

— [Our Issues](#) [Countries](#) [Policy Recommendations](#) [Explore the Map](#)

FREEDOM ON THE NET 2018

Singapore **59**
PARTLY FREE /100

A. <u>Obstacles to Access</u>	19/25
B. <u>Limits on Content</u>	21/35
C. <u>Violations of User Rights</u>	19/40

LAST YEAR'S SCORE & STATUS

59/100 **Partly Free**

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

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

- The Public Order and Safety Act, which went into effect in March 2018, drastically restricts online media and freedom of expression during “serious incidents” (see Legal Environment).



On Singapore

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

- The Parliament convened a Select Committee on Deliberate Online Falsehoods tasked with considering possible responses to the problem of “fake news” online (see Legal Environment).
- During public hearings, members of the Select Committee on Deliberate Online Falsehoods questioned and intimidated a historian and journalist about their writings relating to the government (see Intimidation and Violence).
- The 2016 Administration of Justice (Protection) Act, which codifies the offense of contempt of court, came into force in October 2017. Contempt of court is one of the most frequently applied legal restrictions on public debate in Singapore (see Legal Environment and Prosecutions and Detentions for Online Activities).

[See More >](#)

Country Facts

Global Freedom Score

50/100

Partly Free

Internet Freedom Score

54/100

Partly Free

In Other Reports

[Freedom in the World 2018](#)

Other Years

2020

Introduction

Singapore’s internet freedom environment was stable in 2018. The government continued to actively promote digital technologies while restricting their use for political dissent and for expression that could cause friction between ethnic or religious communities.

Singapore topped the World Economic Forum’s Networked Readiness Index global ranking in both 2015 and 2016. ¹

The internet remains the country’s most vital platform for alternative voices, as it is much more open than other media or public spaces. However, online and offline restrictions mean that the internet cannot foster any significant challenge to the political dominance of the ruling People’s Action Party (PAP).

The government has appeared less defensive about its free

speech restrictions in recent years. This is partly because of its strong performance in the 2015 general elections, which it took as evidence of public support for a governance model that prizes order over personal liberty. It has also been noticeably emboldened by the troubled politics of major democracies. Government officials and supporters have not only pointed to the rise of irrational populism, Britain’s Brexit referendum, and the election of Donald Trump as proof of the folly of too much democracy, but also used these developments to argue for more regulation, particularly in the case of “fake news.”

In January 2018, the government introduced a Green Paper by the Ministry of Communications and Information and the Ministry of Law entitled “Deliberate Online Falsehoods: Challenges and Implications,” which laid out the problems caused by the spread of online falsehoods as well as policy options for Singapore to consider in response. **2**

A new public order law that took effect in May 2018 expands police powers during “serious incidents,” such as terrorist attacks or acts “causing large-scale public disorder.” It allows the police commissioner to issue a communications stop order that would ban the making or exhibiting of relevant films and images and the communication of text or audio messages for the duration of the designated incidents. **3**

A. Obstacles to Access

As a wealthy and compact city-state, Singapore has highly developed information and communication technology (ICT) infrastructure. The government has 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.

Availability and Ease of Access

The internet penetration rate is high, as is the general quality of service. Some 91 percent of resident households had broadband internet access as of 2016. **4** Mobile data usage reached 15.78 petabytes in the final quarter of 2017—an increase of almost three petabytes from the year before.

5

The fiber-based Next Generation Nationwide Broadband Network (Next Gen 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. As of December 2017 there were over 3,900 [Wireless@SG](#) hotspots across the island. **6**

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

The government's current information-technology (IT) master plan, called Intelligent Nation, aims to integrate technologies more seamlessly and improve Singaporeans' skills in creating, as well as using, new technologies. 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**

The digital divide cuts mainly along generational lines. While 99 percent of residents aged 15 to 24 reported in 2015 that they had used the internet in the past three months, the rate was 30 percent for those aged 60 and older. **9** The government's Digital Inclusion Fund aims to make internet connectivity more accessible and affordable to older and lower-income Singaporeans. Under its Home Access

program, around 8,000 households will receive four years of fiber connectivity and a basic computing device for SGD 6 (US\$4) per month. **10**

