opinion Foundation in November 2020, 68 percent of respondents reported being concerned about the NCC's independence.

#### **45**

Recordings leaked in October 2022 raised concerns about political interference in the NCC's January 2022 licensing approval of Mirror TV, the first news TV channel license issued by the NCC over the past 10 years. The recording purportedly features a former Mirror TV executive stating that the premier and president at the time—Su Tseng-chang and Tsai Ing-wen, respectively, both of the Democratic Progressive Party (DPP)—had pressured the NCC to expedite the license. **46** A special task force was established by opposition lawmakers in July 2024 to investigate this matter. **47**

In August 2022, the government inaugurated the new Ministry of Digital Affairs (MODA), led by Audrey Tang, a former minister without portfolio, to develop and promote digital policy innovation and reform in the areas of telecommunication, information, cyber security, internet, and communications. **48** Several other government bodies oversee digital technology. For example, the Fair Trade Commission (FTC) oversees competition law as it relates to telecommunications or digital services. FTC and NCC decisions can be appealed to the judiciary. **49** In recent years, several different government bodies have supervised the implementation of Taiwan's Personal Data Protection Act (PDPA) (see C6). The Department of Cyber Security (DCS) oversees issues related to the security of critical infrastructure (see C8).

The nature of online information dictates which agency is tasked with the regulation of particular content (see B2 and B3). **50** For example, online content related to food hygiene is handled by the Ministry of Health and Welfare. The Institute of Watch Internet Network (iWIN), a semiofficial organization funded by several government departments, is responsible for content related to children and youth (see B2). **51**

## B. Limits on Content

**B1** 0-6 pts

<p><b>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?</b></p>	<p><b>5/6</b></p>
--	-------------------

The government does not generally compel service providers to block or filter websites or social media platforms. However, certain laws authorize the restriction of content online, and the DNS Response Policy Zone (DNS RPZ) antifraud website-blocking system has led to occasional collateral effects (see B3).

Websites are sometimes mistakenly blocked under the DNS RPZ's antifraud measures (see B3). In April 2024, WordPress-hosted websites were reportedly blocked for seven hours, with users being redirected to the antifraud page provided by the Criminal Investigation Bureau (CIB) of Taiwan's National Police Agency (NPA). **52** Similarly, in August 2022, during the previous coverage period, internet users on Taiwan Mobile networks reported that the Google Maps website was blocked and redirected to the CIB's antifraud page. **53** During Meta's global outages in March 2024, some Taiwanese users reported being unable to access Instagram, with some being redirected to the CIB antifraud page; the CIB denied ordering any blockage of Instagram. **54**

In May 2024, National Tsing Hua University (NTHU) briefly blocked Telegram, redirecting visitors to a page displaying the seal of the Ministry of Justice Investigation Bureau (MJIB). Bloggers obtained documents that attributed the block to an order from the Hsinchu City government, where NTHU was located; the

government had reportedly instructed a range of agencies and institutions to block Telegram, the bulletin board service SOGO, and a porn website. **55** The Hsinchu City blocking order was issued amid a national discussion about blocking Telegram; the same month, Taiwan’s minister of health and welfare threatened to block the platform altogether if it did not comply with the ministry’s request to remove an allegedly illegal pornographic online forum within 24 hours. The statement prompted widespread backlash about censorship, **56** and the ministry later backed down, saying that blocking the site would be technically difficult. **57**

The government has sought to impose limits on access to platforms owned by platforms based in the People’s Republic of China in recent years. **58** In August 2020, the Ministry of Economic Affairs announced that beginning the following month, Taiwanese companies could not provide video-streaming-related services originating with Chinese companies or people, particularly Tencent or the Baidu-owned platform iQIYI. The rule updated Taiwan’s Act Governing Relations between the People of the Taiwan Area and the Mainland Area and formally prohibited companies and individuals in Taiwan from serving as agents of any Chinese over-the-top (OTT) media services or distributing them via television or other broadcast methods, including with Chunghwa Telecom’s digital television channel Media on Demand (MOD). **59** Since 2019, the government has prohibited users of government-owned electronic devices from installing or using TikTok for cybersecurity reasons. **60**

The Ministry of Education’s Network Guardian Angels (NGA) is a content-filtering software program available to the public, geared toward parents and educational institutions. According to a national report, NGA was downloaded nearly 99,000 times between January and November 2020. **61** The Taiwan Association for Human Rights (TAHR) found that NGA-filtered content is based on unclear standards and has targeted civil society websites, including the Taiwan Alliance to End the Death Penalty and the Taiwan Tongzhi Hotline Association, a group serving the LGBT+ community. **62**

**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,**

**3/4**

**particularly material that is protected by international human rights standards?**

Expression protected by international human rights standards is generally not forcibly removed, and intermediaries do not face onerous liability for content generated by third parties. However, a range of laws prohibits the publishing of certain kinds of content and has permitted content removal (see B3). **63** The TAHR reported, for example, that the government cited the Commodity Inspection Act and the Consumer Protection Act a combined total of 714 times in requests to remove content between 2017 and 2018. **64** The Copyright Act also lays out a notice-and-takedown procedure that obligates intermediaries to remove third-party content that infringes on copyright. **65**

The judiciary has addressed cases that include requests to remove content in recent years, though not during the coverage period. In January 2022, a court ordered a city councilor to remove a YouTube video that spread false information about another legislator. **66** In September 2021, a court ordered Liang Mu-yang, a newspaper journalist and former legislator, to remove Facebook posts and 49 YouTube videos about a county magistrate with whom Liang was in dispute, after the magistrate filed a civil claim over Liang's posting of purportedly false and biased information. **67**

iWIN was established under Article 46 of the Protection of Children and Youths Welfare and Rights Act (PCYWRA). The act requires that content hosts limit the receiving and browsing of content deemed harmful to the physical and mental health of children and youth, such as content featuring violence, blood, sex, obscenity, and gambling. **68** Among other measures, iWIN identifies this content through a complaint mechanism for users, content-screening software, the promotion and review of a content rating system, and the operation of a self-discipline mechanism by internet service providers (ISPs). **69**

iWIN reported receiving 3,007 complaints in 2023, including 1,221 cases related to pornography and 97 cases related to false information. iWIN reported 1,245 of the complaints to companies and deny-listed 440 pieces of content through filtering

software. **70** It is unclear what percentage of the complaints and reports to companies led to actual content removal on the platform's end.

