FREEDOM ON THE NET 2020

Singapore

PARTLY FREE

54 /100

A. Obstacles to Access	19 /25
B. Limits on Content	17 /35
C. Violations of User Rights	18 /40

LAST YEAR'S SCORE & STATUS
56 /100 Partly Free

Scores are based on a scale of 0 (least free) to 100 (most free)

Overview

Internet freedom in Singapore declined as the government increased its control over content. The authorities employed the newly enacted Protection from Online Falsehoods and Manipulation Act (POFMA) to crack down on critical voices and censor a range of online material. Ahead of the July 2020 general elections, POFMA was used against media platforms and opposition politicians. Moreover, ordinary users continued to be investigated by

On Singapore

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

police and criminally charged for the political and social content they posted, further reducing the space for free expression and free assembly online.

The ruling People's Action Party (PAP) has dominated Singapore's parliamentary system since independence. It allows for some political pluralism, but it constrains the growth of credible opposition parties and limits freedoms of expression, assembly, and association.

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

- POFMA came into effect in October 2019, giving any government minister broad censorship powers and the ability to undermine free expression without judicial oversight (see B2, B3, B6, C1, and C2).
- In January 2020, the website of Lawyers for Liberty, a Malaysian nongovernmental organization (NGO), was blocked after the group failed to comply with a POFMA correction notice regarding its statements on Singapore's system of capital punishment (see B1 and B2).
- Ministers repeatedly invoked POFMA to order independent news websites, opposition politicians, NGOs, and social media users to publicize correction notices pertaining to their online content (see B2 and B3).
- Only a handful of more than 40 orders issued under POFMA were challenged in the High Court during the coverage period; the suits were brought by the Singapore Democratic Party and the *Online Citizen*, a media outlet (see B3).

See More

Country Facts

Global Freedom Score
50 /100
Partly Free

Internet Freedom Score
54 /100
Partly Free

Freedom in the World Status
Partly Free

Networks Restricted
No

Social Media Blocked
No

Websites Blocked
Yes

Pro-government Commentators
No

Users Arrested
Yes

In Other Reports

Freedom in the World 2020

- Under the Public Order Act, police interrogated two Singaporeans about images on social media in which they held signs meant to raise awareness of the country's climate change policies. The scrutiny illustrated the shrinking space for digital activism (see B8 and C3).
- As part of its efforts to limit the spread of COVID-19, the government launched the TraceTogether application, which used Bluetooth technology to identify and notify individuals who have been in close contact with someone who tested positive for the virus (see C5).

Other Years

2019

A. Obstacles to Access

As a wealthy and compact city-state, Singapore has developed its information and communication technology (ICT) infrastructure to an advanced level. The government achieved its target of 90 percent home broadband penetration as part of its Intelligent Nation 2015 master plan for an ultra-high-speed, pervasive network. The national wireless network offers free public access.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**6** / 6

Singapore's internet penetration rate is high, as is the general quality of service. Some 93 percent of resident households had broadband internet access as of 2019. [1] In the third quarter of 2019, there were more than 10.7 million broadband subscriptions on the island. [2]

Mobile data usage reached 36.06 PB in the third quarter of

2019. [3] Fifth-generation (5G) mobile network deployment was set to begin in 2020, with the aim of standalone coverage by 2025. [4]

The fiber-based Nationwide Broadband Network (NBN), providing speeds of 1 Gbps or more, reaches more than 95 percent of homes and businesses. The national wireless network, Wireless@SG, offers free public access via hotspots running at 5 Mbps. The Infocomm Media Development Authority (IMDA), the industry regulator, told local media in August 2018 that there were over 20,000 public Wireless@SG Wi-Fi hotspots across the island. [5] However, a list released by IMDA in December 2019 showed the locations of only a little more than 5,000 hotspots. [6]

The government is experimenting with a heterogeneous network (HetNet), a new wireless system that allows smartphone users to switch automatically between mobile and Wi-Fi networks for smoother mobile internet use. [7]

The government is active in promoting its Smart Nation initiative, seeking to position Singapore as a "leading economy powered by digital innovation." As part of the plan, the government is building the backbone infrastructure to support big data, the so-called internet of things, and other advances. [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?	**3**/3

The internet is largely available to all users in Singapore. The government has undertaken projects to limit any existing digital divide, such as that which cuts along generational

lines.

There has been less of a digital divide based on age in recent years. While 100 percent of residents between 15 and 24 years of age reported in 2018 that they had used the internet in the past three months, the rate was 55 percent for those 60 and older. [9] There has also been an increase in the number of older people using portable internet-enabled equipment, such as smartphones: 73 percent of people over the age of 60 reported using such devices in 2018, up from 47 percent in 2016. [10]

A3 0-6 pts

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

No known restrictions have been placed on ICT connectivity, either permanently or during specific events. The Singapore Internet Exchange (SGIX), a nonprofit entity established by the government in 2009, provides an open, neutral, and self-regulated central point for service providers to exchange traffic with one another directly, instead of routing it through international carriers. This improves latency and resilience when there are cable outages on the international network. [11]

Singapore's NBN structure is built and operated by an entity that supplies wholesale-only, open-access, and nondiscriminatory services to all telecommunications carriers and service providers. [12] To avoid conflicts of interest, separate companies have responsibility for passive infrastructure and active infrastructure such as routers, as well as for retail-level service provision downstream.

A4 0-6 pts

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

Service providers do not face onerous obstacles to entry or operation within Singapore. However, users' choices among internet service providers (ISPs) and mobile providers remain limited.