The shutdown of the 2G mobile network in April 2017 raised concerns about the impact on people using older phones, particularly elderly Singaporeans and migrant workers. **11** Around 100,000 subscribers were still registered on 2G networks on the eve of the shutdown. **12**

Restrictions on Connectivity

No known restrictions have been placed on ICT connectivity, either permanently or during specific events. The Singapore Internet Exchange (SGIX), a not-for-profit 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 through international carriers, thus improving latency and resilience when there are cable outages on the international network. **13**

Singapore has adopted a National Broadband Network (NBN) structure, with the network built and operated by an entity that supplies telecommunications services on a wholesale-only, open-access, and nondiscriminatory basis to all telecommunications carriers and service providers. **14** To avoid conflicts of interest, separate companies have responsibility for passive infrastructure and active infrastructure such as routers, as well as for retail service provision downstream.

ICT Market

The dominant internet access providers are also the mobile telephone providers: SingTel, Starhub, and M1. SingTel, formerly a state telecom monopoly and now majority

owned by the government's investment arm, has a controlling stake in Starhub. The market is open to independent entrants. MyRepublic launched a broadband service in 2014. In October 2015, it started 4G trials to prepare for its bid for a telco (telephone company) license.

15 ViewQwest, another new player in the broadband market, was launched in 2015. **16** Circles.Life, the country's first fully digital telecommunications company, launched in 2016. **17** Zero Mobile, a new virtual mobile telco, launched at the end of 2017. **18**

Regulatory Bodies

The Infocommunications Media Development Authority (IMDA) develops and regulates the converging infocommunications and media sectors. **19** IMDA is not an independent public agency but a statutory body of the Ministry of Communications and Information (MCI), taking instruction from the cabinet.

B. Limits on Content

During the coverage period, there was no repetition of a 2015 order to shut down a website accused of inciting hatred against foreigners, the only known case of its kind to date. A licensing system introduced in 2013 has been used to limit the growth of independent online news start-ups by restricting their funding options. Despite such measures, the internet remains significantly more open than print or broadcasting as a medium for news and political discourse.

Blocking and Filtering

The government introduced internet content regulation in 1996 but promised that it would exercise its powers with a "light touch." As of 2018, it had apparently refrained from

blocking or filtering any political content.

The Broadcasting Act has included explicit internet regulations since 1996. Internet content providers and internet service providers (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.”

20

As a matter of policy, the IMDA blocks a list of 100 websites for the purpose of signposting 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. **21** Outside of this list, the Canada-based extramarital dating website Ashley Madison has been blocked since 2013, after it announced its plan to launch in Singapore. **22** No other site is known to have been singled out for blocking in this manner. 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. **23**

The Broadcasting Act empowers the MCI minister to prohibit disclosure of any directions to censor content. **24** This—together with the fact that most ISPs and large online media companies are close to the government—results in a lack of transparency and public accountability surrounding online content regulation.

Content Removal

Since the Class License system was introduced in 1996 (see Blocking and Filtering), it has been used once to ban a

politically sensitive site. In May 2015, the Media Development Authority (MDA)—since replaced by the IMDA—declared that the *Real Singapore* website had violated the Internet Code of Practice and that its Class License was therefore suspended. The regulator said several of the site’s articles had “sought to incite anti-foreigner sentiments in Singapore.” Some articles were “deliberately fabricated” and “falsely attributed.” The site was taken down soon after. **25**

The information minister said that this was only the 27th intervention against online content since 1996. Previous cases apparently involved takedown notices for specific content, but these were not made public. However, in 2013 the minister informed Parliament that most takedowns were for pornographic content or solicitation; others were related to gambling or drugs. He told lawmakers that the MDA had never directed websites to take down content “just because it is critical of the government.” **26**

A separate notice-and-takedown framework exists for high-impact online news sites—those receiving visits from a monthly average of at least 50,000 unique IP (internet protocol) 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 June 2013, the framework removes the identified 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 SGD 50,000 (US\$37,000) as an incentive to remain in compliance. **27** The bond is in line with the requirement for niche television broadcasters. **28**

Eleven news sites have been licensed under this framework.