In early 2024, iWIN ordered the removal of several webpages allegedly containing illustrations that the organization characterized as child sexual abuse images. iWIN claimed that the fictional characters in these images appeared to be children, thus violating the PCYWRA. The order triggered public concern over censorship and infringement on freedom of expression. Critics questioned the legitimacy of iWIN's decision, highlighting the absence of real-life victims in the case. **71** To settle the public outcry, iWIN and the Ministry of Health and Welfare met with children protection civil society organizations (CSOs), anime creators, and representatives of publishing industry in March, discussing the proportionality of content regulation within the ACGN (anime, comics, games, novels) subculture. Consensus was reached, according to a government official, that only three types of fictional content will be subject to regulation under the PCYWRA: sexual imagery of children, pornographic drawings depicting real-life subjects, and realistic pornographic drawings generated by artificial intelligence. **72**

Taiwanese government requests to platforms to remove online content have surged, primarily under antifraud laws. Requests to Google increased from 17 requests in the first half of 2022 to 10,104 requests in the corresponding period of 2023, most of them citing antifraud provisions under Taiwan's criminal code. Google removed nearly 350 items in the first half of 2023 in response to these requests. **73** Meta disclosed that it had restricted an estimated 24,700 pieces of content in Taiwan in the first half of 2023, compared to 1,420 pieces in the first half of previous year. The content, all allegedly in violation of local laws related to regulated goods, scams and fraud, was reportedly blocked in response to requests by various government agencies. **74**

**B3** 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	3/4
---	-----

Technical censorship is not routine in Taiwan. However, civil society has raised concerns over a lack of oversight over law enforcement agencies' removal orders, and a lack of transparency regarding how frequently such requests are complied with by tech companies (see B2). **75**

Taiwanese authorities use a system known as the DNS RPZ to order ISPs to block websites. Under the DNS RPZ system, TWNIC coordinates with service providers to stop resolving DNS requests to domains upon receipt of a court order or legally authorized administrative order (referred to as RPZ 1.0) or an emergency request from a law enforcement agency (known as RPZ 1.5). **76** The RPZ 1.5 system is controversial, and is often perceived as circumvention of legal due process and lacking in provision for remedy avenues. **77** According to TWNIC's transparency report, from June 2023 to May 2024, there were 29 domain names blocked based on RPZ 1.0 court orders, in contrast to 36,559 blocked via RPZ 1.5 emergency requests. **78**

In a February 2024 press release, the government stated that that the mandate of the DNS RPZ covered "financial crimes, fake government websites, fraudulent websites, and fake websites during elections." **79** According to law enforcement agencies, the legal basis of DNS RPZ is Article 38 of the Criminal Law and Article 133(1) of the Criminal Procedure Law. **80**

Technologists and civil society have criticized the DNS RPZ for its limited transparency and the lack of judicial oversight over RPZ 1.5 website blocks. **81** During the coverage period, TWNIC transparency reports only disclosed domain names blocked under RPZ 1.0; the TWNIC disclosed the total number of domains blocked under RPZ 1.5 and a list of domains requested by certain agencies. **82** The TWNIC has also removed information from its transparency disclosures, including meeting minutes, the list of providers and agencies that participate in the DNS RPZ, and information about the mechanism for filing complaints. **83**

In July 2024, after the coverage period, the Legislative Yuan passed the Fraudulent Crime Prevention Bill, a national antifraud package that includes a provision authorizing government agencies to file emergency requests to restrict access to

websites for fraud prevention. **84** CSOs, including TAHR and the Judicial Reform Foundation, criticized the legislation for creating a legal justification for website blocking in the name of antifraud measures while lacking independent oversight, transparency, and due process within the framework. **85**

Beyond antifraud measures, a range of laws prohibit publishing certain kinds of content, including the PCYWRA, the Act Governing Food Safety and Sanitation, the Pharmaceutical Affairs Act, the Consumer Protection Act, and the Cosmetic Hygiene and Safety Act. **86** The Statute for Prevention and Control of Infectious Animal Diseases, for example, allows the government to compel providers to block access to websites or remove webpages that sell animal products that are banned or subjected to quarantine. **87** No regulation mandates that the government disclose such content-restriction requests.

