

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

FREEDOM ON THE NET 2018

South Korea

PARTLY FREE

64
/100

A. <u>Obstacles to Access</u>	22 /25
B. <u>Limits on Content</u>	22 /35
C. <u>Violations of User Rights</u>	20 /40

LAST YEAR'S SCORE & STATUS

65 /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

- Women were increasingly targeted for supporting feminist causes on social media and subjected to gender-based harassment and discrimination online (see Intimidation and Violence).



On South
Korea

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

- The Seoul High Court upheld a 2017 Seoul Administrative Court ruling that the Korea Communications Standards Commission's decision to block *North Korea Tech* was unlawful (see [Blocking and Filtering](#)).
- An internet user and a journalist were sentenced to one year and 14 months, respectively, under the National Security Act for publishing North Korea-related online content (see [Prosecutions and Detentions for Online Activity](#)).
- In August 2017, the High Court sentenced the former director of the National Intelligence Service to four years in prison for election interference, including manipulating online posts, in the run-up to the 2012 election (see [Media, Diversity, and Content Manipulation](#)).

[See More >](#)

Country Facts

Global Freedom Score

83/100

Free

Internet Freedom Score

66/100

Partly Free

In Other Reports

[Freedom in the World 2018](#)

Other Years

2020

Introduction

Internet freedom declined in South Korea during the reporting period due to the troubling trend of women being targeted and punished for their online support of feminist campaigns and messages.

On May 10, 2017, a new liberal government came into power. In response to popular pressure, much of which was digitally mediated mobilization, the National Assembly voted on December 9, 2016, to impeach the eighteenth president Park Geun-hye for alleged corruption and for violating the constitution. On March 10, 2017, the Constitutional Court unanimously upheld the vote. On May 9, Moon Jae-in, a former human rights lawyer and the leader of the left-of-center Democratic Party, was elected to be the new president. Park, who maintains her innocence, is currently

serving a 33-year sentence. **1** Park's predecessor Lee Myung-bak was also arrested on March 22, 2018, on charges of bribery, embezzlement, and tax evasion. **2**

These extraordinary developments showcased, on the one hand, Korean citizens' innovative and effective use of physical and digital resources to exercise their political rights. **3** On the other hand, investigations resulting from the scandal around Park Geun-hye and her entourage revealed the extent to which freedom of expression had been eroded under conservative rule since 2008.

In 2017, an internal National Intelligence Service (NIS) inquiry admitted that the NIS—an agency prohibited from interfering with domestic politics—had manipulated online content to ensure another conservative would succeed outgoing President Lee Myung-bak. Intelligence agents and hired civilians were tasked with spreading pro-government opinions and suppressing anti-government views online. **4**

Former President Park was also criticized for crackdowns on dissent during her unfinished term. **5** In the midst of the 2016 presidential scandal, it was discovered that her administration as well as her predecessor Lee had compiled a blacklist of almost 10,000 artists, writers, and other cultural practitioners who were considered critical of the conservatives or supportive of the liberal opposition. **6** Further revelations made during the coverage period highlighted that online information and discussions had been distorted by various entities besides the central government.

A. Obstacles to Access

South Korea boasts one of the world's highest broadband and smartphone penetration rates. The internet service

sector is relatively diverse and open to competition, while the mobile market is subject to more state influence. Broadcasting and telecommunications activities are regulated by the Korea Communications Commission (KCC) and the content and ethical standards of such activities are monitored by the Korea Communications Standards Commission (KCSC).

Availability and Ease of Access

South Korea is one of the most wired countries in the world, for both use and connection speed. **7** Smartphone penetration was at 88 percent in 2015, surpassing other advanced economies in global surveys. **8** Taking connected mobile phones, televisions, and game consoles into consideration, an estimated 97 percent of households had internet access by 2012. **9**

Several factors have contributed to the country's high degree of connectivity. High-speed internet is relatively affordable, and roughly 70 percent of South Koreans live in cities dominated by multi-story apartment buildings that can easily be connected to fiber-optic cables. **10** The government has also implemented a series of programs to expand internet access since the 1990s, including subsidies for low-income communities. **11**

Omnipresent and affordable *PC bang* (“computer rooms”) offer broadband access for approximately US\$1 per hour and serve as venues for social interaction and online gaming. Free Wi-Fi is offered in over 12,000 public spaces across the country, as of October 2016, including train stations, airports, libraries, health centers, and community centers.