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 cooperate with the government (see Media, Diversity, and Content Manipulation).

The only such outlets that do not belong to national mainstream media firms are Yahoo Singapore’s news site and an independent start-up, *Mothership*. After it was licensed, Yahoo’s reporters were granted the official accreditation that they had sought for several years. In 2015, *Mothership* became the first individually licensed site not belonging to a major corporation. ²⁹ It appears to have been designated purely because it had crossed the regulatory threshold of 50,000 visitors a month. Although it is popular for its irreverent commentary, *Mothership* is considered moderate and not antiestablishment.

Apart from the IMDA’s notice-and-takedown framework, critical content may be removed by bloggers under threat of criminal prosecution or defamation suits (see Prosecutions and Detentions for Online Activities). In March 2017, the Attorney-General’s Chambers told activist-blogger Han Hui Hui that she would be charged with contempt of court unless she removed a YouTube video and five Facebook posts alleging that judges were persecuting her for political reasons. She took down the offending statements and apologized. ³⁰

Government officials are also known to demand retractions or apologies for comments on social media that they take issue with. In February 2018, a Facebook user who had posted a spoof of a Chinese newspaper’s front page apologized for his actions after the Attorney-General’s Chambers indicated that they were examining the spoofed image as a potential case of contempt of court. ³¹ The offending content was removed. ³²

Media, Diversity, and Content Manipulation

The online landscape is significantly more diverse than offline media. YouTube, Facebook, Twitter, and international blog-hosting services are freely available, and most bloggers operate openly. All major opposition parties and many nongovernmental organizations (NGOs) are active online. However, independent and opposition-oriented online news outlets are too small and weak to redress the imbalance in Singapore's media environment, which continues to be dominated by the PAP establishment.

The biggest online news players, in terms of resources and viewership, are the internet platforms 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 September 2017. **33** 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. **34** Both companies' websites are subject to the notice-and-takedown framework (see Content Removal), but the main avenue of control is the routine self-censorship that also afflicts their parent news organizations.

Online-only news outlets struggled to remain financially viable in 2017 and 2018. The *Middle Ground*, considered a more politically middle-of-the-road website, announced in October 2017 that it was winding down its operations, citing financial difficulties. **35** Its demise follows those of other independent sociopolitical projects, such as *Inconvenient Questions* and *SIX-SIX*, both of which shut down due to a

lack of financial resources in 2016. **36**

Meanwhile, the *Online Citizen* and the *Independent*, two sites known for critical commentary, have never had the capacity to generate original daily news or regular investigative features. **37** These sites come under special IMDA registration rules that prohibit foreign funding and require the sites to provide details about funding sources.

38 In effect, this shuts out grants and loans from foreign foundations, which have been essential for most independent political sites in the region.

In April 2018, the Accounting and Corporate Regulatory Authority publicly declined to register a Singapore subsidiary of the British company that publishes *New Naratif*, a website founded by Singaporeans. In its statement, the authorities said that it would be “contrary to Singapore’s national interests” to allow registration, pointing to the political purposes of the company and its work, such as “publishing articles critical of politics in regional countries” and organizing democracy classrooms. **39**

So far, *Mothership* appears to be sustaining itself financially, though some of its sponsored content has been suspected of being paid for by the government. The site identifies its sponsored posts without naming the sponsor. 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. **40** Reinforcing the trend is the proliferation of social media, which seems to have encouraged a previously silent mainstream population to air their views more readily.

Furthermore, especially since the 2011 general elections, individual ministers and government agencies have ramped up and professionalized their social media capacity. 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. **41**

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. **42**

Analysts described some possible content manipulation around the 2015 general elections, when online rumors in the form of bookies’ odds gave detailed predictions of opposition victories in several constituencies. Since election laws ban opinion polling, these underground predictions were the only quantitative indicators of likely outcomes available to voters. Several versions were circulated widely via WhatsApp within the nine-day campaign period. The messages, pointing to an impending opposition landslide, may have spooked some swing voters and caused them to vote more conservatively. **43** The case illustrates how political operatives might be able to manipulate voter sentiment in an environment where high-quality information is limited by regulatory constraints. Bloggers have pointed out some (largely progovernment) online commentators who hide behind anonymous profiles; these accounts are often referred to as members of the “Internet Brigade,” or IBs. **44** However, there is no concrete evidence of large-scale covert deployment of paid online commentators.