Taiwanese authorities have passed more proportionate measures relating to online content in recent years. The government amended the Public Officials Election and Recall Act in June 2023 to permit candidates in public elections to report to the police any nonconsensual and misleading content of themselves generating using artificial intelligence (AI) tools. If police technical experts confirm the content to be AI-generated, the candidate may request that internet platforms remove the content; platforms must act accordingly within two days. **88** In August 2023, amendments to the Sexual Assault Crime Prevention Act entered into effect requiring that service providers remove content relating to the nonconsensual production, leaking, distribution, or manipulation of sexual images and videos when notified by law enforcement. **89** Amendments to the Child and Youth Sexual Exploitation Prevention Act passed in February 2023 require platforms to create technical systems to remove or restrict the access to illegal content immediately once the content is detected. **90**

The judiciary has issued rulings around online censorship. In May 2022, the High Court ruled that Google should delist information that contains personal attacks or vulgar language but leave up contents related to public interest. The court cited the right to information privacy protected by Constitutional Interpretation No. 603 to make the verdict, rather than the right to be forgotten. **91**

In June 2022, the NCC published the draft Digital Intermediary Services Act (DISA), **92** only to retract it within several months in the face of widespread criticism. **93** The DISA would have imposed varying degrees of obligations on digital communications platforms, including mandates that online platforms release transparency reports and online advertising disclosures and provide strong notice-and-appeal mechanisms relating to content removal. It would also have required service providers to label content mandated by administrative agencies and to comply with court orders to remove and restrict the spread of content. **94** Free expression advocates raised concerns about the law’s potential for censorship and called for revisions, while others in civil society supported the effort toward platform regulation. **95** The government did not reintroduce DISA during the coverage period.

**B4** 0-4 pts

**Do online journalists, commentators, and ordinary users practice self-censorship?**

**3/4**

Journalists, civil society groups, activists, and ordinary users generally do not self-censor online. However, some laws that include liability for online content—such as the Social Order Maintenance Act (SOMA) and criminal defamation provisions—may influence self-censorship (see C2 and C3).

Concerns about Chinese technology may also drive self-censorship. In January 2022, the NCC reported that some mobile phones produced by Chinese manufacturer Xiaomi monitor content for certain keywords and could potentially block or filter that content or transmit users’ online activity “to servers in Beijing.” **96**

Self-censorship is also driven by fear of online harassment for commentary, real or perceived, on politics in China and Hong Kong. In July 2023, IKEA Taiwan removed a Facebook post with the caption and image of “eight people arrested” (逮八人), a punning meme on a homophone for “Taipei people” (台北人) in the Hokkien dialect, after a Facebook page that supports the Hong Kong national security police criticized the post. **97** Hong Kong’s National Security Law, along with the Hong Kong Basic Law Article 23 that went effect in March 2024 and a June 2024 Chinese law that

threatens the death penalty for supporters of Taiwanese independence, **98** may also encourage self-censorship of China-related speech because the scope of the penalties extends to speech made outside China. **99**

High-profile prosecutions have left some Taiwanese people who need to travel to China wary of discussing China-related issues online. For example, Taiwanese activist Lee Ming-che was arrested by the Chinese government in 2017 while transiting through the Chinese special administrative region of Macau and later sentenced to five years in prison for “subverting state power”; social media content he posted while in Taiwan was used as evidence in court. **100** Lee was released and returned to Taiwan in April 2022. **101**

**B5** 0-4 pts

<p><b>Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?</b></p>	<p><b>2/4</b></p>
--	-------------------

The government does not issue formal directives or attempt to coerce online outlets to influence their reporting. However, political disinformation and online influence operations are a significant issue, particularly those which support the Chinese government’s positions or emanate directly from Chinese party-state actors. **102**

Perennial topics have included Beijing’s propaganda pushing for “reunification” of the Chinese mainland and Taiwan, flaws in Taiwanese democracy, information discrediting the government’s response to the COVID-19 pandemic, and content aimed at smearing proindependence candidates, particularly during elections. **103** A March 2023 report by Doublethink Lab ranked Taiwan as the most influenced by China in the media domain, among the 82 countries studied. **104** In the 2022 Beijing’s Global Media Influence report, which is produced by Freedom House, Taiwan was identified as experiencing the highest level of Chinese influence efforts (as well as the highest level of local resilience.) **105** In response, the civil society has taken innovative action to counteract false and manipulated information in the country (see B7). **106**

Taiwanese CSOs reported on a range of online influence operations that sought to shape views of the 2024 election, many of them linked to China-based actors. According to Doublethink Lab, prominent narratives during the electoral period sought to invent scandals involving prominent DPP officials, including then president Tsai and then vice president Lai, and amplified distrust in the Taiwanese government's capacity to provide public services. **107** For example, an e-book that smeared Tsai circulated widely online; the e-book then featured heavily in videos on social media platforms in which AI-generated avatars read from the text. Doublethink Lab, which identified the campaign, attributed it as likely linked to the Chinese Communist Party (CCP). **108** The Taiwan Information Environment Research Center (IORG) identified a strong prevalence of narratives that painted US-Taiwan relations in a negative light. **109** The IORG also found that false claims casting doubt on the impartiality of election administrators and the integrity of the balloting spread widely ahead of and after election day. **110** Similarly, Doublethink Lab identified a group of fashion and beauty influencers who posted videos with similar scripts about vote rigging. **111**

Previously, Doublethink Lab released two studies examining the impact of pro-China content manipulation on the 2022 local election. These studies pointed out that the Chinese government primarily deployed local Taiwanese online influencers and nationalist Chinese netizens to spread pro-Beijing messages to influence the election and that such content manipulation may have impacted the election results. The studies also found that many people feel they did not have access to accurate information from the Taiwanese government. **112** In January 2022, the MJIB reported on the existence of inauthentic accounts on Facebook and Taiwanese platforms PTT and CK101 that distributed false information and content originating from Chinese content farms. **113**

Other researchers have also observed changes in the ways China's disinformation and propaganda are targeting Taiwan. For example, after US House Speaker Nancy Pelosi's visit to Taiwan, videos implying a threat of war were uploaded on YouTube and to Reddit in the Southern Min dialect, which is spoken by many Taiwanese people.