12

There is no significant digital divide with respect to gender or income, although differences persist along generational

and professional lines. **13**

Restrictions on Connectivity

The country's internet backbone market is oligarchic, with Korea Telecom (KT) as the biggest provider. KT was founded in 1981 and remained state-owned until privatization in 2002. The network infrastructure is connected to the international internet predominantly from the southern cities of Busan and Keoje, through international submarine cables connecting to Japan and China. For national security reasons, the police and the NIS have oversight of the access points, but the government is not known to implement politically motivated restrictions on internet or mobile access. **14**

ICT Market

The telecommunications sector in South Korea is relatively diverse and open to competition, with 94 internet service providers (ISPs) operating as of January 2018. **15**

Nevertheless, it is dominated by three companies: Korea Telecom (41.3 percent), SK Telecom (25.6 percent), and LG Telecom (18 percent). The same firms also control the country's mobile service market, with 28.4 percent, 36.9 percent, and 22.4 percent market share, respectively. **16** All three companies are publicly traded, but they are part of the country's *chaebols*—large, family-controlled conglomerates connected to the political elite, often by marriage ties. **17** This has given rise to speculation that favoritism was at play in the privatization process and in the selection of bidders for mobile phone licenses. **18**

Korea Mobile Internet (KMI), a consortium of mobile virtual network operators who rent capacity from the main players, made a sixth attempt to enter the market in 2014. The then Ministry of Science, ICT and Future Planning (MSIP) rejected

the consortium's bid for a license for failing to meet financial requirements, which KMI described as "excessively strict." ¹⁹ Media reports say previously unsuccessful bidders, namely K Mobile (founded by a former KMI executive), Sejong Telecom, and Quantum Mobile, intend to re-apply under the new government. Cable TV companies are also reported to have expressed interest.

With the stated aim of easing the information asymmetry caused by the effective oligopoly of the mobile phone market, the Mobile Device Distribution Improvement Act came into effect in October 2014 limiting service carriers' subsidies for consumers. However, it ended up hiking up the prices of mobile handsets and subscriptions, leading to a public furor. ²⁰ While the Act remains in force, the subsidy cap was lifted in October 2017. ²¹

Regulatory Bodies

The Korea Communications Commission (KCC), which is responsible to the president, regulates the telecommunications and broadcast sectors. ²² The conservative Lee Myung-bak government, which was in power from February 2008 to February 2013, created the five-member KCC in 2008. ²³ The president appoints two commissioners, including the chair, while the National Assembly chooses the remainder. Since August 2017, the chairman has been Lee Hyo-seong. ²⁴

Politicized appointments have marred the credibility of the commission. The first KCC chairman, Choi See-joong, was a close associate of then President Lee. ²⁵ Choi resigned in 2012 amid bribery scandals, and was later sentenced to two and a half years in prison and a fine of KRW 600 million (US\$540,000) for influence peddling. ²⁶ Lee pardoned him just before the end of his presidential term. ²⁷ In 2013, then President Park Geun-hye named a close aide, four-term

lawmaker Lee Kyeong-jae, to head the KCC. ²⁸ He was succeeded by a former judge, Choi Sung-joon, who completed his term on April 7, 2017. After an internal audit following Park's impeachment, the KCC is reportedly planning to request a prosecutorial investigation into former chief Choi Sung-joon's alleged preferential treatment of LG mobile operator. ²⁹

B. Limits on Content

Although South Korean cyberspace is vibrant and creative, there are a number of restrictions on the free circulation of information and opinions. Technical filtering and administrative deletion of content are particularly evident. Content that “praises or benefits” North Korea or undermines the traditional social values of the country is blocked or deleted. Systematic manipulation of online discussions was documented in the past, with several new revelations in the coverage period indicating that the scope was broader than first imagined.

Blocking and Filtering

Service providers continued blocking content deemed to violate the law or social norms, including threats to national security and public morality, mainly on the orders of the KCSC. ³⁰

The KCSC has occasionally responded to pressure to reverse censorship orders, however. In April 2016, British journalist Martyn Williams legally disputed the KCSC's blocking of his website *North Korea Tech*. A year later, on April 21, 2017, the Seoul Administrative Court ruled that the blocking order was unlawful. ³¹ The ruling was upheld in the Seoul High Court on October 18, 2017. ³²

Founded in February 2008, around the same time as the

establishment of the KCC, the KCSC monitors internet content and issues censorship orders to content hosts and other service providers. Noncompliant service providers face up to two years of imprisonment or a fine of up to KRW 20 million (US\$18,000), according to Article 73 of the Information and Communications Network Act.