The dominant ISPs are also the main mobile service providers: SingTel, Starhub, and M1. SingTel, formerly a state telecommunications monopoly and now majority-owned by the government's investment arm, has a controlling stake in Starhub. MyRepublic launched a broadband service in 2014, and began offering mobile services in 2018. [13] Other relatively new players include ViewQwest and Circles.Life, Singapore's first fully digital telecommunications company. [14] The virtual mobile telecommunications carrier Zero Mobile stopped offering mobile plans in December 2019, although it insisted that it was not exiting the market. [15] The Australian telecommunications company TPG Telecom launched commercial services at the end of March 2020, and has submitted a bid for one of four 5G licenses. [16]

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?	**1**/4

Government agencies oversee service providers and digital technology, and the regulatory framework lacks independence. Under the Telecommunications Act, licenses for telecommunications systems and services can be issued either unconditionally or with conditions as specified by the authorities. [17] The IMDA is responsible for both the

development and regulation of the converging infocommunications and media sectors. [18] The IMDA is not an independent public agency but a statutory body of the Ministry of Communications and Information (MCI).

B. Limits on Content

POFMA, the Protection from Online Falsehoods and Manipulation Act, went into effect during the coverage period, granting broad censorship power to any government minister. Ministers issued correction orders to a range of entities and people in practice, and ISPs were ordered to block at least one website for not complying with POFMA. Separately, the space for online activism continued to shrink, with police opening investigations against digital campaigners. Despite such measures, the internet remained significantly more open than print or broadcasting as a medium for news and political discourse.

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?	**4**/6

Long-term blocks are imposed on certain websites, and the government directed ISPs to restrict access to at least one website during the coverage period in response to its critical content.

In January 2020, the MCI ordered ISPs to block the website of the Malaysian NGO Lawyers for Liberty. The block came after the group failed to publish a POFMA correction notice related to its statements on Singapore's methods of capital punishment (see B2). [19] The website remained blocked as of May 2020.

In December 2018, the IMDA had temporarily blocked access to the news site *Singapore Herald*, after it refused to comply with a number of takedown orders. The authorities claimed that eight articles published that month on a maritime dispute between Singapore and neighboring Malaysia "blatantly mispresent[ed]" Singapore's position and used "false statements" and "emotionally charged phrases." [20] The *Singapore Herald* is known for its strident criticism of the ruling party, and it is edited by Alex Tan, who also ran the *States Times Review*, a news site that shifted its activity to Facebook after November 2018. [21] A July 2020 test by the Open Observatory of Network Interference found signs of DNS tampering, suggesting that the website could still be blocked. [22]

In November 2018, the IMDA had directed ISPs to restrict access to the *States Times Review* after it refused to comply with an order to take down an article claiming that Prime Minister Lee Hsien Loong was a key target of money-laundering investigations surrounding 1Malaysia Development Berhad (1MDB), a Malaysian state investment fund. The article's claims were rejected by both the Singaporean government and the *Sarawak Report*, an online investigative journalism outlet that helped expose the 1MDB corruption scandal. [23] The IMDA said that the article contained "prohibited content" under its Internet Code of Practice, claiming that the content "undermined public confidence in the integrity of the Singapore government and is objectionable on grounds of public interest." [24] An April 2020 test by the Open Observatory of Network Interference found signs of DNS tampering, suggesting that the website could still be blocked. [25]

As a matter of policy, the IMDA blocks a list of 100 websites to signal societal values. This floating list has never been made public, but no political site is thought to have been

blocked. Other than a few overseas sites run by religious extremists, the list is known to comprise pornographic sites. [26] In addition to this list, the Canada-based extramarital dating website Ashley Madison has been blocked since 2013, after it announced its plan to launch in Singapore. [27] The use of regulation to signpost societal values has been linked to the influence of religious conservatives (mainly evangelical Christians), who have asserted themselves more in public morality debates in recent years. [28]

In May 2018, the High Court ordered ISPs to block 53 websites containing pirated materials, including Pirate Bay and SolarMovie. [29] In July 2018, the High Court also ruled in favor of "dynamic site blocking," allowing the blocking of websites that link to the original 53 sites. [30]

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?	**1** / 4

The state has sought to employ legal, administrative, and other means to remove content. Since the implementation of POFMA in October 2019, correction orders have been issued against news outlets, opposition figures, and NGOs.

Government ministers did not order content to be removed under POFMA during the coverage period. [31] However, ministers repeatedly used the law to order the publication of correction notices. [32] Such correction orders were issued to independent news websites, opposition politicians, and social media users, in relation to a variety of allegedly false claims, on topics including the annual salary of the chief executive of state-owned investment company Temasek Holdings and local transmission of the coronavirus

driving the COVID-19 pandemic. [33] After the reporting period, POFMA orders were issued during the election cycle by senior civil servants who had been temporarily appointed by government ministers as alternate authorities. These orders targeted content related to statements or talking points from opposition politicians about funding for foreign students, [34] Singapore's population policies, [35] and handling of COVID-19. [36]

Authorities ordered the Malaysian NGO Lawyers for Liberty to issue a correction for its publication of allegations by an anonymous former prison officer that the Singapore Prison Service used illegal methods of execution if deemed necessary (see B1). [37] Three entities that shared the article, including Yahoo Singapore and the *Online Citizen*, also received ministerial orders to correct the "falsehoods." Lawyers for Liberty has since filed a motion in the Kuala Lumpur High Court against Singapore's home affairs minister, claiming that the correction order was an attempt to encroach on freedom of expression in Malaysia. [38]

In February 2020, Facebook complied with a request from the MCI to disable Singapore-based users' access to the *States Times Review*. Its publisher, Alex Tan, had refused to comply with POFMA orders after the outlet was designated as a "declared online location" (see B6). [39] The *States Times Review* had previously received three separate correction orders. [40] In June 2020, Facebook said that it complied with ministry requests to disable Singapore-based users' access to *National Times Singapore*'s page, also administered by Tan. [41] Facebook was similarly told to restrict access to the affiliated *Singapore States Times* and Tan's own Facebook page. [42] Tan himself did not comply with any of the orders.

