

South Korea

| | 2015 | 2016 | | |
|----------------------------------|-------------|-------------|--|--------------|
| Internet Freedom Status | Partly Free | Partly Free | Population: | 50.6 million |
| Obstacles to Access (0-25) | 3 | 3 | Internet Penetration 2015 (ITU): | 90 percent |
| Limits on Content (0-35) | 14 | 15 | Social Media/ICT Apps Blocked: | No |
| Violations of User Rights (0-40) | 17 | 18 | Political/Social Content Blocked: | Yes |
| TOTAL* (0-100) | 34 | 36 | Bloggers/ICT Users Arrested: | Yes |
| | | | Press Freedom 2016 Status: | Partly Free |

* 0=most free, 100=least free

Key Developments: June 2015 – May 2016

- An antiterrorism law passed in March 2016 grants the National Intelligence Service (NIS) powers to access private communication records and censor online content without judicial oversight during terrorism investigations (see **Surveillance, Privacy, and Anonymity**).
- In July 2015, leaked documents revealed that the NIS purchased spy tools from the Italian company Hacking Team ahead of the 2012 presidential election (see **Surveillance, Privacy, and Anonymity**).
- An amendment to the Newspaper Act, effective from November 2015, bars internet news agencies from fulfilling mandatory registration requirements if they employ fewer than five staff (see **Media, Diversity, and Content Manipulation**).
- Internet users continued to face prosecution for online activities; unlike many local residents, a Japanese journalist was acquitted of defaming President Park Geun-hye in December 2015 (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom declined in 2015-16. The passage of an antiterrorism law with implications for privacy and free speech, and separate, tighter restrictions on news websites were among several issues of concern for internet freedom advocates.

Observers say that freedom of expression, both online and offline, has been undermined since the conservative party returned to power in 2008. Three UN Special Rapporteurs shared concerns after visiting the country in 2010, 2013, and 2016, respectively, saying that the government's new laws, along with more restrictive interpretations and application of existing laws, affect citizens' rights to free speech, assembly, and association.¹

During the coverage period of this report, Park Geun-hye of the conservative Saenuri Party entered the second half of her single, five-year presidential term. However, the investigation into the extent of online content manipulation by the National Intelligence Service (NIS), which was allegedly conducted to aid Park's victory in the 2012 election, was ongoing.² The NIS has been accused of political meddling and abuse of power, and concerns about their activities have extended to the digital realm. In 2016, news reports said NIS and other law enforcement agencies had repeatedly accessed telecommunications company data about labor rights activists and others without their knowledge, though they were not under investigation. Documents publicly leaked in July 2015 indicated that the NIS purchased spy tools from the Italian company Hacking Team for domestic surveillance purposes ahead of the 2012 election.³ An antiterrorism law passed in March 2016 enables the agency to access personal communications and order the removal of online content without judicial oversight during terrorism investigations.⁴

Arrests and prosecutions continue to be documented on grounds of rumormongering and defamation, which South Korean law punishes more severely online than offline. State prosecutors have sought heavy penalties in relation to online speech involving the sinking of Ferry Sewol in April 2014, a disaster that resulted in hundreds of deaths and widespread criticism of the Park administration's response. At least one person was also arrested for comments about an outbreak of the Middle East Respiratory Syndrome (MERS) in mid-2015.

1 Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (A/HRC/17/27/Add.2), 2011, <http://bit.ly/1QgytnP>; Margaret Sekaggya, "Report of the Special Rapporteur on the situation of human rights defenders" (A/HRC/25/55/Add.1), 2013, <http://bit.ly/1oJBN1t>; Maina Kiai, "Statement by the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association at the conclusion of his visit to the Republic of Korea," 2016, <http://bit.ly/1RfNjiy>; see also Amnesty International, "Annual Report 2015/16 – South Korea," 2016, <http://bit.ly/1DkoIB4>.

2 Youngji Seo, "Controversy over the judges' favoritism towards Won Sei-hoon. Senior prosecutor leaves the courtroom in protest" (in Korean), *Hankyoreh*, November 1, 2015, <http://bit.ly/1RD1JW1>; for the case background information, see also Yoo Eun Lee, "South Korea's spy agency, military sent 24.2 million tweets to manipulate election," *Global Voices*, November 25, 2013, <http://bit.ly/1jB00Sp>; Chico Harlan, "In South Korea's latest controversies, spy agency takes a leading role," *The Washington Post*, July 6, 2013, <http://wapo.st/1mO8QJQ>; Aidan Foster-Carter, "Intelligence scandals, Seoul-style," *Asia Times*, November 12, 2013, <http://bit.ly/1b0WGb4>.

3 Bill Marczak & Sarah McKune, "What we know about the South Korea NIS's use of Hacking Team's RCS," *Citizen Lab*, August 9, 2015, <http://bit.ly/1N5ctvi>.

4 Steven Borowiec, "South Korean lawmakers try first filibuster since 1969 to block anti-terrorism bill," *Los Angeles Times*, February 24, 2016, <http://lat.ms/1QpKNmV>.

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). Both commissions are chaired by presidential appointees.