The KCSC's nine members are appointed by the president and the National Assembly. **33** Park Hyo-chong, a key figure in the country's neoconservative movement, led an all-male commission from June 2014 to June 2017. Former journalism professor Kang Sang-Hyun chairs the current commission, which was formed in January 2018.

The commissioners meet every two weeks to deliberate, according to a former commissioner. **34** The KCSC evaluates online content flagged by a team of in-house monitoring officers, but also considers censorship requests from other agencies and individuals. Observers criticize the KCSC's vaguely defined standards and wide discretionary power to determine what information should be censored, which allow the small number of commissioners to make politically, socially, and culturally biased judgments, often lacking legal grounds. **35** Also, in many cases, the commission blocks entire sites even though only a small portion of posts are considered to be problematic. In 2017, 66,659 websites or pages were blocked and 15,499 deleted, marking a decrease in the number of websites blocked for the first time since the commission's establishment in 2008.

36

The KCSC does not publish a list of blocked sites, but it does release the number of websites blocked under different categories of banned content, including “gambling,” “illegitimate food and medicine,” “obscenity,” “violation of others' rights,” and “violation of other laws and regulations.” The last category includes websites containing what is

deemed to be North Korean propaganda, based on Article 7 of the 1948 National Security Act, which bans content that “praises, promotes, and glorifies North Korea.” **37** Besides the KCSC’s usual monitoring, an increasing number of requests were initiated by the NIS and the police, from 700 in 2013 (two from NIS and 698 from police) to 1,996 between January and August 2016 (209 from NIS and 1,787 from police).

A legal amendment to Article 25(2) to the Act of the Establishment and Operation of the Korea Communications Commission was passed on December 29, 2014, to mandate notifying owners of censored content. **38** Affected users are allowed to challenge the commission’s ruling in principle, but with no independent avenue for appeal available. **39**

Content Removal

In addition to blocking, some political and social content is subject to removal by service providers based on instructions from the KCSC as well as from complaints from individuals, the police, and other government agencies. On receiving a takedown request from individual users, the company must hide the content in question for 30 days **40** and delete it if the content owner does not revise it or appeal within that time. According to the *Associated Press*, “hundreds of thousands of online posts get deleted every year by such temporary removal requests, which in effect lead the posts to be deleted permanently.” **41**

Restrictions on political speech surrounding elections are more stringent in South Korea than in many democracies due to limits prescribed in the 1994 Public Official Election Act. In 2011, a ban on posting election-related commentary online in the days before the polls was declared unconstitutional. However, content posted about candidates is still closely monitored by the National Election

Commission (NEC). According to the latest Korea Internet Transparency Report, the NEC and its regional branches had 17,101 online posts deleted in the lead-up to the National Assembly election in April 2016. The most frequent reasons were for “unauthorized displays of opinion poll results” (46.2 percent), “distribution of false information” (27.04 percent), and “slander against candidates” (17.64 percent). **42**

The number of deletions increased to at least 31,004 surrounding the May 2017 presidential election. 20,104 posts were deleted for containing false information, more popularly dubbed “fake news.” Naver BAND, a home-grown group communication app, received the most deletion orders (8,115), followed by Facebook (7,361) and Twitter (6,842). **43**

Separately, an audit of the country’s two largest web portals, Naver and Daum, revealed the existence of internal regulations authorizing staff to alter their real-time lists of popular search terms as per requests from government or official agencies. The portals operate search engines, blog platforms, and news aggregators, among other internet services. In the past, both companies maintained that the trending search terms were selected automatically by an algorithm. The Korea Internet Self-governance Organization (KISO), an industry group of major internet firms, of which Naver and Daum are members, conducted the audit at Naver’s request to investigate allegations that companies were complicit in the content manipulation scandal surrounding the 2012 presidential election (see Media, Diversity, and Content Manipulation).

The KISO report, published in December 2016, shows that Naver routinely removes search terms from its public list without oversight, some based on requests from users, companies, and educational institutions, and some without a clear reason. Naver removed 1,408 popular search terms

from the real-time rankings between January and May 2016, amounting to an average of nine per day. **44** Naver said that this enabled the company to comply with requests from law enforcement, such as keeping the names of criminal suspects off the list. However, observers claimed that the lack of transparency over the process, coupled with the fact that the companies had agreed to allow political influence over content that affects the public's perception during an election year, were cause for concern.