Streaming platforms have also complied with requests to

remove content. In February 2020, for example, Netflix reported that it had complied with five requests from the IMDA between 2018 and 2020 to remove titles related to marijuana or Christianity from its platform. **43**

In July 2019, the IMDA issued requests to remove an online rap video by siblings Preeti and Subhas Nair that criticized a controversial advertisement in which a Chinese actor darkened his skin to portray characters of other ethnicities. Police opened an investigation following reports against the two (see C3). **44** Activists Roy Ngerng and Jolovan Wham reported that they also received takedown orders to remove Facebook posts sharing the rap video. Twitter users reported that some posts sharing the video were unavailable to other accounts based in Singapore, with at least one user citing a tweet that was "withheld in Singapore in response to a legal demand." **45** Preeti and Subhas Nair publicly apologized twice about their video after it was removed. **46**

In November 2019, Facebook removed NUSSU-NUS Students United, a page spoofing a local university group, after the government said that it had used a quote from Minister for Law and Home Affairs K. Shanmugam in a misleading way. Facebook said that the group had failed to meet the company's authenticity and community guidelines. **47** An employee of the Housing Development Board was fired in May 2020 for his alleged involvement with the page, and he was placed under investigation by the police for allegedly impersonating another person to run the page. **48**

In December 2019, the Singapore Democratic Party called on Google to explain its decision to ban political advertising in Singapore. In response, Google said it would not accept any advertising that is regulated under Singapore's Code of Practice for Transparency of Online Political Advertisements, **49** which was established under POFMA.

The code requires hosts, platforms, or other intermediaries to develop due-diligence measures that include disclosure notices indicating who requested or paid for the advertisement, providing the government with a record of all online political advertisements, and implementing government reporting channels. [50] The Singapore Democratic Party argues that Google's ban on political advertising could disproportionately affect opposition parties, which receive less coverage in the mainstream media.

Since the Class License system was introduced in 1996 (see B3), it has been used to restrict access to sensitive websites. In late 2018, the IMDA ordered the *States Times Review* and *Singapore Herald* to remove content from their websites after both sites allegedly breached the Internet Code of Practice. When they refused to comply, the IMDA directed ISPs to temporarily block the pages (see B1).

In September 2018, Terry Xu, chief editor of the *Online Citizen*, complied with an IMDA request demanding that he remove a reader's letter within six hours. [51] The letter contained a reference to corruption at the "highest echelons" of the political elite, as well as "tampering of the Constitution." Both Xu and the letter's author were investigated and charged with criminal defamation (see C3).

Eleven news sites have been licensed under a notice-and-takedown framework, which requires them to comply with government orders to remove content within 24 hours (see B3). Nine are run by either Singapore Press Holdings (SPH) or MediaCorp—which, as newspaper and broadcasting companies, are already subject to discretionary individual licensing and traditionally have cooperated with the government (see B6).

Individual government officials are known to demand

retractions or apologies for comments on social media that they take issue with. In September 2019, Prime Minister Lee Hsien Loong demanded that Xu remove and apologize for an *Online Citizen* article that he claimed was defamatory. [52] After Xu refused, Lee initiated defamation proceedings against him (see C3). [53] In May 2020, Minister for Manpower Josephine Teo sent letters demanding that activist Jolovan Wham and another individual withdraw comments suggesting corruption on the part of her and her husband, the chief executive of Temasek Holdings, during the COVID-19 outbreak. [54] Both men withdrew their comments and apologized. [55]

After the reporting period in June 2020, and ahead of the July general elections, Facebook announced that it had removed accounts and pages for "inauthentic behavior." [56] Among those removed included the progovernment Fabrications About the PAP page, [57] as well as three accounts running the *Critical Spectator*, a commentary page that also posts progovernment content. [58]

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

There is a lack of transparency in the process for restricting online and digital content.

POFMA, which came into effect in October 2019, provides any government minister with the power to order correction notices and remove or restrict access to content if they find that it contains false statements and are of the opinion that it would be in the public interest to take action (see C1 and C2). Ministers are not required to obtain court

orders to have their directives enforced; instead, the directives must first be complied with, even if one intends to lodge an appeal with the High Court. [59] In addition to content publishers, internet intermediaries can be held liable if they do not comply with orders to issue corrections or remove content.

Only a handful of the more than 40 orders issued during the coverage period were challenged in the High Court. [60] The first two cases, brought by the Singapore Democratic Party and the *Online Citizen*, were in chambers and not open court. [61] The High Court has since dismissed both appeals. [62] While the High Court judge in the Singapore Democratic Party's case ruled that the burden of proof of a statement's falsehood should lie with the government, [63] the judge in the *Online Citizen*'s case later disagreed and said the onus should be on the appellant. [64] Both the Singapore Democratic Party and the *Online Citizen* were granted leave, in February and March, [65] respectively, to appeal the High Court's decisions. Separately, the *Online Citizen* filed another appeal against a subsequent POFMA order, [66] while the independent media platform New Naratif indicated its intention to challenge a POFMA order it received in May 2020. [67]

The Broadcasting Act has included explicit internet regulations since 1996. Internet content providers and ISPs are licensed as a class and must comply with the act's Class License Conditions and the Internet Code of Practice. Under this regime, ISPs are required to take "all reasonable steps" to filter any content that the regulator deems "undesirable, harmful, or obscene." [68]

The Broadcasting Act empowers the MCI minister to prohibit disclosure of any orders to censor content. [69] This—together with the fact that most ISPs and large online

media companies have close ties to the government —results in a lack of transparency and public accountability surrounding online content regulation.