Digital Activism

The internet is regularly used for popular mobilization by groups from across the political spectrum. The success of these efforts is constrained less by online regulation than by offline restrictions on fund-raising and public assembly. There is only one location—a small downtown park

designated as a Speakers' Corner—where Singaporeans can gather without a police permit.

In May 2017, the organizers of Singapore's largest LGBT (lesbian, gay, bisexual, and transgender) pride rally, Pink Dot, announced that barricades would be erected around Speakers' Corner during their event, in compliance with new regulations introduced by the government that ban the presence of foreigners at cause-related assemblies in the park. ⁴⁵ The requirements were criticized by Singaporeans online; some declared that they would attend the event out of principle. ⁴⁶ Pink Dot took place on July 1, 2017, filling the park to maximum capacity with only Singaporeans and permanent residents. ⁴⁷

C. Violations of User Rights

Self-censorship in online discourse is mainly due to fear of postpublication punitive action—especially through strict laws on defamation, racial and religious insult, and contempt of court. While citizens remain free from major human rights abuses and enjoy high levels of personal security in Singapore, the government places a premium on order and stability at the expense of civil liberties and political dissent. The authorities are believed to exercise broad legal powers to obtain personal data for surveillance purposes in national security investigations.

Legal Environment

The republic's constitution enshrines freedom of expression, but it also grants Parliament leeway to impose limits on that freedom. ⁴⁸ As the ruling party controls over 80 percent of the seats in the legislature, the laws it passes tend to be

short on checks and balances.

Several legislative initiatives that were pursued over the past year have the potential to negatively affect internet freedom in Singapore.

In January 2018, Parliament voted unanimously to convene a Select Committee on Deliberate Online Falsehoods tasked with considering possible responses to the problem of “fake news” online. **49** Although the Select Committee’s terms of reference stated that it would look into a variety of options, new legislation seemed likely. The law minister had remarked in 2017 that new laws on “fake news” would be introduced. **50** The government’s definition of false news appears to be fairly broad: In October 2017 the MCI accused Reuters of running a fabricated headline, as it disputed the news agency’s interpretation of a comment made by a government minister. **51**

The Cybersecurity Act was passed by Parliament in February 2018 and came into force the following month. The law 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. The bill also allows authorized officers to take or make copies of hard disks as part of investigations or assessments of cybersecurity threats, prompting some members of Parliament to express concerns about privacy.

52

Parliament passed the Public Order and Safety (Special Powers) Act in March 2018, and the measure took effect in May. It gives the authorities the power to ban communications—such as recording or distributing videos or images, or sending text or audio messages—during a period of special authorization in the event of a “serious

incident.” The definition of “serious incident” encompasses terrorist attacks as well as peaceful protests like large sit-down demonstrations. **53** Being found guilty of violating this ban results in punishment of up to two years in prison and a fine of SGD 20,000 (US\$15,200). **54** This new law gravely restricts online media and freedom of expression, impeding reporting and the dissemination of information once the government deems a situation a “serious incident.”

In August 2016, Parliament passed a new statute codifying the offense of contempt of court. **55** The Administration of Justice (Protection) Act, which officially came into force in October 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” and “poses a risk that public confidence in the administration of justice would be undermined.” This lowers the previous threshold of a “real risk” of harm to the administration of justice. The act also allows the attorney general, with leave from the High Court, 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 new act is three years in prison and a fine of SGD 100,000 (US\$75,000), a harsher punishment than judges had previously imposed. **56**

Contempt of court was already one of the most frequently applied legal restrictions on public debate in Singapore, invoked against bloggers who wrote about such issues as discrimination against LGBTI people and the treatment of opposition politicians in the courts. **57** Critics had been calling for Singapore’s contempt laws to be liberalized in line with other Commonwealth jurisdictions, but the new law was passed with 72 votes to 9, with members of the opposition Workers’ Party voting against.