Taiwan’s leading political parties—the DPP, the Kuomintang (KMT), and the Taiwan People’s Party (TPP)—have each claimed that their opponents have hired or deployed commentators to spread manipulated information online. **114** In June 2022, Ko Wen-je, then Taipei’s mayor and the TPP’s chairperson, was criticized for allegedly coordinating an army of online commentators after civil servants were discovered posting anti-DPP content from government IP addresses during working hours. **115** Ko denied the allegation. **116** In December 2022, following the local elections, a report alleged that it uncovered a list of pro-DPP online commentator groups; the DPP responded that the groups were simply for regular political discussion. **117**

In face of widespread electoral misinformation campaigns, the Legislative Yuan passed the 2023 amendment to the Public Officials Election and Recall Act, aiming to prevent foreign interference. The amendments oblige all political advertising (both online and offline) to disclose who was paying for its placement, among other relevant information, as part of an effort to enhance transparency. **118** Platforms are required to verify the source of funds sponsoring political advertising, as they are prohibited from accepting funds associated with individuals and organizations in foreign countries, with China, Hong Kong and Macau particularly singled out.

**B6** 0-3 pts

<p><b>Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?</b></p>	<p><b>3/3</b></p>
---	-------------------

Taiwanese users do not face onerous constraints on their ability to publish content online. Online or digital news outlets are not required to obtain a license in order to publish. Service providers are regulated by the TMA and must provide services in a nondiscriminatory manner in terms of connection quality, price, condition, and information (see A4). **119**

Some regulations restrict online advertisement or investment originating from China. The Act Governing Relations between the People of the Taiwan Area and the Mainland Area requires government approval for mainland Chinese entities to directly own media properties and entities. It also bans CCP advertisements. **120**

To bolster the sustainability of news media, there have been discussions around implementing a tax on social media platforms to support local journalism, modeled on Australia’s News Media Bargaining Code. In December 2022, the Ministry of Digital Affairs (MODA) hosted meetings with Google, Meta, and news media organizations.

**121** In March 2024, Congress proposed the Digital News Development and Democracy Resilience Act draft which includes an objective to improve working conditions for frontline journalists and newsroom workers. The draft has received preliminary tripartisan support. **122**

**B7** 0-4 pts

**Does the online information landscape lack diversity and reliability?**

**4** / 4

Taiwan’s online information and digital media ecosystem reflects varied interests, experiences, communities, and languages. A range of newer online outlets contributes to this diversity. According to a 2022 survey conducted for the Reuters Institute for the Study of Journalism at the University of Oxford, 84 percent of Taiwan’s population consumed news online and 58 percent obtained it via social media; only 16 percent read print news, down from 41 percent in 2017. **123**

However, the media environment suffers from political polarization and sensationalist content. **124** Only 27 percent of the people surveyed for the Reuters Institute’s 2022 report considered the news reliable, the lowest among people surveyed in Asia-Pacific countries. **125** A study from the Taiwan Media Watch Foundation also found that people in Taiwan viewed the media environment as less credible and less reliable in 2018 than they did in 2014. **126**

Misinformation online and across Facebook, X, Instagram, the Japanese-owned Line social media and messaging service, and the popular Taiwan-based PTT online bulletin board can undermine people’s ability to access reliable information (see B5).

**127** For instance, misinformation circulated widely during the period of the 2022 “nine-in-one” elections. False claims included those that the eligibility age for presidential candidates would be lowered to 18 years old if a constitutional

amendment to lower the voting age to 18 was passed, and that voting would be prohibited for people wearing gloves. **128**

The government, technology industry, and civil society have designed innovative tools to counteract the impact of false and misleading information in Taiwan (see B5). **129** For example, Line users can submit information for fact-checking to Cofacts, a platform created by the decentralized “gov-zero (gov)” community, **130** and can receive information about its validity. Organizations like Doublethink Lab have also conducted innovative research to uncover and analyze disinformation campaigns and their impact. For example, Doublethink’s project “Escape the Mist: Disinfo Walkthrough” aims to support civil society efforts to counter mis- and disinformation. **131**

**B8** 0-6 pts

**Do conditions impede users’ ability to mobilize, form communities, and campaign, particularly on political and social issues?**

**6/6**

People in Taiwan can freely use digital platforms and online sources to debate and mobilize around social and political issues, including on social media platforms like Line and Facebook, as well as the online bulletin board PTT.

Current events tend to prompt considerable debate and mobilization on social media. In May 2024, the opposition KMT-TPP coalition, which together hold a majority in the Legislative Yuan, sought to rush through a bill that would boost the legislature’s power to punish citizens who refuse to turn over private information, ostensibly to strengthen government oversight. The proposal sparked widespread protests, organized in part through social media platforms, over concerns of overreach and a lack of parliamentary deliberation. **132** Young people who joined the protests, commonly referred to as the Bluebird Movement, used the Meta-owned platforms Threads and Instagram to spread information and mobilize. **133**

Candidates used social media to mobilize their supporters during the 2024 election. For example, Threads was popular among DPP supporters. **134** Social media

mobilization was also prominent during the 2022 “nine-in-one” elections and the 2023 Nantou legislative by-election. **135**

In June 2023, people in Taiwan launched a series of #MeToo campaigns on Facebook and other social media to call attention to sexual harassment. **136** The campaigns evolved into a national movement, with more than 150 public figures accused of sexual harassment and sexual assault incidents by the end of the month. **137** Some people faced legal threats relating to their allegations of abuse. **138**

The Platform for Online Participation in Public Policy, maintained by the NDC, offers an official way for the general public to propose, engage, monitor, and reply to public policies online. **139** The NDC reported in 2021 that users expressed a high degree of satisfaction with the platform, though only 0.43% of proposals were ultimately adopted. **140**