The IMDA's notice-and-takedown framework exists for high-impact online news sites—those receiving visits from a monthly average of at least 50,000 unique internet protocol (IP) addresses in Singapore. Since the IMDA is not obliged to make its takedown orders public, and there is no culture of leaks from major media organizations, it is not possible to gauge how often this mechanism is used.

Introduced in 2013, the notice-and-takedown framework removes the relevant sites from the class license and subjects them to individual licensing, under which they are required to comply with any takedown notice within 24 hours. The sites are obliged to put up a "performance bond" of S$50,000 (US$37,000) as an incentive to remain in compliance. [70] The bond is in line with the requirement for niche television broadcasters. [71]

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**2** / 4

Self-censorship is common among journalists, commentators, and ordinary users, who are all aware that there could be repercussions, including civil and criminal penalties, for certain types of speech or expression (see C3). [72] Matters of race and religion, as well as any comment on the independence of the judiciary or alleged government malfeasance, are considered particularly sensitive, given Singapore's laws relating to sedition, religious harmony, contempt of court, and defamation (see C2). [73]

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?	**2**/4

Given the dominance of the ruling PAP, mainstream online sources of information generally toe the government line, although these outlets occasionally publish critical content.

The government exerts influence over online information through formal ownership or executive oversight of mainstream outlets. The most read online news sources are the websites of the mainstream newspaper and broadcast outlets owned by SPH and MediaCorp. MediaCorp is state owned; while SPH previously held a 20 percent stake in MediaCorp Press, it sold its shares back to MediaCorp in 2017. **74** SPH is a publicly listed company, but under the Newspaper and Printing Presses Act, the government can nominate individuals to its board of directors. Since the 1980s, every SPH chairman has been a former cabinet minister. The government is known to have a say in the appointment of SPH's chief executives and chief editors. **75** The government's ability to control online content was on display in October 2018, when the political editor of the mainstream outlet the *Straits Times* was transferred to another desk after government officials complained about coverage under her watch. **76**

In addition to influencing the online media environment, the government uses more informal means to advance progovernment commentary. Individual ministers and government agencies have ramped up and professionalized their social media capacity, including publishing press releases on social media platforms like Facebook. The organizers of major government campaigns regularly and openly commission bloggers and creative professionals. In

January 2018, the Ministry of Finance paid over 50 "influencers" on Instagram to promote public awareness of the upcoming budget debate. [77]

Certain pro-PAP websites and Facebook pages that attack the opposition have been described as engaging in "guerrilla-type activism," with supporters responding quickly to antiestablishment comments online. [78] Bloggers have pointed out that some (largely progovernment) online commentators hide behind anonymous profiles; these accounts are often referred to as the "Internet Brigades," or IBs. [79] However, there is no concrete evidence of large-scale covert deployment of paid online commentators. After the end of the coverage period, some pro-PAP Facebook pages were removed by Facebook for violating its policies (see B2).

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**1** /3

Online-only news outlets struggle to remain financially viable, due in part to restrictions on foreign funding and registration rules. POFMA may exacerbate financial instability by allowing the government to demonetize websites (see B3 and C1). Under the new law, government ministers can designate any website or page as a "declared online location" if it has repeatedly published allegedly false information. Websites with this designation are not allowed to accept donations or sell advertising or subscriptions. [80] In February 2020, the Facebook page of the *States Times Review* was made the first "declared online location." [81] Since then, three other pages administered by Tan—the *Singapore States Times*, *National Times Singapore*, and Tan's

own Facebook page—have been designated "declared online locations" after receiving POFMA orders (see B2). [82]

Special IMDA registration rules prohibit foreign funding and require certain sites to provide details about funding sources. [83] In effect, this prevents sites from receiving grants and loans from foreign foundations, which have been essential for most independent political sites in the region. The *Online Citizen* and the *Independent*, two sites known for critical commentary, fall under these registration rules and have never had the capacity to generate original daily news or regular investigative features. [84]

In September 2018, the minister of finance rejected an appeal from New Naratif—an online platform cofounded by Singaporeans that advocates for democracy in Southeast Asia—to register as a Singapore subsidiary of its parent entity, which is based in the United Kingdom. In April 2018, the Accounting and Corporate Regulatory Authority publicly declined to register the group on the grounds that it would be "contrary to Singapore's national interests" to allow registration, pointing to the political orientation of New Naratif and its work, such as "publishing articles critical of politics in regional countries" and organizing democracy classrooms. [85] The refusal to allow the platform to register as a subsidiary company limits its ability to operate as a legal entity in Singapore, which is necessary to open bank accounts, hire employees, and rent venues.

Some online outlets have found ways to sustain themselves financially, although there are concerns that the COVID-19 pandemic will present new financial challenges. The media start-up Mothership appears to be financially stable, and counts among its advertising partners multiple government ministries and agencies, including the Ministry of Defence, the Ministry of Finance, and the Economic Development

Board. [86] This has contributed to what analysts call a "normalization" of online space, with the PAP's ideological dominance of the offline world increasingly reflected online. [87] Rice Media, a niche digital outlet that launched in 2016, has also managed to sustain itself through advertising and seed funding from venture-capital investors. [88]

B7 0-4 pts

Does the online information landscape lack diversity?	**3**/4

While the online information landscape is significantly more diverse than offline media, independent and opposition-oriented online news outlets are too small and weak to counterbalance the media domination of the PAP establishment. Struggling financially and working with limited resources, independent sources of online news are unable to challenge the newsgathering and dissemination capabilities of mainstream media.

The only two licensed outlets that do not belong to national mainstream media firms are Yahoo Singapore's news site and Mothership. After Yahoo was licensed, its reporters were granted the official accreditation that they had sought for several years. In 2015, Mothership became the first individually licensed site that was not part of a major corporation, after it crossed the regulatory threshold of 50,000 visitors a month. [89] Although it is popular for its irreverent commentary, Mothership is not considered an antiestablishment outlet.