Availability and Ease of Access

South Korea is one of the most wired countries in the world, for both usage and connection speed.⁵ Internet penetration was at 90 percent in 2015.⁶ Counting access via mobile phone, television, and game consoles, an estimated 97 percent of households had access by 2012.⁷

Several factors have contributed to the country's high degree of connectivity. First, high-speed access is relatively affordable. Most residences have connections capable of reaching 100 Mbps for under KRW 30,000 (US\$27) per month.⁸ Second, the population is densely concentrated in urban areas. Roughly 70 percent of South Koreans live in cities dominated by high-rise apartment buildings that can easily be connected to fiber-optic cables.⁹ Finally, the government has implemented a series of programs to expand internet access since the 1990s, including subsidies for low-income groups.¹⁰

Omnipresent and affordable cybercafes have also helped prevent a digital divide in South Korea. Known as *PC bang* ("computer rooms"), many offer broadband access for approximately US\$1 per hour, and also serve as venues for social interaction and online gaming. There is no significant gap in access to information and communication technologies (ICTs) with respect to gender or income levels, although differences persist along generational and professional lines.¹¹

Mobile phone penetration was at 118 percent in 2015—a sign that many users now have more than one device.¹² Moreover, the rate of smartphone ownership rose to 88 percent of the population by spring 2015, surpassing other advanced economies in global surveys.¹³ Wi-Fi coverage has increased rapidly to accommodate smartphones and tablet computers. Free Wi-Fi is offered in over 2,000 public spaces across the country, including train stations, airports, libraries, health centers, and com-

5 Matthew Speiser, "The 10 countries with the world's fastest internet speeds," *Business Insider*, May 17, 2015, <http://bit.ly/1Qppsqs>.

6 International Telecommunication Union, "Percentage of individuals using the internet, 2000-2015," <http://bit.ly/1cblxxY>. A government index reported 81.6 percent penetration, excluding mobile access. <http://bit.ly/1ESUBvJ>.

7 South Korea has been on the top of the Organisation for Economic Co-operation and Development's (OECD) list of internet access rates in 34 member countries since 2000: OECD, "Households with access to the internet in selected OECD countries," *Key ICT Indicators*, July 2012, <http://bit.ly/19Xqbzx>.

8 John D. Sutter, "Why internet connections are fastest in South Korea," *CNN*, March 31, 2010, <http://cnn.it/1mOyYUT>; Edward Wyatt, "U.S. struggles to keep pace in delivering broadband service," *The New York Times*, December 29, 2013, <http://nyti.ms/1cBCKJb>.

9 J. C. Herz, "The bandwidth capital of the world," *Wired*, August 2002, <http://wrd.cm/1f2ENfX>.

10 Sutter, "Why internet connections are fastest in South Korea."

11 Ministry of Science, ICT and Future Planning, "The digital divide index, 2010-2014" (in Korean), *IT Statistics of Korea*, <http://bit.ly/1e2FFNb>.

12 International Telecommunication Union, "Mobile-cellular telephone subscriptions, 2000-2015," <http://bit.ly/1cblxxY>.

13 Jacob Poushter, "Smartphone ownership and internet usage continues to climb in emerging economies," *Pew Research Center*, February 22, 2016, <http://pewrsr.ch/1RX3lqq>.

munity centers.¹⁴ The Ministry of Science, ICT and Future Planning said it would extend this to 12,000 public hotspots by 2017.¹⁵ Jeju, South Korea's biggest and most popular holiday island, will have 640 hotspots by the end of 2016, providing tourists with free and universal Wi-Fi access anywhere on the island.¹⁶

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, police and the National Intelligence Service have oversight over the access points, but the government is not known to implement politically motivated restrictions on internet or mobile access.¹⁷

In January 2016, the independent investigative news site *Newstapa* and other media outlets reported that the Presidential Security Service routinely undertake blanket mobile phone jamming in the vicinity of the President's movements under a loose interpretation of the Presidential Security Act.¹⁸

ICT Market

The telecommunications sector in South Korea is relatively diverse and open to competition, with 94 internet service providers (ISPs) operating as of December 2015.¹⁹ Nevertheless, it is dominated by three companies: Korea Telecom (41.5 percent), SK Telecom (25 percent), and LG Telecom (17 percent). The same firms also control the country's mobile service market, with 25 percent, 38 percent, and 23 percent market share, respectively.²⁰ All three companies are publicly traded, but they are part of the country's *chaebol*—large, family-controlled conglomerates connected to the political elite, often by marriage ties.²¹ 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.²² 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 Ministry of Science, ICT and Future Planning rejected

14 Searchable at http://www.wififree.kr/en/service/map_search.jsp.

15 Ministry of Science, ICT and Future Planning, *Public Wi-Fi Free Service*, <http://bit.ly/1EfmhKz>; Inyoung Choi, "Significant expansion of free public Wi-Fi by 2017" (in Korean), *Yonhap News*, July 12, 2013, <http://bit.ly/1GjEYSO>.

16 Choong-il Choi, "Free Wi-Fi all around Jeju. Available regardless of carriers" (in Korean), *JTBC*, January 2, 2016, <http://bit.ly/1oWUJor>.

17 Interviews with ICT professionals, August 2015.

18 Eun-yong Lee, "'Mobile phone jamming' wherever the president visits. All phones must freeze" (in Korean), *Newstapa*, January 29, 2016, <http://newstapa.org/31493>.