## C. Violations of User Rights

**C1** 0-6 pts

<p><b>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?</b></p>	<p><b>5/6</b></p>
--	-------------------

Freedom of speech and freedom of the press are constitutionally protected. **141** The government has also incorporated free expression and access to information protections under the International Covenant on Civil and Political Rights (ICCPR) into domestic law. **142** The Freedom of Government Information Law was enacted in 2005. **143**

Taiwan’s judiciary is relatively independent and protected by the Judges Act. **144** The judicial system provides considerable protection for speech (see C3). However, at least one court ruling has undermined strong free expression standards. In 2000, the Constitutional Court stated that the crime of defamation does not violate the constitution’s free speech protections (see C2). **145**

In February 2023, during the previous coverage period, the Ministry of National Defense (MND) proposed revising the All-Out Defense Mobilization Readiness Act, which addresses wartime mobilization. After a wave of criticism, the ministry withdrew the draft amendments in early March. **146** Provisions of the proposed amendments that obligated the publishing industry, media, broadcast TV, and internet platforms to cooperate with the government during mobilization raised free expression concerns; the bill’s supporters argued that the provisions sought to counter information operations during wartime. **147**

## C2 0-4 pts

<p><b>Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?</b></p>	<p><b>2/4</b></p>
---	-------------------

A range of laws criminalize online activities. Defamation and slander are criminal offenses. Article 309 of the criminal code imposes up to two months’ detention or a fine of NT\$9,000 (US\$324) for publicly insulting another person. Article 140 outlines liability of up to one year in prison or a fine of up to NT\$100,000 (US\$3,600) if an individual “offers an insult to a public official during the legal discharge of his duties.” In December 2021, the Legislative Yuan amended Article 140 to remove a clause criminalizing “insult to a public office” and to raise the punishment for the remaining provision. **148** Some legislators have argued that Article 140 violates free expression protections and called for amending the criminal code. **149**

Article 310 of the criminal code imposes sentences of up to two years in prison or a fine if an individual is found guilty of “point[ing] out or disseminat[ing] a fact which will injure the reputation of another for purpose that it be communicated to the public” in writing. **150** People who allege they are slandered can also request financial compensation. For defamation cases, the law excludes speech that can be proven to be true, is related to public concern, and is a “fair comment on a fact subject to public criticism.” Prominent politicians and prosecutors have criticized the criminal insult and defamation provisions as conflicting with the constitution. **151** In June 2023, the Constitutional Court upheld the constitutionality of Article 310, ruling that

the standard was proportionate and did not violate freedom of expression rights. **152** The court specified that freedom of expression did not extend to false information transmitted without efforts to verify the information. **153**

Several laws impose liability for disseminating false or misleading information. Under the SOMA, users can be penalized for “spreading rumors in a way that is sufficient to undermine public order and peace” with up to three days of detention or a fine of no more than NT\$30,000 (US\$1,080). **154** The law has been used to investigate online activities (see C3).

In September 2021, the Constitutional Court stated that Article 38 of the SOMA was unconstitutional. That article allowed law enforcement units to simultaneously seek administrative fines and criminal penalties for a single case. After the ruling, law enforcement departments may only charge a person accused of crimes with an administrative fine or a criminal penalty, including in cases that relate to online expression. **155**

Article 14 of the Special Act for Prevention, Relief, and Revitalization Measures for Severe Pneumonia with Novel Pathogens, which came into force in January 2020 to combat the COVID-19 pandemic and expired in June 2023 (see C6), imposes up to three years of imprisonment and high fines for the dissemination of rumors or false information regarding epidemics deemed to cause damage to the public and others. **156** Similarly, Article 63 of the Communicable Disease Control Act, promulgated in June 2019, calls for fines of no more than NT\$3 million (US\$108,000) for spreading rumors or false information about an epidemic that causes substantial harm to the public or others. **157**

Spreading false information during election periods can also lead to criminal penalties. Article 104 of the Civil Servants Election and Recall Act imposes a maximum penalty of five years in prison for damaging the public by disseminating rumors or fraudulent content in order to elect or not elect a candidate, or for a political proposal. **158** In December 2019, the legislature passed the Anti-Infiltration Act, which includes criminal penalties for spreading election-related disinformation that is instructed, funded, or sponsored by hostile foreign forces. **159** After the

passage of the act, pro-Beijing online media outlet Master Chain announced that it was ending operations in Taiwan. **160**

Under the Disaster Prevention and Rescue Law, anyone who knowingly reports false information about a disaster faces fines of between NT\$300,000 to NT\$500,000 (between US\$10,800 to US\$18,000). **161** The Food Administration Act states that no one shall “deliberately disseminate rumors or false information” relating to market food prices and the implementation of food productive programs, among other issues. **162**

The draft amendment to the All-Out Defense Mobilization Readiness Act introduced in February 2023 and withdrawn the following month (see C1) included a provision that imposed a maximum penalty of three years in prison or a fine of up to NT\$ 1 million (US\$32,000) for spreading false information during wartime. Those who spread false information through broadcast TV, electronic communication, or the internet would be subject to more severe penalties. **163**

### **C3** 0-6 pts

**Are individuals penalized for online activities, particularly those that are protected under international human rights standards?**

**5/6**

*Score Change: The score improved from 4 to 5 because people were not sentenced to imprisonment for their online speech under SOMA during the coverage period.*

Internet users in Taiwan have been investigated or prosecuted for their online activities, although cases rarely lead to significant penalties like prison terms or steep fines.