YouTube, Facebook, Twitter, and international blog-hosting services are freely available, and most bloggers operate openly. All major opposition parties and many NGOs are active online.

B8 0-6 pts

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

Score Change: The score declined from 4 to 3 because the space for online activism has dwindled, with users facing interrogation or criminal charges for their participation in digital mobilization efforts.

The internet is regularly used for popular mobilization by groups from across the political spectrum, and mobilization tools are unrestricted. However, the success of these efforts is significantly constrained by police investigations and arrests for those participating in online activism, as well as by offline restrictions on fundraising and public assembly. There is only one location—a small downtown park known as Speakers' Corner—where Singaporeans can gather without a police permit. The country's restrictive laws generally limit public demonstrations, including solo protests (see C2 and C3).

In March 2020, two young Singaporeans posted photos of themselves on social media holding up placards meant to draw attention to the presence of major oil companies in Singapore and raise awareness about the country's climate policies. Both individuals were interrogated by police as part of an investigation under Singapore's Public Order Act. [90]

In January 2019, activist Jolovan Wham was found guilty of organizing an illegal assembly and refusing to sign a police statement (see C3). [91] The assembly in question was an indoor forum held in 2016, in which Hong Kong prodemocracy activist Joshua Wong participated as a speaker via Skype. The authorities argued that because Wong was a foreign speaker, a permit should have been

obtained for the event. In a separate charge against Wham in March 2019, police argued that he was protesting without a permit when he used social media to criticize a criminal defamation case against Terry Xu, chief editor of the *Online Citizen*, and a reader of the outlet (see C3). **92**

In September 2019, more than 1,700 Singaporeans attended the country's first climate rally, **93** whose organizers relied largely on the internet and social media platforms to promote and share information about the event. **94** Similarly, Speak for Climate has mobilized online to encourage Singaporeans to participate in the public consultation process organized by the National Climate Change Secretariat. **95**

With the introduction of social-distancing rules and a partial lockdown in Singapore during the COVID-19 pandemic, civil society events shifted online, which allowed organizers to accommodate and reach more people. In March 2020, organizers of Singapore's largest LGBT+ pride rally, Pink Dot, announced that the physical event would be canceled and replaced with a live-streamed event in June. **96**

In April 2019, a student at the National University of Singapore declared on Instagram that the university administration and police did not adequately respond to her complaint that she was sexually harassed on campus. **97** In response, students mobilized—largely online—to pressure the administration to hold a town-hall meeting to hear their concerns. **98** The university ultimately held the requested meeting and strengthened its policy on campus sexual harassment. **99**

C. Violations of User Rights

While citizens remain free from major human rights abuses and enjoy high levels of personal security, the government places a premium on order and stability at the expense of free speech and political dissent. The enforcement of POFMA, the Protection from Online Falsehoods and Manipulation Act, during the coverage period demonstrated the government's growing efforts to undermine legal protections for freedom of expression. The authorities are also believed to exercise broad legal powers to obtain personal data for surveillance purposes in national security investigations.

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?	**1** / 6

Score Change: The score declined from 2 to 1 due to the implementation of the Protection from Online Falsehoods and Manipulation Act, which added to the country's growing legal restrictions on free expression.

The constitution enshrines freedom of expression, but it also grants Parliament the authority to impose limits on that freedom. **100** The PAP has consistently controlled roughly 90 percent of the seats in Parliament, limiting opposition influence and oversight of legislation.

POFMA, which came into effect in October 2019, gives individual government ministers broad power to order the blocking and removal of online content that they deem a "false statement of fact" and contrary to the public interest (see B3). Ministers can also order social media platforms to issue general corrections to their end users. Appeals can

only be made to the High Court if the minister who ordered content removed fails to revise the initial decision, essentially giving ministers the ability to decide what is true or false twice before the judiciary weighs in. The legislation does not clearly explain what constitutes false or misleading content and broadly defines "public interest" to include the preservation of "public tranquility," "friendly relations" with other countries, and public confidence in government institutions. **101** The law was adopted based on the recommendations of Parliament's Select Committee on Deliberate Online Falsehoods, which released its report in September 2018. **102**

As part of its efforts to combat disinformation, the government announced in February 2019 that it was considering legislation to counter foreign interference. This would include prohibiting foreign funding for "politically involved individuals and organizations" in Singapore. **103** It is unclear how the government will define "politically involved," but the need to counter foreign interference has previously been used as a justification for clamping down on civil society activities and independent media (see B6 and B8). In comments related to the potential introduction of such a law, the law minister made references to independent media outlets the *Online Citizen* and New Naratif. **104**

Contempt of court charges have frequently been lodged to stifle public debate in Singapore, including against bloggers who wrote about issues such as discrimination against LGBT+ people and the treatment of opposition politicians in the courts. **105** A contempt of court law was passed by Parliament in 2016, and it came into force a year later (see C2). **106**

The Newspaper and Printing Presses Act and the

Broadcasting Act, which also covers the internet, grant sweeping powers to ministers as well as significant scope for administrative officials to apply vaguely articulated subsidiary regulations as they see fit, including website licensing and registration rules (see B6). Other laws that have been used to restrict online communication, such as the Sedition Act and the Political Donations Act, are open to broad interpretation by the authorities (see C2).

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	**2**/4

A number of laws apply criminal and civil penalties to online activities. The 2018 Public Order and Safety (Special Powers) Act gives the authorities the power to ban communications—including videos, images, text, or audio messages—in the event of a "serious incident." The definition of a "serious incident" encompasses terrorist attacks as well as peaceful protests such as large sit-down demonstrations. [107] Those found guilty of violating the law could be sentenced to up to two years in prison and a fine of S$20,000 (US$15,000). [108] The measure effectively allows heavy restrictions on online journalism and information sharing surrounding major public events.