19 Korea Internet & Security Agency, "ISP statistics" (in Korean), *Infrastructure Statistics*, <http://bit.ly/1TPRXSs>.

20 Ministry of Science, ICT and Future Planning, "Wire and wireless communication service subscribers, as of December 2015" (in Korean), *IT Statistics of Korea: Statistical Resources*, <http://bit.ly/1RkOh6B>.

21 Hyeok-cheol Kwon, "Is *Chojoongdong* one big family?" (in Korean), *Hankyoreh*, July 29, 2005, <http://bit.ly/1lhqYQM>.

22 Hyun-ah Kim, "KMI criticizes the selection criteria for the 4th mobile operator and issues an open inquiry" (in Korean), *e-Daily*, February 18, 2013, <http://bit.ly/1fXe7y8>.

their bid for a license for failing to meet financial requirements, which a KMI spokesman described as “excessively strict.”²³

Under the stated aim of easing the information asymmetry caused by the effective oligopoly of the mobile phone market, an 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, and is currently under reconsideration.²⁴

Regulatory Bodies

The conservative Lee Myung-bak government, which was in power from February 2008 to February 2013, restructured the regulatory institutions overseeing the ICT sector. The Ministry of Information and Communication and the Korean Broadcasting Commission merged in February 2008 to create the Korea Communications Commission (KCC), tasked with overseeing both telecommunications and broadcasting to improve policy coherence between the two sectors.²⁵ The KCC consists of five commissioners, with the president appointing two (including the chairman) and the National Assembly choosing the remainder. The KCC struggled to earn credibility, as its first chairman, Choi See-joong, was a close associate of President Lee, causing some observers to view the restructuring as a government effort to tighten control over the media and ICT sectors.²⁶ Lee reappointed Choi as chairman in 2011, despite the objections of opposition lawmakers, who said that Choi’s personnel choices politicized the agency and that his licensing decisions favored conservative-leaning media outlets. Choi resigned in 2012, and was later sentenced to two and a half years in prison and a fine of KRW 600 million (US\$545,000) for influence peddling.²⁷ Lee pardoned him at the end of his presidential term in January 2013.²⁸

In 2013, President Park Geun-hye missed an opportunity to distance herself from this history of cronyism, naming her close aide and four-term lawmaker Lee Kyeong-jae to head the KCC.²⁹ She transferred the KCC’s policy and strategy-related responsibilities to the new Ministry of Science, ICT and Future Planning. The KCC retains its regulatory remit and is currently led by a former judge, Choi Sung-joon.

The content of broadcasting and internet communications is qualitatively monitored by the Korea Communications Standards Commission (KCSC). Established in 2008, the KCSC is nominally an independent organization, but its nine members are appointed by the president and the National

23 Yoon-seung Kang, “Gov’t nixes consortium’s application for new mobile carrier license,” *Yonhap News*, July 24, 2014, <http://bit.ly/1uTA4aR>;

Min-ki Kim, “Bidders for the position of the 4th mobile operator complain of high opening bid of \$260 million” (in Korean), *Yonhap News*, January 20, 2014, <http://bit.ly/1iy4Pfg>.

24 Kwan-yul Cheon, “The birth of ‘that law’ that everybody hates” (in Korean), *SisaIN*, October 31, 2014, <http://bit.ly/1Elq1vz>.

25 Jong Sung Hwang & Sang-Hyun Park, “Republic of Korea,” in *Digital Review of Asia Pacific 2009-2010*, eds. Shahid Akhtar and Patricia Arinto, (London: SAGE, 2009), 234-240.

26 Ji-nam Kang, “Who’s who behind Lee Myung-bak: Choi See-joong the appointed chairman of the KCC” (in Korean), *Shindonga* 583, 2008, <http://bit.ly/1aYiNCd>.

27 Rahn Kim, “President’s mentor gets prison term,” *Korea Times*, September 14, 2012, <http://bit.ly/1esLXak>.

28 “South Korean president issues controversial pardons,” *BBC News*, January 29, 2013, <http://bbc.in/L3ce7o>.

29 “Park appoints former veteran lawmaker as communications commission chief,” *Yonhap News*, March 24, 2013, <http://bit.ly/1gkאוV>.

Assembly.³⁰ The current chair of the commission is Park Hyo-chong, a key figure in the country's neo-conservative movement.

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 is particularly evident. Content that "praises or benefits" communist North Korea or that undermines the traditional social values of the country is blocked or deleted based on the recommendations of the Korea Communications Standards Commission. Systematic manipulation of online discussions is also being investigated. Won Sei-hoon, the former chief of the National Intelligence Service, was sentenced to three years in jail in February 2015 for directing an online smear campaign against the rival of the current president in the December 2012 election. The top court granted Won a retrial in July 2015.³¹

Blocking and Filtering

Censored content is classified by categories including gambling, illegitimate food and medicine, obscenity, violation of others' rights, and violation of other laws and regulations. The last category includes websites containing North Korean propaganda or promoting reunification, based on Article 7 of the 1948 National Security Act, which bans content that "praises, promotes, and glorifies North Korea."³²

Censorship is predominantly carried out on the orders of the Korea Communications Standards Commission (KCSC). In 2008, its first year of operation, 4,731 websites or pages were blocked, and 6,442 deleted.³³ Its activities have steadily increased since then. In 2015, a total of 111,008 websites or pages were blocked and 27,650 deleted.³⁴

A team of 20 to 30 monitoring officers flag possible offenses, including threats to national security and public morals. The police and other authorities can refer matters to the KCSC, and individuals can also submit petitions. Commissioners meet every two weeks to deliberate over flagged cases, and then issue censorship orders to content hosts or service providers.³⁵ Noncompliant service providers face up to two years' imprisonment, or a fine of up to KRW 10 million (US\$9,000), under the

30 Six members are nominated by the president and the party with a parliamentary majority, while three are nominated by the opposition.