Companies are also known to proactively delete user-generated content that they judge to potentially violate the law, even without being prompted by a complaint, to avoid legal liability. Under Article 44(3) of the Information and Communications Network Act, intermediaries are encouraged to monitor and carry out proactive 30-day takedowns of problematic content. **45** Companies that can demonstrate proactive efforts to regulate content would be favorably considered by the courts, while those that do not may be liable for illegal content posted on their platforms.

46

Article 17 of the Children and Youth Protection Act places responsibility for removing child pornography on online service providers, with possible penalties of up to three years of imprisonment or fines of up to KRW 20 million (US\$18,000). In 2015, the then CEO of KakaoTalk, the country's most popular mobile messaging application, was charged under this Article because underage users had shared explicit images of themselves on the service. Since holding a CEO personally liable for user activity was unprecedented in South Korea, critics alleged that this charge was punishment for "refusing to curb users' opinions critical of the government." **47** In June 2018, the Constitutional Court upheld the Article, stating that it is within the online service providers' legal obligation to

prevent the circulation of child or juvenile pornography. **48**

The legal grounds for takedown requests have expanded in recent years. An antiterrorism law passed in March 2016 granted the NIS the power to order the removal of any online content during terrorism investigations (see Surveillance, Privacy, and Anonymity). The KCSC separately amended its regulations in December 2015 to accept takedown requests from third parties based on perceived defamation of other people, despite opposition from civil society groups. **49**

Media, Diversity, and Content Manipulation

Onerous registration requirements for online news agencies were struck down during the previous reporting period, although online media freedom may be restricted by emerging attempts to curb “fake news.” Revelations continued to unfold about the extent of the manipulation scandal surrounding the two former conservative governments.

South Korea’s overall media environment is partly restricted, **50** and activist media outlets have developed online in part to challenge those restrictions. **51** *Newstapa*, a user-funded investigative journalism platform, has accumulated more than 40,000 regular donors and 74 million views on its YouTube channel since it launched in 2012. **52** It was a leading source of information on the election manipulation scandal in 2013, **53** and one of the first to allege systemic corruption and negligence behind the sinking of Ferry Sewol in 2014, a disaster that resulted in 304 deaths.

Former President Park Geun-hye’s administration was overshadowed by an investigation into the politicized manipulation of online comments by intelligence agents to

aid her victory in the December 2012 election. Park Geun-hye denied ordering or benefiting from election manipulation. **54** In August 2017, the High Court sentenced former director of the NIS Won Sei-hoon to four years in prison for election interference. Won was first indicted in 2013, accused of authorizing agents to post thousands of online comments and 1.2 million tweets characterizing members of the political opposition as North Korea sympathizers. **55** Won and his successor, Nam Jae-joon, admitted to having refuted North Korean propaganda in online forums, but denied political motives. **56**

Similarly, in 2013, the Defense Ministry's cyber command unit, launched in 2010 to "combat psychological warfare in cyberspace," stated that some officials had posted inappropriate political content online during the same period, but without the knowledge of the unit heads. Like Won, they denied the more serious charge of election meddling. **57** However, the ministry's own investigation in the aftermath of Park's impeachment confirmed that former Defense Minister Kim Kwan-jin had mobilized the cyber command unit for smear campaigns against opposition candidates in the 2012 election. **58**

The cyber command unit's interference was not limited to that election. Investigators revealed in February 2018 that the unit operated an assessment team from early 2011 to October 2013 to identify citizens who posted comments critical of the president, government policies, and the military. Referring to those people as "black pen" and "red pen," the team then shared the findings with the National Police Agency and some of the data with the Defense Security Command. **59** The investigators also found that the unit had directly operated an internet news outlet, *Point News*, from 2012 to 2015, using a total of KRW 342 million (\$307,800) of its budget, and that the NIS had authorized

the spending. **60**

Efforts to interfere with online discussions continued after the 2012 presidential election under the oversight of Park's long-time top aid Kim Ki-choon, who has been popularly described as Park's "puppet master." **61** Jinbonet, a civil society organization specializing in digital rights, published handwritten notes from staffers that showed Kim's orders to steer online discussions on various issues during Park's presidency. **62**