In 2016, Parliament passed a new statute codifying the offense of contempt of court. [109] The Administration of Justice (Protection) Act, which came into force in 2017, specifies that it is an offense to publish material that interferes with ongoing judicial proceedings or to "scandalize the court" by publishing anything that "imputes improper motives to or impugns the integrity, propriety, or impartiality of any court" or "poses a risk that public confidence in the administration of justice would be

undermined." The law lowered the threshold for what constitutes a "risk" of harm to the administration of justice. It also allows the attorney general to "direct the publisher of any matter to refrain from or cease publishing" content that might be in contempt of court. The maximum penalty under the law is three years in prison and a fine of S$100,000 (US$73,000), a harsher punishment than judges had previously imposed. [110]

The Sedition Act, which dates to the colonial era, makes it an offense "to bring into hatred or contempt or to excite disaffection against the government" or "to promote feelings of ill will and hostility between different races or classes of the population of Singapore." [111] Punishments for first-time offenders can include a prison term of up to three years. Section 298 of the penal code provides for prison terms of up to three years for offenders who act through any medium with the "deliberate intention of wounding the religious or racial feelings of any person." [112] Police appear to regularly investigate such complaints. In most known cases, police intervention at an early stage has been enough to elicit apologies that satisfy complainants.

Defamation is criminalized in the penal code (see C3). [113] In addition to criminal charges, civil defamation suits remain a powerful deterrent. PAP leaders have been awarded damages ranging from S$100,000 (US$73,000) to S$300,000 (US$220,000) in defamation suits brought against opposition politicians and foreign media corporations. [114]

Under the 2014 Protection from Harassment Act, a person who uses "threatening, abusive, or insulting" language likely to cause "harassment, alarm, or distress" can be fined up to S$5,000 (US$3,700). [115] Victims can also apply to the court for a protection order, which could include a ban on

continued publication of the offending communication. Another provision in the law provides civil remedies for the publication of "false statements of fact" about a person. The affected party can seek a court order requiring that the publication of the falsehood cease unless a notice is inserted to correct the record. The law was amended in May 2019 to outlaw doxing with intent to either harass or provoke the use of violence. The amendments also allow victims of harassment to seek protection for family members or prevent similar material from being circulated. [116]

Singapore's broad public assembly laws, such as the Public Order Act, have been used in prosecutions that cite people's online activity (see C3). [117] Those convicted of organizing public assemblies without a permit can be fined up to S$5,000 (US$3,700); repeat offenders can be fined up to S$10,000 (US$7,300) and imprisoned for up to six months.

POFMA includes harsh penalties for online activities. For example, the malicious communication of statements that are "false or misleading" can lead to fines of up to S$50,000 (US$37,000) or up to five years' imprisonment. Failure to comply with orders to correct or remove content can draw fines of up to S$20,000 (US$15,000) or up to one year of imprisonment (see B3).

C3 0-6 pts

Are individuals penalized for online activities?	**3**/6

Police opened investigations into individuals for their online activities during the coverage period, and cases initiated earlier continued to be adjudicated.

Users have been investigated and arrested for their online

mobilization (see B8). In April 2020 the police began investigations into Wong J-min and Nguyen Nhat Minh, two young climate activists who had posted photos of themselves holding signs in public places to draw attention to climate change and Singapore's relationship with fossil fuels (see B8). [118] The two were investigated under the Public Order Act, which bans even solo protests without a permit. As part of the investigation, their mobile phones were confiscated, as was Nguyen's laptop. Both were later issued warnings by the police but were not charged. Similarly, an investigation was opened into activist Jolovan Wham in May 2020 for a photo he posted on social media in which he held a cardboard placard in public with a smiley face drawn on it. [119] Wham had taken the photo as a show of solidarity with Wong and Nguyen.

Wham had previously been convicted in January 2019 for organizing an illegal assembly and refusing to sign a police statement. [120] That case involved a 2016 forum in which Hong Kong prodemocracy activist Joshua Wong participated as a speaker via Skype; the authorities argued that a permit was required for events with a foreign "speaker" (see B8). [121] Wham was fined S$3,200 (US$2,300) for both offenses, but an appeal was ongoing as of July 2020. [122]

In a separate case involving Wham, he and opposition politician John Tan were convicted in October 2018 of contempt of court and sentenced to a fine of S$5,000 (US$3,700) each in April 2019. [123] The Attorney-General's Chambers initiated the proceedings in May 2018 against Wham, and later against Tan, marking the first such cases since the Administration of Justice (Protection) Act came into force. [124] Wham was accused of scandalizing the judiciary for a 2017 Facebook post claiming that Malaysian judges were more independent than their Singaporean

counterparts in cases with political implications. Tan was similarly accused of scandalizing the judiciary by writing on Facebook that the Attorney-General's Chambers decision to commence contempt of court proceedings against Wham "only confirms what he said was true." Both Wham's and Tan's appeals against their convictions were dismissed by the Court of Appeal. [125] In March 2020, Wham served a one-week term in jail in lieu of paying the S$5,000 fine. [126]

Singapore's criminal defamation law was used to punish online speech for the first time in decades during the previous coverage period. In December 2018, Terry Xu, chief editor of the *Online Citizen*, was charged with criminal defamation, as was Daniel De Costa, a reader who had written a letter published on the website about government corruption and "tampering of the Constitution" (see B2). [127] De Costa was also charged with unauthorized access to computer material for allegedly using another person's email account to submit the letter. [128] Xu faced a prison sentence of up to two years and a fine, while De Costa faced the same penalties as well as up to two years in prison and a fine of up to S$5,000 (US$3,700) for violating the Computer Misuse Act. [129] Their cases were ongoing at the end of the coverage period.