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 fill in the details through vaguely articulated subsidiary regulations, such as website licensing and registration rules (see Content Removal and Media, Diversity, and Content Manipulation). Other laws that have been used to restrict online communication, such as the Seditious Act and the Political Donations Act, are open to broad interpretation by the authorities.

The Seditious 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,” among other things.

58 Punishments for first-time offenders can include a prison term of up to three years. Newer provisions in the penal code (Section 298) provide 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.” **59** In Singapore’s first cases of imprisonment for online speech in 2005, the defendants were punished under the Seditious Act for posts that insulted Muslims. **60** Police appear to regularly investigate complaints of insult and offense. 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, but to date, no charges have been brought under this law to punish online speech. **61** Civil defamation suits remain a powerful deterrent. PAP leaders have been awarded damages in the range of SGD 100,000 to 300,000 each (US\$75,000 to 224,000) in defamation suits brought against opposition politicians and foreign media corporations. **62** In March

2016, for example, blogger Roy Ngerng reached a settlement in a 2014 lawsuit that called for him to pay Prime Minister Lee Hsien Loong damages of SGD 150,000 (US\$112,000) in installments; he was expected to complete the payments in 2033. ⁶³

Under the 2014 Protection from Harassment Act, a person who uses “threatening, abusive, or insulting” expression likely to cause “harassment, alarm, or distress” can be fined up to SGD 5,000 (US\$3,700). ⁶⁴ Victims can also apply to the court for a protection order, which could include a ban on continued publication of the offending communication. The government inserted into the law a section providing 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 set the record straight.

The government quickly attempted to use the law against its critics: The Ministry of Defence applied for a court order against an article published in the *Online Citizen*. However, although a district court initially granted the order, it was overturned by the High Court in December 2015. The court ruled that government departments could not be considered a “person” under the act and therefore could not apply for protection from harassment. ⁶⁵ In January 2017, the Court of Appeal, the country’s apex court, dismissed the Ministry of Defence’s appeal with costs. ⁶⁶

Prosecutions and Detentions for Online Activities

A few individuals were charged for using the internet for social or political activities during this report’s coverage period, though there were no new convictions leading to prison sentences.

In November 2017, activist Jolovan Wham was charged with organizing public assemblies without a permit, vandalism, and refusing to sign statements to the police. **67** One of the assemblies in question was an indoor forum in which Hong Kong prodemocracy activist Joshua Wong participated as a speaker via Skype. The authorities argued that because Wong is a foreign speaker, a permit should have been obtained for the event. **68** Those convicted of organizing public assemblies without a permit can be fined up to SGD 5,000 (US\$3,700); repeat offenders can be fined up to SGD 10,000 (US\$7,500) and imprisoned for up to six months. Although the vandalism law provides for a fine of up to SGD 2,000 (US\$1,500) or up to three years' imprisonment with three to eight strokes of the cane, first-time offenders who use nonpermanent substances will not be caned.

The Attorney-General's Chambers sought in May 2018 leave to commence contempt of court proceedings against Wham and opposition politician John Tan—the first since the Administration of Justice (Protection) Act came into force. **69** Wham was accused of scandalizing the judiciary by posting a link to a news article on a constitutional challenge in Malaysia on Facebook with a comment 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.”

In August 2017, the Attorney-General's Chambers sought and was granted permission to begin contempt of court proceedings against Li Shengwu, the nephew of Prime Minister Lee Hsien Loong. **70** Li's 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.

The authorities have been targeting internet users for online activities more aggressively in the past few years. In 2015, teenage blogger Amos Yee was sentenced to four weeks in jail. He was found guilty of wounding Christians’ feelings under Section 298 of the penal code through an expletive-ridden video that likened the adulation of the late Singaporean leader Lee Kuan Yew to Christians’ worship of Jesus. He was also found guilty of transmitting an obscene image under Section 292 of the penal code. Referencing a comment by the late British prime minister Margaret Thatcher that Lee was usually right, Yee had posted a manipulated image depicting the two politicians having sex.