Jeong-hwan Lee, "A private organization under the president? The KCSC's structural irony" (in Korean), *Media Today*, September 14, 2011, <http://bit.ly/1aYr0GA>.

31 Ju-min Park, "South Korea court orders retrial of ex-spy chief in vote-meddling case," *Reuters*, July 16, 2015, <http://reut.rs/1pn7aiO>.

32 OpenNet Initiative, "South Korea," August 6, 2012, <http://bit.ly/19XA93S>.

33 3,816 websites or pages were blocked for "encouraging gambling," 549 for "disturbing social order," and 366 for "obscenity;" 3,238 were deleted for "disturbing social order," 1,460 for "obscenity," 1,201 for "violating others' rights," 424 for "violence, cruelty, and hatred," and 119 for "encouraging gambling."

34 Among those blocked, 46,940 were for "encouraging gambling," 37,391 for "prostitution and obscenity," 18,027 for "illegitimate food and medicine," 4,932 for "violating other laws and regulations," and 3,718 for "violating others' rights." Among those deleted, 10,495 for "violating other laws and regulations," 8,106 for "prostitution and obscenity," 7,290 were for "illegitimate food and medicine," 1,661 for "violating others' rights," and 98 for "encouraging gambling." Statistics published quarterly by the Korea Communications Standards Commission at <http://bit.ly/1iDTDgX> (in Korean).

35 Author's interview with Park Kyung Sin, who served as a commissioner until his resignation in 2014, at the KCSC office, April 4, 2013.

Comprehensive Measures on Internet Information Protection issued by the KCC in 2008.³⁶ Observers criticize the KCSC's vaguely defined standards and wide discretionary power to determine what information should be censored, allowing the small number of commissioners to make politically, socially, and culturally biased judgments, often lacking legal grounds.³⁷

Moreover, in many cases, the commission blocks entire sites even though only a small portion of posts are considered to be problematic. In March 2015, for example, the commission blocked the entire platform of an adult cartoon service, saying that part of its content was obscene. However, the service provider argued that the content was provided through an age-authentication system in compliance with the law. Faced with a public furor, the commission withdrew the shutdown order after only two days.³⁸ In May 2016, U.K. journalist Martyn Williams said he would legally dispute the KCSC's blocking of his website *North Korea Tech*, a media outlet that reports on technology in North Korea.³⁹

Content Removal

Political and social content is subject to removal by private companies based on instructions from the KCSC and complaints from individuals, other government agencies, and the police. Individuals may also be requested to remove content. Since domestic companies do not publicize the amount or nature of items subject to removal, the impact on legitimate content is hard to gauge, but during the coverage period at least one candidate for parliamentary elections used takedown requests to delete online references to a compromising news story, indicating the scope for abuse.

The legal grounds for takedown requests was strengthened during the coverage period, when the National Assembly passed an antiterrorism law in March 2016, granting NIS agents 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 receive takedown requests initiated by third parties—meaning other than the victims of the alleged violation—based on perceived defamation, despite opposition from civil society groups.⁴⁰

On receiving a takedown request, the company must hide the content in question for 30 days.⁴¹ The content is deleted if its owner does not revise it or appeal within that time. "Hundreds of thousands of online posts get deleted every year by such temporary removal requests, which in effect remove the posts permanently," according to the Associated Press.⁴² Users and service providers were requested to delete 22,928 items on national security grounds between January 2013 and August

36 Ha-won Jung, "Internet to be stripped of anonymity," *Korea JoongAng Daily*, July 23, 2008, <http://bit.ly/1eOpT9A>.

37 Jillian York & Rainey Reitman, "In South Korea, the only thing worse than online censorship is secret online censorship," *Electronic Frontier Foundation*, September 6, 2011, <http://bit.ly/1gkiKFw>.

38 Sung-won Yoon, "Watchdog hit for excessive digital censorship," *Korea Times*, March 30, 2015, <http://bit.ly/1IWCXcu>.

39 Martyn Williams, "Lawsuit planned over South Korea's blocking of North Korea Tech website," *North Korea Tech*, May 11, 2016, <http://bit.ly/28OGj84>.

40 Young-joo Choi, "KCSC passes an amendment to its regulations on defamation" (in Korean), *PD Journal*, December 10, 2015, <http://bit.ly/1Rlsmwd>.

41 Kyung Sin Park, *Guilty of Spreading Truth* (in Korean), (Seoul: Dasan Books, 2012), 125-130.

42 Associated Press, "Online curbs limit South Korea pre-election speech freedoms," April 11, 2016, <http://apne.ws/2cV37sl>.