Authorities began another investigation into Wham in March 2019, for a photo he posted on social media in support of Xu and De Costa. [130] The police argued that Wham was protesting without a permit, though Wham asserted that he was not holding a solo protest in the photo. His mobile phone was confiscated as part of the investigation, [131] and he was required to seek permission from the police and the courts before traveling out of Singapore. The case remained pending at the end of the coverage period.

In another case involving the *Online Citizen*, in September 2019 Prime Minister Lee Hsien Loong sued Xu for defamation over an article that referenced claims made by Lee's estranged sister that he had misled their father, longtime prime minister Lee Kuan Yew, about the status of the family home. [132]

In November 2018, the Monetary Authority of Singapore filed a police report claiming that a *States Times Review* article alleging government corruption was false and had damaged the government's integrity (see B1 and B2). [133] During the same month, the prime minister sued financial adviser and government critic Leong Sze Hian for defamation after he shared the *States Times Review* article on Facebook. Lee described the action as "an attack against me personally as well as against the Singapore Government." Leong countersued the prime minister for abusing the court process, but this claim was dismissed by the High Court. Leong's appeal against that decision was dismissed in September 2019. [134] The case was still ongoing at the end of the coverage period.

Users were prosecuted for online activity amid the COVID-19 pandemic. In May 2020, taxi driver Kenneth Lai was sentenced to four months' imprisonment after he pleaded guilty to transmitting a false message under the Miscellaneous Offences (Public Order and Nuisance) Act. [135] Lai had published a post in a Facebook group communicating false information about the closure of food centers and supermarkets in Singapore, then removed it 15 minutes later after other members of the group urged him not to spread unverified rumors.

After the reporting period in July 2020, a police investigation was opened into Raeesah Khan, a parliamentary candidate for the opposition Workers' Party,

over two Facebook posts. One was published in May 2020, and another dated to 2018; both raised the issues of racial and ethnic discrimination in law enforcement and government policy. The investigation was opened under Section 298A of the penal code, which criminalizes acts that knowingly promote enmity between racial and religious groups. [136]

In June 2020, Li Shengwu, the nephew of Prime Minister Lee, was found guilty of contempt of court and fined S$15,000 (US$11,000). In 2017, the Attorney-General's Chambers had sought and was granted permission to begin the proceedings against Li. [137] His father, Lee Hsien Yang, had been involved in a public feud—largely conducted over social media—with his brother, the prime minister. Li had shared a *Wall Street Journal* article in a friends-only post on his Facebook page with the comment that the "Singapore government is very litigious and has a pliant court system," which the Attorney-General's Chambers described as an "egregious and baseless attack" on the judiciary. Proceedings were initiated after Li refused to retract his statement and apologize.

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**2**/4

While many people attempt to communicate anonymously online in Singapore, their ability to conceal their identities from the government is limited. Registration is required for some forms of digital interaction. Government-issued identity cards or passports must be produced when buying SIM cards, including prepaid cards, and buyers' personal details must be electronically recorded by vendors. Registration for the Wireless@SG public Wi-Fi network also

requires identity details.

The government does not restrict the use of encryption tools. However, the criminal procedure code allows authorities to require access to decryption information or technology if it is available. [138]

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**2**/6

Singapore has no constitutionally recognized right to privacy, and law enforcement authorities have broad powers to search electronic devices without judicial authorization, including while people are in custody (see C3). [139] The full extent of the government's surveillance capabilities and practices is unknown. However, according to the London-based organization Privacy International, "it is widely acknowledged that Singapore has a well-established, centrally controlled technological surveillance system" that includes internet monitoring. [140] According to one analyst, "few doubt that the state can get private data whenever it wants." The government justifies its surveillance regime on security grounds.

Privacy International notes that law enforcement agencies have sophisticated technological capabilities to monitor telephone and other digital communications. According to the group, surveillance is facilitated by the fact that "the legal framework regulating interception of communication falls short of applicable international human rights standards, and judicial authorization is sidelined and democratic oversight inexistent." [141]

A number of laws provide the government with access to users' personal information. For example, some members of

Parliament have expressed privacy concerns about the 2018 Cybersecurity Act, which allows authorized officers to take or make copies of hard disks as part of investigations or assessments of cybersecurity threats (see C8). [142]

Under the criminal procedure code, police officers investigating arrestable offenses may at any time access and search the data of any computer they suspect has been used in connection with the offense. [143] No warrant or special authorization is needed. The police have seized electronic devices in relation to a number of investigations in recent years, including those of Jolovan Wham, Terry Xu, and Daniel De Costa (see C3). [144] Penalties for noncompliance can include a fine of up to S$5,000 (US$3,700), six months in jail, or both. With authorization from the public prosecutor, police can also require individuals to hand over decryption codes. Failure to provide decryption information can result in fines of up to S$10,000 (US$7,300), jail terms of up to three months, or both.

According to information leaked by former US National Security Agency contractor Edward Snowden, SingTel has facilitated intelligence agencies' access to traffic carried on a major undersea telecommunications cable. [145]

Singapore has adopted concepts contained in the US Defense Department's Total Information Awareness program to gather electronic records en masse and search for evidence of impending security threats. The idea, which has proven controversial in the United States, has been incorporated into Singapore's Risk Assessment and Horizon Scanning program. According to one analyst, "Singapore has become a laboratory not only for testing how mass surveillance and big-data analysis might prevent terrorism, but for determining whether technology can be used to engineer a more harmonious society." [146]

As part of efforts to halt the spread of COVID-19, the government launched the TraceTogether app, which uses Bluetooth technology to identify and notify people who have been in close contact with infected individuals. [147] The government has made efforts to assure Singaporeans that the TraceTogether app respects user privacy. According to the official website, the information collected is the user's mobile number, identification details, and a random anonymized user identification code, stored in a secure server. [148]

However, in May 2020, the Ministry of Manpower announced that use of the TraceTogether app would be made mandatory for migrant workers living in dormitories or working in the construction, marine, and chemical processing sectors, raising significant concerns that migrant workers could be subjected to enhanced surveillance. [149]

Apart from TraceTogether, a contact tracing system known as SafeEntry has also been introduced, requiring individuals to scan a QR code and log their identification number and contact number before entering venues like malls and supermarkets. [150] For individuals who do not have smartphones, particularly older adults, the government has begun distributing Bluetooth-enabled dongles as alternatives to the TraceTogether app. [151]

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	**3**/6

In the absence of a constitutional right to privacy, service providers and technology companies can be required to hand information over to the government.