71

Following his release, Yee continued with his online commentary, including on religious themes. Again falling foul of Section 298, he pleaded guilty in September 2016 to six counts of posting videos and blogs that were derogatory of Christianity and Islam. He was sentenced to six weeks in jail.

Yee fled to the United States in December 2016 and was granted political asylum by a Chicago judge in March 2017. The US Department of Homeland Security appealed the decision, but it was ultimately upheld. **72** Human Rights Watch, supporting the asylum bid, said that Yee was being persecuted for his political opinions, which never amounted to advocacy of violence. **73** It also noted that Singapore had

tried Yee as an adult even though under international human rights law he was still a child at the time of his trials. **74**

In a separate case in June 2016, the owner of the *Real Singapore* website (see Content Removal), Yang Kaiheng, was sentenced to eight months in jail for posts that violated the Sedition Act. **75** His wife, Australian national Ai Takagi, had been sentenced to 10 months in jail in March. They were accused of using the site to exploit racial and xenophobic tensions in Singaporean society through posts that criticized foreigners from the Philippines, India, and China. The prosecution said that the couple had invented sensational stories in order to attract readers and advertising revenue.

76

Actions have also been taken against internet users in connection with election law violations. In August 2016, the police served the *Middle Ground* with a “stern warning” in lieu of prosecution for publishing an article on its street poll of 50 voters ahead of a May 2016 by-election. **77** The site had already complied with an order to take down the article.

78 The Parliamentary Elections Act prohibits the publication of election surveys during the official campaign period.

The election law also prohibits campaigning on polling day and the day before (“cooling-off day”). The offense is defined broadly to cover commentary, including by individuals and groups with no party affiliations. In February 2017, police issued stern warnings to four individuals for breaching this rule. One was the founder of the pro-PAP Facebook page “Fabrications About the PAP,” while the other three were associated with the *Independent*, which has no formal party links. **79** Two prominent activists, Roy Ngerng and Teo Soh Lung, were also investigated for breaches of cooling-off day rules; their phones and computers were confiscated (see Surveillance, Privacy, and

Anonymity). **80** In contrast, the authorities do not appear to have investigated suspicious “fake news” that may have affected the 2015 general elections result (see Media, Diversity, and Content Manipulation).

Surveillance, Privacy, and Anonymity

Singapore has no constitutionally recognized right to privacy, and law enforcement authorities have broad powers to conduct searches on computers without judicial authorization. **81** While many people try 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’ details must be electronically recorded by vendors. Registration for the [Wireless@SG](#) public Wi-Fi network also requires identity details.

The full extent of Singapore’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. **82** 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. “Whether by compulsion or natural tendency, most Singaporeans appear to be relatively sympathetic to this rationale and do not protest the government’s collection, monitoring, or even transfer abroad of data about them,” a recent study found. **83**

Privacy International notes that law enforcement agencies have sophisticated technological capabilities to monitor telephone and other digital communications. Surveillance is

also 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 nonexistent.” **84**

Under the sweeping Computer Misuse and Cybersecurity Act, the minister for home affairs can authorize the collection of information from any computer, including in real time, when satisfied that it is necessary to address any threat to national security. **85** Court permission is not required. Failure to comply with collection orders is punishable with a fine of up to SGD 50,000 (US\$37,000), a prison term of up to 10 years, or both.

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. **86** No warrant or special authorization is needed. Penalties for noncompliance can include a fine of up to SGD 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, failing which they are subject to fines of up to SGD 10,000 (US\$7,500), jail terms of up to three months, or both.

In mid-2016, police seized devices belonging to lawyer Teo Soh Lung from her home without a warrant after questioning her in relation to a Facebook post made prior to a May by-election. The police claimed that Teo’s post violated restrictions on political advertising in the Parliamentary Elections Act, which bars campaigning and election advertising from the day before polling (see Prosecutions and Detentions for Online Activities). **87**

Website registration requirements, though imposed on only

a small number of platforms, have raised concerns about unwarranted official intrusion into the sites' operations (see Media, Diversity, and Content Manipulation). In 2013, the owner of one site, the *Breakfast Network*, declined to register because the MDA required the names of anyone involved in the "provision, management and/or operation of the website," including volunteers. **88**