2014.⁴³ From 2010 to 2014, over 1.4 million posts on web portals were hidden based on takedown requests. There were around 454,000 such cases in 2014, up from 145,000 in 2010.⁴⁴

Companies are also known to proactively delete content they judge to potentially violate the law to avoid legal liability, even without a complaint. Under Article 44(3) of the Information and Communications Network Act, intermediaries are encouraged to monitor and carry out proactive 30-day takedowns of irregular content.⁴⁵ Companies who can demonstrate proactive efforts to regulate content would be favorably considered by the courts, while those who do not are potentially liable for defamatory or malicious content posted on their platforms by users.⁴⁶ This potential liability encourages compliance with takedown requests even if they have no legal basis. In 2016, the KCSC also asked the web portal Naver to exercise “voluntary restraint” after it posted links to a video drama depicting homosexual themes.⁴⁷

In the lead up to the April 2016 parliamentary election, one blogger told the Associated Press that Kakao deleted as many as two of his posts every day to comply with rules about political information online.⁴⁸ Although a ban on posting election-related commentary in the days before the polls was lifted after it was declared unconstitutional in 2011, content about candidates is still monitored by the National Election Commission, which has a remit to correct information published about candidates in news stories, online, and offline.⁴⁹ In one case during the reporting period, the National Election Commission ordered companies to delete at least 600 online posts that referenced a news story alleging that conservative candidate Na Kyung-won’s daughter had received special treatment during a college admissions program for disabled students in 2012. Na’s campaign had complained to the election commission about a factual error in the story which was unrelated to the allegations.⁵⁰ The commission subsequently warned *Newstapa* for breaching Article 8 of the Public Official Election Act (“responsibilities of the press for fair reports”)⁵¹ Na separately filed a criminal lawsuit against the journalist responsible for the report in March 2016.⁵²

In 2011, the KCSC expanded their remit to social media, mobile applications, and podcasts, creating a team to systematically monitor platforms such as Twitter and Facebook for illegal content.⁵³ The KCSC first warns users to voluntarily delete posts containing false or harmful information. In 2012, a former commissioner said social media cases amounted to roughly five percent of the total consid-

43 Chang, “66 years on, the National Security Act evolves into something for cyberland.”

44 Jiyong Choi, “Portals screen 450,000 posts from view in 2014 – a threefold increase since 2010” (in Korean), *OhmyNews*, September 10, 2015, <http://bit.ly/1Qq8qIP>.

45 Yoo Eun Lee, “Is South Korea encouraging portal sites to self-censor?” *Global Voices*, November 23, 2013, <http://bit.ly/1ff3EhD>.

46 Hyeon-seok Kang, “Portal sites that neglected malicious comments liable for defamation” (in Korean), *Nocut News*, April 16, 2009, <http://bit.ly/1kTPiql>.

47 Dong-hwan Ko, “Lesbian romance in Internet drama slammed,” *The Korea Times*, March 28, 2016, <http://bit.ly/1URtSMQ>.

48 Associated Press, “Online curbs limit South Korea pre-election speech freedoms,” April 11, 2016, <http://apne.ws/2cV37sl>.

49 People’s Solidarity for Participatory Democracy, “Online campaigning permitted? The NEC’s crackdown continues” (in Korean), *OhmyNews*, October 6, 2016, <http://bit.ly/2dIPA6Z>.

50 Associated Press, “Online curbs limit South Korea pre-election speech freedoms.”

51 Kyunghyang Shinmun, “NEC warns Newstapa for reporting the illicit admission of Na Kyung-won’s daughter” (in Korean), *Kyunghyang Shinmun*, April 2, 2016, <http://bit.ly/28KONfp>.

52 Hyeon-cheol Park, “Na Kyung-won files a lawsuit against Newstapa for the allegation of ‘illicit admission’ of her daughter” (in Korean), *Hankyoreh*, March 18, 2016, <http://bit.ly/28Lx2Q0>.

53 Matt Brian, “South Korea may begin censoring social networking, mobile apps from next week,” *The Next Web*, December 1, 2011, <http://tnw.co/1hFQkCf>.

ered by the KCSC.⁵⁴ South Korean officials sent 129 content removal requests to Twitter in 2015, out of a worldwide total of 5,631, although the company did not comply with them.⁵⁵

Until recently, a major cause for concern was that authors of blocked or deleted content were never notified of the KCSC's decision, though ISPs are legally required to notify authors that their content has been taken down. Affected users are allowed to challenge the commission's ruling in principle, but with no independent avenue for appeal available, only 0.07 percent of cases involving censorship have resulted in appeal. 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 before and after deletion.⁵⁶

A copyright law that restricts file sharing was passed in 2009. Often referred to as the "three strikes rule," it allows the Minister of Culture, Sports and Tourism, acting through the Korea Copyright Commission, to shut down an entire forum for failure to comply with a third warning to take down pirated content. Internet companies and civil liberties advocates say the law threatens fair use and free expression.⁵⁷ In 2013, a controversy arose when the commission and the KCSC blocked U.S.-based music-streaming site Grooveshark, among other overseas torrent sites.⁵⁸ Online freedom activists and some users of the site submitted an administrative litigation against the order in February 2014, but the case was dismissed in 2015.⁵⁹