Most investigations under SOMA are dismissed by the judiciary. In January 2024, for example, a man reposted a Facebook video of ballots between the panels of voting booths and labeled it “election fraud.” He was arrested on SOMA charges and stood trial. The court acquitted him, ruling that while his claim posed risks to election integrity and democracy, it could be easily discerned and proved inaccurate by the public. **164** The court also dismissed a similar case in March 2024 in which a man was

accused of SOMA violations after uploading a video related to the same election fraud conspiracy, which attracted around two thousand replies. **165**

In May 2024, the Constitutional Court nullified the conviction of Yang Hui-ru, who had been found guilty of insulting a public official under Article 140 of the criminal code; the court held that the offense of insulting a public office, distinct from insults aimed at a civil servant acting in their official capacity, was unconstitutional and infringed on freedom of speech **166** In February 2022, a court had sentenced Yang and another defendant, Cai Fu-ming, to five months' imprisonment (convertible to a fine) for violating Article 140. Yang was also charged under the SOMA, though the court found her not guilty on those charges. **167** Yang and Cai were charged in relation to claims that they incited people to spread rumors that allegedly contributed to a diplomat's death by suicide in 2018. **168**

During the previous coverage period, several people had been fined under the SOMA for political speech. In September 2022, an influencer was fined NT\$3,000 (US\$108) for spreading false information on the video-game streaming platform Twitch that President Tsai had died. **169** In June 2022, a man was fined NT\$5,000 (US\$160) in a SOMA case over messages he sent via Line containing false claims about COVID-19 vaccines. **170** The most recent data available showed that cases under Article 63(5) of the SOMA—which criminalized spreading rumors that undermined public order—spiked at 151 in 2019 and 320 in 2020. **171** The majority of those cases do not lead to convictions; **172** 243 of the 320 cases reported in 2020 resulted in no penalty, for instance. **173**

During the previous coverage period, internet users were found guilty of and fined for violating Article 14 of the Special Act for Prevention, Relief, and Revitalization Measures for Severe Pneumonia with Novel Pathogens, which expired in June 2023. One user, for example, was issued a suspended sentence and a NT\$5,000 (US\$160) fine in January 2023 for claiming to be COVID-positive to a Line group. **174**

#### **C4** 0-4 pts

**Does the government place restrictions on anonymous communication or encryption?**

**3/4**

There are some limits on anonymous communication, as Taiwan has mandatory SIM card registration requirements. **175** Telecommunications-related laws and regulations require service providers to record basic user information, including names and identification numbers, when selling all telecommunications numbers (including prepaid SIM cards). **176** The NCC emphasized in 2017 that registration assists government agencies in criminal and fraud investigation and prevention. **177**

Residents of Taiwan can freely use encryption technology. The Communication Security and Surveillance Act (CSSA) authorizes law enforcement agencies to intercept wired and wireless telecommunications signals with court authorization. **178** There is currently no explicit legal obligation for telecommunications companies to decrypt messages or provide decryption keys to law enforcement agencies, although they are required to ensure that both their hardware and software are compatible with interception efforts so that they can assist government surveillance. **179** Some within law enforcement agencies have complained that failure to decrypt messages undermines criminal investigations. **180**

In May 2024, the draft Technology Investigation and Security Law was sent to the Legislative Yuan for review. **181** A 2020 version of the draft law included a provision authorizing the government to use malware to intercept encrypted communications, **182** which CSOs such as the Judicial Reform Foundation mobilized against over its detrimental effect on privacy. **183** The provision ultimately was not included in the 2024 draft, **184** which was passed by the Legislative Yuan as an amendment to the code of criminal procedure, after the coverage period. **185**

**C5** 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	3/6
---	-----

The Taiwanese constitution expressly guarantees private correspondence and requires oversight for law enforcement agencies to monitor people's communications. **186** Judicial interpretations of the constitution have also protected the right to privacy and the right to self-determination of information. **187**

Additionally, the PDPA regulates the collection, processing, and utilization of personal data by government agencies and the private sector (see C6). **188** However, certain surveillance laws and procedures undermine these privacy rights in practice.

The CSSA stipulates that a court-approved “interception warrant” is required to access the content of communications in cases where suspects are accused of a range of serious crimes that carry minimum prison sentences of three years or more. **189** In case of urgent situations and for certain crimes, prosecutors may inform the enforcement authority to start surveillance without the court’s prior permission; however, the prosecutor must apply for a warrant within 24 hours of the operation. If the court does not issue a warrant within 48 hours, the surveillance must cease. **190** For certain serious crimes, including those that could result in prison terms of at least 10 years, prosecutors can directly access metadata without applying for a judicial warrant. **191**

An amendment to the CSSA passed in July 2024, after the coverage period, granted authorities further access to network traffic records including device identifiers, IP addresses, and domain names. The amendment also expanded the range of crimes for which prosecutors could authorize surveillance without prior court permission. **192** In response, CSOs raised serious concerns about the expansion of the government’s power to access people’s data and communications. **193**

As required by the CSSA, the Judicial Yuan publishes statistical reports about communication surveillance and communication record retrieval annually. **194** In practice, however, the law enforcement agencies increasingly conduct surveillance without seeking judicial approval, according to a 2018 Tahr report, indicating that the Judicial Yuan data undercounts the extent of such practices. **195** The High Prosecutors Office has been developing an analytics tool referred to as the Assistant Investigation Tech Platform (AITP) since 2021, **196** and the system may be used for data requests when deployed, further limiting transparency. **197**

The CSSA empowers the National Security Bureau (NSB), the country’s primary intelligence agency, to issue an interception warrant itself—without judicial permission beforehand—to authorize surveillance on communications concerning

“foreign forces” during times of emergency in order to protect national security. However, judicial approval must be obtained within 48 hours of the operation, or the surveillance must cease. **198** The NSB is not required to disclose its surveillance activity. **199**