The 2016 presidential scandal also led to the publication of a government blacklist comprising almost 10,000 artists, writers, and other cultural practitioners, active online and offline. **63** Those on the list were defunded and professionally disadvantaged for satirizing or being critical of then President Park and her predecessor Lee Myung-bak. Actress Kim Gyu-ri, for example, was reportedly blacklisted for her social media post in May 2008 criticizing Lee's resumption of U.S. beef imports despite public concerns over the danger of mad cow disease. In a September 2017 TV interview, Kim said that her career had been hampered since and she was also incessantly bullied online for the subsequent nine years. **64** It was also revealed by the NIS reform task force in September 2017 that the agency under Lee Myung-bak doctored a photo of actor Moon Seong-geun to make it appear that he was lying naked with actress and social activist Kim Yeo-jin, and circulated the photo online in November 2011 for the purpose of defaming the two liberal-supporting celebrities. **65**

In February 2017, the head of the National Police Agency Lee Cheol-seong said that a special unit would investigate malicious cases of "fake news," especially in the context of the May 2017 presidential election, while less serious cases would continue to be censored in cooperation with the KCSC and the NEC. **66** Similarly, it was reported in March

2018 that the National Police Agency again established a “fake news” taskforce prior to the June 2018 local elections.

67

Police confirmed in March 2017 that they had investigated 40 such cases of “fake news” and that 19 of them had been blocked or deleted. **68** While there has been no evidence that legitimate content has been suppressed, the crackdown has established government agencies as the arbiters of whether online information is true or false.

In October 2018, following the reporting period, Prime Minister Lee called “fake news” the “destroyer of democracy.” He announced his intentions for officials and agencies, such as the police, prosecutors, and the KCC, to target those sharing “fake news,” including individuals and media outlets. **69** Critics noted worries about the effects of these efforts on free expression online.

Since long before the term “fake news” entered the public vocabulary, authorities have limited online speech by arguing that their critics were spreading fraudulent content. In 2013, the KCC targeted several independent investigative news websites, calling their work “pseudo journalism.” **70** In May 2014, conservative legislator Han Sun-kyo proposed a legal amendment to punish rumormongering on social media “in times of disaster” with up to five years in prison or up to KRW 50 million (US\$45,000) in fines, although the proposal expired in May 2016.

Digital Activism

South Koreans have long embraced online technology for civic engagement and political mobilization. During the coverage period, South Korean women took to the internet to vocalize their experiences of gender-based discrimination and violence. When prosecutor Seo Ji-hyeon opened up on

national television and online on January 29, 2018 about her own experience of sexual harassment within the Supreme Prosecutors' Office, some observers hastened to liken Seo's whistleblowing to the #MeToo movement. **71** However, back in October 2016, a mass of Korean women began highlighting the prevailing rape culture across different industries in South Korea, using a series of designated hashtags on social media, and successfully crowdfunded for publications and survivor support. **72**

One of the most historic examples of digital mobilization in South Korea was when the public responded to corruption allegations against then President Park Geun-hye in October 2016. Hundreds of thousands of citizens mobilized to pressure the legislative and judicial branches to bring the president and those involved to justice. On this occasion, the will of citizens, expressed through social media alongside a sustained series of mass candlelight rallies offline, successfully led the more conservative mainstream media and legislators to endorse the removal of the president. **73**

C. Violations of User Rights

The Korean government and its investigative agencies have conducted surveillance of politically active individuals. Individual citizens have also been subject defamation and libel criminal cases for their online activity. During the coverage period, survivors of sexual violence and harassment came forward to speak out but ended up facing retaliation. Indeed, women who had as little as liked, followed, or shared feminist content online were targeted in both their personal and professional lives.

Legal Environment

The South Korean constitution guarantees freedom of speech, the press, assembly, and association to all citizens, but it also enables restrictions, stating “neither speech nor the press may violate the honor or rights of other persons nor undermine public morals or social ethics.” South Korea has an independent judiciary and a national human rights commission that have made decisions upholding freedom of expression. Nevertheless, the prosecution of individuals for online activities has a chilling effect, generating international criticism.