Responding to a parliamentary question, the government said in 2013 that, as part of the evidence gathering process, law enforcement agencies made around 600 information requests a year to Google, Facebook, and Microsoft between 2010 and 2012. Most were for Computer Misuse and Cybersecurity Act offenses, while the rest were for crimes related to corruption, terrorist threats, gambling, and vice. Although all requests were for metadata, agencies can request content data if it is required for investigating offenses, the government said. **89** The Personal Data Protection Act exempts public agencies and organizations acting on their behalf. **90**

Recent transparency reports from various communications platforms indicate the extent to which the government seeks access to Singaporean users' data. From January to June 2017, Facebook reported receiving 204 requests for the details of 263 accounts from the Singapore government. Facebook provided data in 59 percent of the cases. **91** From January to June 2017, Google received 230 user data disclosure requests relating to 311 Google accounts. **92**

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. **93**

Singapore has adopted a US Defense Department concept, "Total Information Awareness," to gather electronic records

en masse and look 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." **94**

Intimidation and Violence

There were no violent incidents targeting internet users in the past year. However, the lack of protections for the expression of unpopular or dissenting views means that ICT users cannot be said to operate in an environment free of fear.

Donald Low, associate dean of the Lee Kuan Yew School of Public Policy, was required to retract comments and apologize twice to the law minister on Facebook in 2017 after the minister said that one of Low's posts had "seriously misconstrued" a comment he had made during an interview.

95

In April 2018, members of civil society criticized the way the Select Committee on Deliberate Online Falsehoods held its public hearings, accusing the committee of not adhering to its own terms of reference. **96** Historian Thum Pingtjin was questioned for six hours about his work and expertise on Singapore history in response to a claim he made in his submission that the government had itself been guilty of spreading "fake news" when it carried out detentions without trial. During her session, journalist Kirsten Han was questioned about an article she had written in an exchange that ended with a committee member telling her that she had "not yet" been sued or jailed.

Thum and Han are the managing director and editor in chief, respectively, of *New Naratif*. Shortly after the Select Committee sessions, the authorities rejected an application by *New Naratif's* parent company to register a subsidiary in Singapore (see Media, Diversity, and Content Manipulation).

Technical Attacks

Hacking of public-sector websites in past years has prompted the government to strengthen safeguards against technical attacks. A Cyber Security Agency (CSA) was established in 2015 to mitigate attacks and protect critical sectors such as energy, water, and banking. In 2017, the Ministry of Defence announced that it would deploy conscripts to the CSA and its military equivalent as part of a long-term plan to train cybersecurity personnel. **97** Singapore has compulsory national service for all males. In 2017 the government implemented an Internet Surfing Separation policy for public-service officers to insulate its systems from attacks via the public internet. **98**

In April 2017, Parliament approved the addition of new cybersecurity provisions to the Computer Misuse and Cybersecurity Act. **99** The amendments make it an offense for a person to use or trade illegally obtained data even if they were not involved in the technical attack through which the information was obtained. Separately, the Cybersecurity Act was passed in Parliament in February 2018 and came into force in March (see Legal Environment).

Footnotes

- 1** World Economic Forum, “Singapore,” in Global Information Technology Report 2016, <http://reports.weforum.org/global-information-technology-report-2016/ec...>
- 2** “Deliberate Online Falsehoods: Challenges and Implications,” January 5, 2018, <https://www.mlaw.gov.sg/content/dam/minlaw>

/corp/News/Annexe%20A%20-%20G...

“Public Order and Safety (Special Powers) Bill,” February 27, 2018, <https://www.parliament.gov.sg/docs/default-source/default-document-libr...>

Be the first to know what's happening.

Infocomm Media Development Authority of Singapore,

<https://www.imda.gov.sg/industry-development/facts-and-figures/infocomm...>

Infocomm Media Development Authority of Singapore,

<https://www.imda.gov.sg/industry-development/facts-and-figures/telecomm...>

Join the Freedom House

monthly newsletter
More footnotes

Email

Subscribe

ADDRESS

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

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org

@2020 FreedomHouse