The draft Technology Investigation and Security Law, which was later incorporated as an amendment to the code of criminal procedure and passed by the Legislative Yuan in July 2024, after the coverage period, authorizes law enforcement to track movements with geolocation data and investigate mobile device identifiers during criminal investigations. **200** The law authorizes the use of “M-Cars,” car-mounted IMSI (international mobile subscriber identity) catchers, which mimic mobile network towers and cause nearby phones to send identifying information; the technology enables law enforcement to track specific phones or identify phones in a given area. The law lacks safeguards—for example, prohibiting the use of IMSI catchers around protests and government buildings—that Taiwanese CSOs like the TAHR had urged policymakers to include. **201** In January 2022, the Taiwan High Prosecutors Office (THPO) disclosed that five law enforcement units, including the MJIB and the NPA, are equipped with M-Cars, and the THPO is planning to establish an M-Car team for future investigations. **202**

It is unclear whether the government has access to spyware technology, although some reports suggest that it does. In a 2015 report, Citizen Lab said Taiwan was one of the governments it had identified as “suspected customers” of the FinFisher spyware suite, and traced FinFisher servers to the country. **203** Previously, government agencies were found to have been in conversation with the now-defunct Italian firm Hacking Team about buying spyware, although there is no evidence that it was purchased. **204**

There are also concerns that state agencies conduct social media surveillance. The NSB admitted in 2018 that it monitors social media in order to track disinformation emanating from China and to ensure national security. **205** Other government units have also been found to have purchased monitoring and analytic systems. **206**

**C6** 0-6 pts

**Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?****3/6**

The PDPA governs the collection, processing, and usage of personal data, including by the private sector and nongovernmental agencies. The law broadly defines personal data to include any data that can be used to directly or indirectly identify an individual, including medical information, education, financial data, and social activities. The PDPA also regulates the cross-border transfer of data **207** and stipulates that individuals can apply for judicial relief if a public or private actor violates the law.

In August 2022, the Constitutional Court found that the lack of an independent and dedicated competent authority in PDPA was unconstitutional and ordered the government to remediate the problem within three years (i.e., no later than 2025 August). **208** In accordance, amendments to the PDPA were passed in May 2023 that require the establishment of an independent agency on privacy and data protection: the Personal Data Protection Commission (PDPC). **209** The May 2023 amendments also increased the penalties for data breaches, though opposition lawmakers criticized them for insufficiently addressing public sector data breaches. **210** Following the amended PDPA mandate, the Executive Yuan published several sets of organizational rules in September 2023 for the preparatory office whose mission is to implement the establishment of the PDPC. **211**

The government has enforced the PDPA to protect privacy. In December 2021, the Ministry of Culture ordered the Taiwan-based online outlet known at the time as *Apple Daily*—which had been affiliated with Hong Kong's *Apple Daily* newspaper until that company ceased publication in June 2021 after its assets were frozen under Hong Kong's National Security Law—not to transfer personal data to Hong Kong authorities. The ministry cited concerns that the Chinese government would exploit the information and urged the Taiwanese outlet to delete customers' personal data.

**212**

The TMA and the CSSA require service providers and the telecommunications industry to cooperate with criminal investigations and comply with law enforcement and other government authorities' surveillance requirements (see C5). **213** Compliance rates vary. For example, Taiwan Mobile reported that it received almost 200,000 data requests from law enforcement units in 2023 and complied with 99.98% of the requests. **214** Chunghwa Telecom stated that it received over two million requests from government agencies and law enforcement units in 2023, and it agreed to provide data in 53.49 percent of cases. **215**

Government units with certain investigative powers have also gone directly to state agencies and private companies to request personal data without first receiving a court order or other oversight. **216** For example, the Ministry of Economic Affairs received information in response to all of the 1,112 personal data requests it filed between 2017 and 2018, the most recent data available; 112 of the requests were to government agencies, with 1,000 to nongovernment agencies, including Chunghwa Telecom, Taiwan Mobile, and Yahoo! Taiwan Holdings Limited. **217**

Several laws mandate different data retention requirements. **218** Telecommunications providers are required to store communication records, subscriber information, and billing details for at least a year. **219**

The Special Act for Prevention, Relief, and Revitalization Measures for Severe Pneumonia with Novel Pathogens had been enacted in February 2020 at the beginning of the COVID-19 pandemic **220** and expired in June 2023. **221** It gave the Central Epidemic Command Center (CECC) broad power to conduct contact tracing and publicize personal information but had been criticized by civil society groups and other experts as lacking legality and proportionality. **222**

Introduced in 2020, Taiwan's Electronic Fence System uses mobile location tracking data to ensure individuals remain in quarantine. **223** It remained active during the coverage period, though its restrictions were reportedly loosened in May 2022. **224** The CECC can access aggregated data from the system, and police responding to quarantine-related alerts can access an individual's name, phone number, and

address. Those in quarantine must keep their phones on in order for the tracking to work.

### 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?**

**4/5**

Users are generally free from physical violence or other serious threats due to their online activity, although online harassment remains a concern. “Cyber manhunts” refer to the identification and pursuit of someone following criticism or their involvement in controversial events and often include doxing.