Several laws restrict freedom of expression in traditional media as well as online. The 1948 National Security Act allows prison sentences of up to seven years for praising or expressing sympathy with the North Korean regime. In 2010, the Ministry of Unification issued a notice reminding citizens that the 1990 Act on Exchanges and Collaboration between South and North Korea applies to online communications as well as offline, **74** and that any active engagement with websites or pages maintained by North Korea must be reported to the government in advance. **75** Anyone failing to do so may face a fine of up to KRW one million (US\$900).

Defamation, including written libel and spoken slander, is a criminal offense in South Korea, punishable by up to five years of imprisonment or a fine of up to KRW 10 million (US\$9,000), regardless of the truth of the contested statement. Insult charges, which unlike defamation offenses must be instigated directly by a complainant, are punishable by a maximum KRW two million (US\$1,800) fine or a prison sentence of up to one year. Defamation committed via ICTs draws even heavier penalties—seven years in prison or fines of up to KRW 50 million (US\$45,000)—under the 2005 Information and Communications Network Act, which cites the faster speed and wider audience of online

communication as a basis for the harsher sentencing. **76**

Despite a nine-day filibuster by 38 opposition legislators, a draconian antiterrorism law (Act on Anti-Terrorism for the Protection of Citizens and Public Security) was passed in the then conservative-majority National Assembly in March 2016, 14 years after it was first proposed (see Surveillance, Privacy, and Anonymity).

Proecutions and Detentions for Online Activities

During the coverage period, online defamation and insult cases continued, as did prosecutions and convictions under the National Security Act.

Under the former Park Geun-hye administration, prosecutions for online activity increased. National security arrests increased 19 percent and detentions 37.5 percent during her first year in power. **77** In the post-Park administration, cases involving legitimate speech continue. In one recent example in March 2018, a 53-year-old man, Jeong, was sentenced to one year in prison in the Gwangju District Court for having posted 54 articles that “glorified the North Korean regime and promoted its propaganda” on his blog between 2011 and 2012. **78** In November 2017, a 59-year-old journalist was also sentenced to 14 months in prison for his articles on the pro-communist news site *Jaju Shibo*, including one published in 2016 asserting that North Korean military capacity surpasses that of the U.S. **79** In January 2017, police arrested 67-year-old labor activist Lee Jin-young for distributing Marxist-themed literature online, which was deemed to “benefit the enemy,” but he was cleared of the charge in July 2017. He was reportedly held in solitary confinement and originally faced up to seven years in prison.

The number of online defamation and insult cases increased from 8,880 in 2014 to 14,908 in 2016 and 13,348 in 2017. **80** Recent cases include offenses committed in private KakaoTalk messenger chats, based on complaints from others in the same chats. **81** In August 2017, a 73-year-old man was fined KRW 5 million (US\$4,500) in the Seoul Western District Court for claiming on his blog that former first lady Lee Hui-ho was getting remarried to American rapper Dr. Dre for money laundering purposes. The man was charged for defaming the now deceased 15th president Kim Dae-jung and his widow Lee. **82** Also during the coverage period, numerous survivors of sexual violence and harassment, popularly dubbed “Korean #MeToo victims,” shared their experiences but ended up facing retaliatory defamation lawsuits. **83**

Surveillance, Privacy, and Anonymity

The investigations into the NIS’s abuse of power continued during the reporting period. In a positive development, the number of official requests for communications data decreased slightly in the second half of 2017.

A civilian court cleared a charge against one gay military officer in a case that violated many soldiers’ right to privacy online. In April 2017, it was reported that the country’s army chief, General Jang Jun-kyu, ordered a nationwide “hunt” to out and prosecute gay personnel. **84** Reportedly initiated by a video that a soldier posted on social media showing him having sex with another soldier, the investigation expanded to about 50 soldiers, 22 of whom faced charges under Article 92(6) of the Military Criminal Act. **85** As part of the investigation, army officials seized soldiers’ mobile phones without a warrant to retrieve messenger histories, and signed up for gay dating applications to identify more potential suspects. Seven were found guilty, at least three of

whom are currently appealing their convictions. One officer was discharged upon completion of service in the same month of his indictment. His case was subsequently heard in a civilian court, where his charge was eventually cleared in February 2018. The ruling was considered a welcomed development by the Military Human Rights Center for Korea.