Media, Diversity, and Content Manipulation

South Korea's overall media environment is partly restricted.⁶⁰ In 2012, journalists launched a series of strikes against government interference and censorship for the first time since the country's transition to democratic rule in 1987.⁶¹ In consequence, a variety of alternative and activist media outlets developed online, including *Newstapa*, a user-funded investigative journalism platform. It has accumulated more than 35,000 regular donors since its January 2012 launch, and its YouTube channel had been viewed more than 34 million times by early 2016.⁶² It became a leading source of information on the electoral manipulation scandal in 2013,⁶³ and one of the first to allege systemic corruption and negligence behind the sinking of Ferry Sewol in 2014. In 2013, the KCC called the work of *Newstapa* and a handful of other independent news websites "pseudo journalism," warning their owners not to report on issues outside their remit.⁶⁴

54 Interview with Kyung Sin Park; Ji-hyun Cho, "Criticism escalates over SNS censorship," *The Korea Herald*, January 29, 2012, <http://bit.ly/1jC5NHk>.

55 Twitter Transparency Report: Removal Requests, <http://bit.ly/1mRNH87>.

56 Open Net Korea, "The KCSC now mandated to notify affected content owners before and after censorship orders" (in Korean), January 7, 2015, <http://opennet.or.kr/7974>.

57 Cory Doctorow, "South Korea lives in the future (of brutal copyright enforcement)," *Boing Boing*, March 30, 2013, <http://bit.ly/1fxo4jZ>; "International human rights organizations in support for the abolition of the three-strike rule" (in Korean), *Open Net Korea*, April 1, 2013, <http://opennet.or.kr/1529>.

58 Minoci, "How 'Grooveshark' got blocked: Interview with the KCSC's Rights Violation Monitoring Team" (in Korean), *Slow News*, November 7, 2013, <http://slownews.kr/15204>.

59 Open Net Korea, "Submission of an administrative litigation against the shutdown of Grooveshark" (in Korean), February 3, 2014, <http://opennet.or.kr/5695>.

60 Freedom House, "South Korea," *Freedom of the Press*, 2015, <http://bit.ly/22ZrciQ>.

61 "No news is bad news: Reporters complain of being muzzled," *The Economist*, March 3, 2012, <http://econ.st/1mPL1kL>.

62 *Newstapa's* YouTube page, accessed March 2016, <http://www.youtube.com/user/newstapa>.

63 *Newstapa*, "South Korea spy agency's illegal campaigning on SNS" (in Korean), YouTube video, 15:34, January 6, 2014, <http://bit.ly/1gVTjap>; Yoo Eun Lee, "South Korean authorities discredit dissenting voices as 'not-real' news," *Global Voices*, January 2, 2014, <http://bit.ly/1cpE2sy>.

64 Yoo Eun Lee, "South Korean authorities discredit dissenting voices."

During the coverage period, legal measures introduced new obstacles for journalists seeking to operate in the digital media market. In November 2015, an amendment to the Newspaper Act stipulated that an online news agency must have more than five regular employees to be eligible to register, as part of a crackdown on “substandard” internet media.⁶⁵ The Korea Press Foundation estimated that this could cause at least one third of existing agencies to close down, including most citizen journalism sites; they were given until November 2016 to come into compliance.⁶⁶ All news organizations are required to register, and failure to do so is subject to up to one year of imprisonment or fines up to KRW 20 million (US\$17,200), according to the Act. The constitutionality of the amendment was being challenged in the Constitutional Court in mid-2016.

The diversity of online content was negatively affected in the two weeks before the April 2016 parliamentary election when some media outlets closed their comment functions to comply with the Public Official Election Act, which bans anonymous online communication for 13 days before the polls (see Surveillance, Privacy, and Anonymity).⁶⁷

Trials stemming from a scandal involving politicized manipulation of online comments by intelligence agents saw further developments in 2016. In December 2012, opposition lawmakers accused a National Intelligence Service (NIS) agent of manipulating 40 different online accounts to discredit opponents of then-presidential candidate Park Geun-hye. Police initially cleared the agent,⁶⁸ but in 2013, prosecutors indicted former NIS director Won Sei-hoon on charge of authorizing agents to post thousands of online comments and 1.2 million tweets characterizing members of the political opposition as sympathizers of North Korea.⁶⁹ Park Geun-hye denies ordering or benefiting from digital manipulation.⁷⁰ Won and his successor, Nam Jae-joon, admitted having refuted North Korean propaganda in online forums, but denied political motives.⁷¹ In December 2013, the Defense Ministry’s cyber command unit, launched in 2010 to “combat psychological warfare in cyberspace,” announced that some officials had posted inappropriate political content online during the same period, but without the knowledge of the unit heads. Like Won Sei-hoon, they denied the more serious charge of election meddling.⁷²

In September 2014, the Seoul Central District Court gave Won a suspended sentence under a law that bars intelligence officials from political activity, but acquitted him of trying to sway the elec-

65 Yonhap News, “Editorial from Korea Herald on Nov 21,” *Yonhap News*, November 21, 2015, <http://bit.ly/2dNJH8j>.

66 Sang-geun Jeong, “Exclusive: Internet news agencies with less than 5 employees to be ousted” (in Korean), *Media Today*, November 3, 2015, <http://bit.ly/1L6rAXg>.

67 Associated Press, “Online curbs limit South Korea pre-election speech freedoms,” April 11, 2016, <http://apne.ws/2cV37sl>.