Website registration requirements, though imposed on only a small number of platforms, have raised concerns about unwarranted official intrusion into the sites' operations. For example, in December 2018, the IMDA asked the *Online Citizen*, which is supported by donations, to provide the Singaporean identity numbers of its donors in order to verify that it only receives financial support from Singaporean citizens. [152]

Government authorities can request metadata and content from international social media platforms and other tech companies when required for the investigation of offenses, the government has said. [153] The Personal Data Protection Act exempts public agencies and organizations acting on their behalf from compliance with its privacy safeguards. [154] Recent transparency reports from various social media and technology companies indicate the extent to which the government seeks access to Singaporean users' data. From July to December 2019, Facebook reported receiving 560 requests from the Singapore government for the details of 722 accounts. Facebook provided the data in 77 percent of the cases. [155] From January to June 2019, Google received 527 user data disclosure requests related to 1,174 Google accounts. Some data were provided in 84 percent of the cases. [156]

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	**3**/5

Internet users did not experience violence in retaliation for their online activities during the coverage period. However, due to the lack of protections for the expression of

unpopular or dissenting views, ICT users do not operate in an environment free of fear.

In April 2018, members of civil society criticized the Select Committee on Deliberate Online Falsehoods for breaching its own rules for public hearings. [157] Historian and New Naratif managing director Thum Pingtjin was questioned for six hours about his work and historical expertise after he argued that the government had itself spread "fake news" in the past when it detained people without trial. During her testimony, Kirsten Han, then the editor in chief of New Naratif, was questioned about an article she had written and warned that she had "not yet" been sued or jailed. Shortly after the hearings, the authorities rejected the application by New Naratif's parent entity to register a subsidiary in Singapore (see B6). In the select committee's September 2018 report, a section devoted to Thum claimed that he had lied about his academic credentials and therefore lacked credibility (see C1).

In September 2018, a PAP member of the select committee alleged on Facebook that Thum, Han, Jolovan Wham, and artist Sonny Liew had met with Malaysian prime minister Mahathir Mohamad and invited him to "bring democracy to Singapore." [158] His allegation was amplified by Facebook pages affiliated with the ruling party and some of its members, as well as the mainstream media. [159] The accusation triggered online trolling and harassment against the group.

In September 2019, Law Minister K. Shanmugam characterized Thum's and Han's actions as "nascent attempts" to bring foreign interference into Singapore and claimed that Han sought to use New Naratif as a platform to trigger protests similar to those in Hong Kong. He also singled out writers for the *Online Citizen* as possible

instigators of foreign interference. [160]

In May 2020, the anonymously run and pro-PAP *Global Times Singapore* Facebook page circulated the accusation that individuals who had written critical commentary on Singapore were part of a Chinese conspiracy to undermine the country. For example, journalism professor Cherian George and his wife Zuraidah Ibrahim, an editor at the Hong Kong–based *South China Morning Post*, were alleged to have recruited critics of Singapore's ruling party to write for the paper as part of a Chinese agenda to "put pressure on Singapore." [161] While such pages are known to take aim at activists and government critics, there is no clear evidence of their direct affiliation with the government or the ruling party.

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

Hacking and other forms of cyberattack have historically not been a widespread problem in Singapore. However, during the coverage period, Singapore was subjected to technical attacks and other privacy breaches.

In March 2020 an Indian cybersecurity company reported that credit card details issued by banks in Southeast Asia, including Singapore, had been leaked online. The company said that 25,290 credit card holders in Singapore had been affected. [162]

In March 2019 it was reported that the personal details of over 800,000 blood donors had been exposed for nine weeks after a vendor of the Health Sciences Authority

published the database on the internet. [163]

Prior to that, in October 2018, hackers stole the nonmedical personal data of 1.5 million patients, including the prime minister, from SingHealth, the country's largest group of health care providers; details about the medications of 160,000 patients were also taken. [164] In January 2019, a Committee of Inquiry reported that vulnerabilities in SingHealth's system and a lack of digital-security knowledge among staff contributed to the incident. [165] Although the government claimed to have acted against the perpetrators, it refused to provide details, citing national security concerns. [166] In March 2019, the cybersecurity company Symantec determined that a group known as Whitefly was responsible for the breach, and suggested that the group could be sponsored by a foreign state. [167]

Separately in January 2019, the government announced an online leak of the personal data of 14,200 people with HIV who either lived in Singapore or had visited the country. [168] The alleged perpetrator was a US citizen who had previously been incarcerated for fabricating his academic qualifications and his own HIV test in order to obtain an employment visa in Singapore. His partner had previously been the head of the Ministry of Health's National Public Health Unit and allegedly downloaded the registry.

The 2018 Cybersecurity Act requires owners of computer systems that deal with essential services pertaining to national security, public safety, or the economy to report cybersecurity incidents and conduct audits and risk assessments, among other obligations.

Footnotes

Be the first to know what's happening.

Join the Freedom House monthly newsletter

Email

Subscribe

ADDRESS

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

GENERAL INQUIRIES
info@freedomhouse

PRESS & MEDIA
press@freedomhou

@2020 FreedomHouse