Online harassment escalated during the January 2024 election. A college student who asked critical questions of TPP presidential candidate Ko Wen-je at a forum was later doxed online; <sup>225</sup> similarly, a student asking critical questions of DDP candidate and now president Lai was doxed, as was her father. <sup>226</sup> A YouTuber claimed that she and her family had been cyber-harassed by KMT “net armies.” <sup>227</sup>

The normalization of doxing has also become a barrier to government transparency. For example, in November 2022, the government refused to publish a list of vaccine review experts, citing concerns over their safety and the risks of doxing. <sup>228</sup>

Although not routine, users have faced physical threats in relation to online activities during previous coverage periods. In February 2022, PTT influencer 4xCat was threatened by a candidate for municipal office over Facebook posts criticizing him. <sup>229</sup>

Taiwanese legislators have sought to limit the reach of online sexual harassment (see B3). In November 2021, the Legislative Yuan passed the Anti-Stalking Act, which seeks to prevent harassment and stalking, including online harassment. <sup>230</sup> The law took effect in June 2022. <sup>231</sup>

### C8 0-3 pts

**Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?**

**1/3**

Taiwan faces frequent overseas cyberattacks, emanating from Beijing in particular. Data breaches are common, including during the coverage period.

Cyberattacks spiked ahead of and during the January 2024 election. The cybersecurity and internet infrastructure company Cloudflare reported that distributed denial-of-service (DDoS) attack traffic targeting Taiwan in late 2023 surged by more than 3,000 percent compared to the same period the previous year. **232** Another cybersecurity company, Recorded Future, reported that it observed a string of cyberattacks from a Chinese state-linked hacking group between November 2023 and April 2024 targeting more than 70 Taiwanese organizations, including government agencies and companies that contract with the government. **233**

In a 2024 study conducted by Open Culture Foundation, a Taiwanese organization promoting open source technology, more than half of the 35 interviewed Taiwan CSOs reported that they had experienced cyberattacks posing threats to their online accounts or data. Six organizations reported having their communications intercepted and 12 reported being hacked. Over 80 percent of the interviewed organizations say that foreign authoritarian governments, most notably China, pose a threat of cyberattacks. **234**

In October 2022, during the previous coverage period, security researchers reported that an online hacker forum had offered to sell Taiwan's household registration information that was claimed to include more than 23 million entries, which is almost equivalent to the population of Taiwan. **235** Analysis of a subset of that data found that it included names, identification numbers, home addresses, and other sensitive personal information, and that it likely dated to 2019. **236** In February 2023, the MJIB reported that the hacker is suspected to be a Chinese national. **237**

Private sector data leaks are also a serious issue in Taiwan. Cybersecurity firm Check Point reported that organizations in Taiwan face over 3,000 cyberattacks every week.

**238** Several customer data leaks occurred during the coverage period. Those cases involved car rental and sharing services platform iRent, **239** the state-owned flag carrier China Airlines, **240** and the chain department store Breeze. **241**

The Cyber Security Management Act oversees the cybersecurity of critical infrastructure providers. It requires that public agencies formulate cybersecurity maintenance plans and stipulates report-and-response mechanisms for security incidents. **242** The Executive Yuan also established the DCS in 2016 to safeguard Taiwan’s digital infrastructure. **243**

## Footnotes

- 1** Simon Kemp, “Digital 2024: Taiwan,” DataReportal, February 23, 2024, <https://datareportal.com/reports/digital-2024-taiwan>
- 2** Taiwan Network Information Center, “2023 台灣網路報告[2023 Taiwan Internet Report]”, August 2023, page 20, [https://report.twNIC.tw/2023/assets/download/TWNIC\\_TaiwanInternetReport...](https://report.twNIC.tw/2023/assets/download/TWNIC_TaiwanInternetReport...)
- 3** Taiwan Network Information Center, “2020 台灣網路報告 [2020 Taiwan Internet Report],” 2020, [https://report.twNIC.tw/2020/en/report\\_en.pdf](https://report.twNIC.tw/2020/en/report_en.pdf). Chinese version available here: [https://report.twNIC.tw/2020/assets/download/TWNIC\\_TaiwanInternetReport...](https://report.twNIC.tw/2020/assets/download/TWNIC_TaiwanInternetReport...), “Overview of Overall Internet Usage,” 2022, [https://report.twNIC.tw/2022/en/TrendAnalysis\\_internetUsage.html](https://report.twNIC.tw/2022/en/TrendAnalysis_internetUsage.html); iTaiwan Wifi, “iTaiwan 無線上網服務簡介 [Introduction to iTaiwan Wireless Internet Service,]” Accessed February 15, 2024, [https://itaiwan.gov.tw/faq\\_service.php](https://itaiwan.gov.tw/faq_service.php).
- 4** National Communications Commission, “寬頻上網帳號數(112年)[2023 Number of Fixed-line Broadband Accounts],” December 2023, [https://www.ncc.gov.tw/chinese/news\\_detail.aspx?site\\_content\\_sn=2035&ca...](https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=2035&ca...)
- 5** Taiwan Network Information Center, “2023 台灣網路報告[2023 Taiwan Internet Report]”, August 2023, <https://report.twNIC.tw/2023/>.

More footnotes





### On Taiwan

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

[See More >](#)

### *Country Facts*

Population

**23,570,000**

Global Freedom Score

**93/100** Free

Internet Freedom Score

**79/100** Free

Freedom in the World Status

**Free**

Networks Restricted

**No**

Social Media Blocked

**Yes**

Websites Blocked

**No**

Pro-government Commentators

**No**

Users Arrested

**No**

*In Other Reports*

Freedom in the World 2024

*Other Years*

2025
------

## Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

PO Box 33139  
Washington, DC 20033  
(202) 296-5101

GENERAL INQUIRIES

[info@freedomhouse.org](mailto:info@freedomhouse.org)

PRESS & MEDIA

[press@freedomhouse.org](mailto:press@freedomhouse.org)

@2026 FreedomHouse

Freedom House is a 501(c)(3) organization registered in the US under EIN: 13-1656647.