68 In-ha Ryu, “Breaking news: Seoul Police already plots a scenario before releasing the interim report of investigation into the online comments scandal” (in Korean), *Kyunghyang Shinmun*, September 6, 2013, <http://bit.ly/1aWCZkN>; “Seoul Police warns Kwon Eun-hee, who claims the police investigation into NIS was ‘downscaled and covered up’” (in Korean), *Chosun Ilbo*, September 26, 2013, <http://bit.ly/1v85Yjn>.

69 Harlan, “In South Korea’s latest controversies, spy agency takes a leading role;” Dong-hyun Lee, “Won Sei-hoon ordered operations against opposition candidates in every election, says prosecution” (in Korean), *JoongAng Ilbo*, June 6, 2013, <http://bit.ly/1aYlChK>; Sang-Hun Choe, “South Korean officials accused of political meddling,” December 19, 2013, <http://nyti.ms/1ohP89w>.

70 Sang-Hun Choe, “Prosecutors detail attempt to sway South Korean election,” *The New York Times*, November 21, 2013, <http://nyti.ms/1hvtiyf>; Lee, “South Korea’s spy agency, military sent 24.2 million tweets to manipulate election;” Harry Fawcett, “South Korea’s political cyber war,” *Al Jazeera*, December 19, 2013, <http://bit.ly/1cmfW86>.

71 Ho-jin Song et al., “Nam Jae-joon says online posting is the NIS’s legit work, insisting the allegation of election interference be a political set-up” (in Korean), *Hankyoreh*, August 5, 2013, <http://bit.ly/1aDobNp>.

72 Choe, “South Korean officials accused of political meddling;” “Former chiefs of S. Korean cyber command charged with political intervention,” *Shanghai Daily*, August 19, 2014, <http://bit.ly/1v5n6pZ>.

tion.⁷³ Both sides appealed. Despite the lower court's ruling, Won was sentenced in February 2015 to three years in jail for smearing political candidates,⁷⁴ but the Supreme Court granted him a retrial in July 2015.⁷⁵ In January 2015, the Supreme Court cleared the former chief of Seoul police, Kim Yongpan, of covering up an investigation into the scandal.⁷⁶

In the meantime, a sitting judge who had denounced Won's initial acquittal on an intranet was suspended for two months in December 2014.⁷⁷ State prosecutors involved in the investigation were also subjected to career setbacks. Chae Dong-wook resigned in September 2013, six months into his appointment as Prosecutor General in charge of the case, amid rumors of marital misconduct and political pressure. In January 2016, the Seoul High Court fined an NIS agent for illegally gathering personal information about Chae's eight-year-old extramarital son and leaking it to conservative news outlets as part of a smear campaign.⁷⁸ Other state prosecutors leading the case, Yoon Seokyeol and Park Hyung-cheol, were subjected to a one-month suspension and a one-month salary reduction, respectively, for not following internal procedures. During the investigation for disciplinary action, Yoon testified that he was pressured not to "aid the opposition" while pursuing the investigation. They were later reassigned to non-investigative positions,⁷⁹ and Park resigned in January 2016.

In November 2015, an NIS field agent was arraigned to face charges for malicious comments allegedly made as part of the intelligence-orchestrated manipulation campaign. Prosecutors had identified the agent as the individual behind a notorious ID ("Hanging Commies") active in left-leaning online forums. A victim of his abusive posts pressed charges against him in October 2013.⁸⁰

Digital Activism

South Koreans have embraced online technology for civic engagement and political mobilization. During the coverage period, an online community called Megalia used satire to draw attention to gender-based discrimination and violence and campaigned against a pornography platform known for hosting hidden camera footage taken without the subject's consent, causing it to be shut down.⁸¹ The community also raised money to litigate against Facebook, which it accused of taking down their content, and to support victims of sexual assault.⁸²

73 Sang-Hun Choe, "Former South Korean spy chief convicted in online campaign against liberals," *The New York Times*, September 11, 2014, <http://nyti.ms/1qCE6xW>.

74 "South Korea spy chief sentenced to three years in prison," *BBC News*, February 9, 2015, <http://bbc.in/1dibHgP>.

75 Park, "South Korea court orders retrial of ex-spy chief in vote-meddling case."

76 Rahn Kim, "Former Seoul police chief cleared of election law violation," *The Korea Times*, January 29, 2015, <http://bit.ly/1yQwWx6>.

77 "Sitting judge slams court ruling on ex-spy chief," *Global Post*, September 12, 2014, <http://bit.ly/1BakDtA>; Sohee Park, "Criticizing Won Sei-hoon ruling, Judge Kim Dong-jin suspended for two months" (in Korean), *OhmyNews*, 3 December 2014, <http://bit.ly/1dic3UC>.

78 "Ex-presidential official fined for leaking info on ex-top prosecutor's extramarital son," *Yonhap News*, January 7, 2016, <http://bit.ly/1oZHkSb>.

79 Won-il Cho, "Be in the good book or else. Independence of the state prosecution still a distant dream" (in Korean), *Hankook Ilbo*, January 16, 2016, <http://bit.ly/1QMre4f>.

80 In-ha Ryu, "Vicious comments on 12-year-old daughter by Jwaikhyosu: Victim of online comments files lawsuit against NIS agents," *Kyunghyang Shinmun*, October 22, 2013, <http://bit.ly/1pqSfEd>.