86

Activists have accused government officials of surveilling them on the mobile messenger KakaoTalk, and the company has appeared to face unusual government pressure to comply with data requests. In 2014, Jung Jinwoo, a vice representative of the Labor Party charged with “causing public unrest” during a protest over the Sewol ferry disaster, said prosecutors had accessed two months of his private KakaoTalk conversations, along with the personal details of his 3,000 contacts, as part of the investigation. **87** Yong Hye-in, who initiated a silent protest in support of Sewol victims, was another target. **88** KakaoTalk initially dismissed public concern about this cooperation, but hundreds of thousands of users switched to foreign providers perceived to be beyond the influence of the South Korean government. **89**

Some government agencies may possess more technology that enables them to spy on internet users. In July 2015, leaked documents from the Italian company Hacking Team indicated that the NIS purchased surveillance software to monitor digital activity, especially on domestic mobile devices and KakaoTalk. **90** The agency admitted purchase of the software ahead of the 2012 presidential election, but said it was only used to analyze material related to North Korea. An investigation into possible misuse of the equipment was dropped after a senior intelligence agent, Lim, was found dead in an apparent suicide, leaving a note denying that his team had ever used spyware on citizens. **91**

However, Lim's family has been protesting this conclusion, especially amid the new government's drive to reform the NIS, the Public Prosecutors' Office, and the National Police Agency. **92**

The coverage period saw at least two more suicides associated with investigations into the NIS's abuse of power. An NIS attorney, Jeong, and a prosecutor at the Seoul High Prosecutors' Office, Byun, died in apparent suicide in October and November 2017 respectively, before a court hearing on their alleged involvement in a cover-up of the NIS's election meddling in 2012. **93**

An antiterrorism law passed in March 2016 provided more power to the NIS to undermine individual privacy. **94** The law enables the agency to access individuals' travel records, financial records, private communications, location data, and any other personal information for terrorism investigations, on suspicion alone and without judicial oversight (Article 9). It also allows the NIS to remove content without judicial oversight (Article 12). **95**

Court-issued warrants are otherwise required for investigative agencies to access the content of private communications. However, service providers may "choose" to surrender individuals' metadata to the NIS, police, public prosecutors' offices, and other investigative agencies without a warrant under Article 83(3) of the Telecommunications Business Act. **96** An amendment to Article 16 of the Presidential Enforcement Decree of the Network Act, effective from August 2015, shortened the legally permitted period for retaining users' personal data from three years to one year.

There is limited transparency surrounding official requests for communications data. Service providers have a legal duty to inform the targets, but have been criticized for

failing to fulfill it. **97** Government critics have been particularly vulnerable to undisclosed privacy violations. In 2016, environment activist Lee Heon-seok, civil rights lawyer Yoon Jiyong, and labor union representatives Park Byeong-woo and Kwak Yi-kyung were among dozens to discover in retrospect that they had been the subjects of government requests to mobile carriers, though they were not under arrest or formal investigation at the time. **98**

The government publishes the number of times data was provided to investigative agencies based on these requests, but digital rights advocates say the figures may be misleading, since one request can affect many individuals over a long period of time. **99** According to an official press release, in the second half of 2017, service providers fulfilled 473,145 requests for metadata **100** (a 11.5 percent decrease compared to the same time previous year), and 142,657 requests to access the logs of private communications (a 9.6 percent decrease). **101**

There are some limits on anonymous communication, although a problematic “internet real-name system” was largely dismantled in 2012. First adopted in a 2004 amendment to the Public Official Election Act, **102** the system required users to submit Resident Registration Numbers (RRNs) to join and contribute to major websites. An RRN is a 13-digit number uniquely assigned to Korean citizens at birth. In 2007, the system was applied to any website with more than 100,000 visitors per day under Article 44(5) of the Information and Communications Network Act. The Constitutional Court ruled Article 44(5) unconstitutional in 2012, citing privacy vulnerabilities from cyberattacks among other factors. **103** Under 2013 amendments to the Personal Information Protection Act, website administrators are prohibited from collecting RRNs, and failure to protect an individual’s RRN is punishable by

fines of up to KRW 500 million (US\$450,000). **104**

Mobile service providers still require users to provide their RRNs, and some other registration requirements remain in place. In 2015, the Constitutional Court upheld clauses of the Public Official Election Act requiring people to verify their real names before commenting online during election periods (23 days before a presidential election and 14 days before a general election). **105** Other laws, such as the Children and Youth Protection Act, the Game Industry Promotion Act, and the Telecommunications Business Act, separately require internet users to verify their identities.

106

Intimidation and Violence

During the coverage period, gender-based discrimination and harassment continued, and women were targeted for sharing, subscribing to, following, or even “liking” feminist messages and images on social media. **107**

In an online video interview in July 2017, an elementary school teacher in Seoul, Choi Hyeon-hui, argued for the need to teach feminism in school. She was then subjected to vile online abuse. In September 2017, a conservative parent group filed a report against her to the authorities for “violating the Child Welfare Act by teaching homosexual and misandrous expressions.” **108** While there was a counter-campaign online and offline to defend the teacher and recognize her efforts, she went on prolonged leave in October 2017. **109**

In December 2017, a junior writer at the SBS radio station was removed from her program after many male listeners accused her of “misandry” for following the Instagram account of someone who posts feminist comments. **110** In the same month, an applicant accused a restaurant chain of

rescinding a job offer “on grounds of her feminist activities online.” ¹¹¹ Sexism in the gaming industry resurfaced in the news when the CEO of IMC Games, Kim Hakkyu, announced that he had looked into the case of a female illustrator who followed a women’s rights NGO on Twitter and occasionally retweeted or liked their tweets. The illustrator issued an apology for offending male users. ¹¹²

Besides defamation charges and workplace discrimination, South Korean women have also experienced prevailing violations of their rights to privacy, safety, and dignity. A waxing specialist was murdered in July 2017 by a man who reportedly found a video of her working alone on YouTube, filmed by another YouTuber, located her shop and attempted to rape her before murdering her. ¹¹³

An epidemic problem in South Korea is “spycam porn” (known as “*molka*” in Korean), where small cameras hidden in everyday places, such as toilet stalls, subways, streets, and motels, are used to take pictures or videos of women without consent. The pictures or footage taken are then circulated, traded, and consumed as porn. ¹¹⁴ Having had enough of this invasive and disturbing tactic, more than 12,000 women gathered in central Seoul on May 19, 2018, to condemn this culture. On June 9, some 22,000 women demonstrated, ¹¹⁵ which was at the time the biggest women’s rally in South Korean history. ¹¹⁶ In response to the mass protests, Minister of the Interior Kim Boo Kyum vowed zero tolerance of spycam porn. ¹¹⁷ President Moon also urged harsher penalties for *molka* crimes. ¹¹⁸

Technical Attacks

C8 0-3 pts

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

2/3

of cyberattack?	
-----------------	--

According to the statistics provided by the Korean National Police Agency Cyber Bureau, **119** the number of cyberattacks—including hacking, DDoS, and malware-based attacks—has been increasing, from 2,291 cases in 2014 to 3,156 in 2017. Reported violations of electronic personal data tripled between 2010 and 2013, from 54,832 incidents to 177,736. However, in 2017 the number decreased to 105,122. The government is not known to instigate such attacks.

On February 9, during the opening ceremony of the 2018 Winter Olympics in Pyeongchang, a cyberattack affected internet connectivity, the official Olympic website, and internet users attending the event. **120** It was later reported, citing U.S. intelligence, that Russian military spies hacked several hundred computers used by the South Korean Olympic authorities, with the intention of making the attack look like a North Korean operation. **121**

Local officials alleged that the North Korean government was behind cyberattacks on major banks and broadcasting stations in March 2013, **122**

CrowdStrike, CrowdStrike Global Threat Report, January 22, 2014, p.25, <http://bit.ly/1ffcUUB>. on nuclear power plants in December 2014, **123** and an attack which seized control of a large university hospital network for 8 months in 2015, **124** among many other incidents, which highlight vulnerabilities in the country's ICT infrastructure. **125**

Footnotes

- 1** “Park Geun-hye: More jail time for South Korea ex-leader,” BBC News, July 20, 2018, <https://bbc.in/2LBr3OD>.

Sang-hun Choe, "In South Korea, another former president lands in jail," New York Times, March 22, 2018, <https://nyti.ms/2DNMG9T>.

Be the first to know what's happening.

Isnaan Tharoor, "South Korea: 'I've lived the world how to do democracy,'" Washington Post, <https://nyti.ms/2qGpMy8>.

Justin M. Sizemore, "South Korea spy agency admits trying to rig 2012 presidential election," The Guardian, <https://nyti.ms/2qGpMy8>, 2017,

Join the Freedom House

monthly newsletter

"Editorial: South Korea targets democracy," New York Times, November 19, 2015, <http://nyti.ms/2FjokdJ>.

Email

Subscribe

More footnotes

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