81 Hannah Cho, "Sora.net: When online conspiracies become a reality," *Columbia Journal of Transnational Law*, February 15, 2016, <http://bit.ly/1QhMwX2>; Bo-eun Kim, "Police shut down nation's largest porn site server," *The Korea Times*, April 7, 2016, <http://bit.ly/28MBUSU>.

82 The fundraising took place at <https://tumblrbug.com/mersgall4>.

Violations of User Rights

South Koreans faced increasing challenges to online privacy during the coverage period. A new antiterrorism law granted the National Intelligence Service (NIS) powers to collect personal data and monitor individuals' online activity without judicial oversight. Publicly leaked materials in July 2015 also revealed that the NIS purchased spy tools from the Italian company Hacking Team ahead of the December 2012 presidential election for domestic surveillance purposes. Cases involving surveillance or arrest were ongoing in the aftermath of the 2014 Sewol ferry accident. A Japanese journalist was indicted for defaming President Park Geun-hye in 2014. Unlike many local residents, however, he was acquitted in December 2015.

Legal Environment

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

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,⁸³ and that any active engagement with websites or pages maintained by people of North Korea must be reported to the government in advance.⁸⁴ Anyone failing to do so faces 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' 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\$45,500)—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.⁸⁵

In May 2014, a month after the Sewol ferry disaster, conservative legislator Han Sun-kyo proposed amending the Information and Communications Network Act to criminalize rumormongering on social networking sites “in times of disaster,” punishable by up to five years in prison or up to KRW 50 million (US\$45,500) in fines. The proposed clause evolved from 47(1) of the 1983 Telecommunica-

⁸³ Ministry of Unification, “Notice on the use of North Korean internet sites” (in Korean), April 8, 2010, <http://bit.ly/1VVn7ad>.

⁸⁴ Reports of such contact, online and offline, are to be made through an online system at <http://www.tongtong.go.kr/>.

⁸⁵ Act on Promotion of Information and Communications Network Utilization and Data Protection, Art. 61 amended December 30, 2005, <http://bit.ly/LoN97A>.

tions Business Act, which was ruled unconstitutional in 2009. The proposal remained under consideration at the time of writing this report.

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

Prosecutions and Detentions for Online Activities

Prosecutions against individuals expressing North Korean sympathies have increased under conservative rule. In the first year of the Park Geun-hye administration, national security arrests increased 19 percent and detentions 37.5 percent.⁸⁶ Between 2012 and 2014, 104 people were convicted for violation of the National Security Act in cyberspace, although a legislator of the ruling conservative party argued in April 2015 that the number should have been even larger, considering the increase in the number of offenses being committed online.⁸⁷

Numerous online defamation cases have involved President Park Geun-hye since she took office in 2013. With public criticism of her response to the ferry disaster mounting, President Park told a cabinet meeting on September 16, 2014, that “profanity towards the president had gone too far” and that “insulting the president is equal to insulting the nation.”⁸⁸ Two days after this remark, the public prosecutors’ office set up a special investigation unit for an enhanced monitoring of “online slanders and rumors.”

Several prosecutions followed. In March 2015, the Supreme Court sentenced a 31-year-old citizen, Kim, to one year in prison for posting a fake screenshot of a messenger conversation suggesting that the Sewol rescue operation had been deliberately held back, although he deleted it within 10 minutes.⁸⁹ In May 2015, a man in his 50s named Wu, who had repeatedly posted a conspiracy theory about the ferry incident between August and November 2014, was sentenced to 18 months in prison for defaming the coast guard.⁹⁰ Civic activist Park Seong-soo was given a one-year suspended prison term in December 2015 for distributing flyers and Facebook posts containing allegations about the president’s negligence during the rescue operation, which had already been published in *Chosun Ilbo* in Korea and *Sankei Shimbun* in Japan.⁹¹ In the same month, the Supreme Court found Seoul civil servant Kim Minho guilty posting “defamatory remarks” about President Park and other members of the conservative party in May 2014; he was fined KRW 2.5 million (US\$2,780) and lost his position in the City Hall after 22 years.⁹²

86 Hong-du Park, “In Park’s first year, the number of violators of the National Security Act has leaped” (in Korean), *Kyunghyang Shinmun*, February 19, 2014, <http://bit.ly/1fzlxmM>; see also Amnesty International Report 2015/16.

87 “According to Cho Hae-jin, “Online violation of the NSA increasing dramatically but mostly going unpunished” (in Korean), *Yonhap News*, April 10, 2015, <http://bit.ly/1PzwA89>.

88 Full text of the president’s speech to the cabinet (in Korean) available at <http://bit.ly/1ejqd8e>.

89 “A white-collar man who had distributed a fake Kakaotalk on Sewol found to be guilty of cyber defamation” (in Korean), *Kyunghyang Shinmun*, March 1, 2015, <http://bit.ly/1FOli0s>.

90 “A man in his 50s sentenced for one and a half years for posting ‘malicious rumors about Sewol’ around 600 times” (in Korean), *Yonhap News*, May 16, 2015, <http://bit.ly/1F1rBIB>.

91 Miran Kim, “Civic activist Park Seong-soo found guilty for defaming Park Geun-hye’s ‘personal self’” (in Korean), *Gobal News*, December 22, 2015, <http://bit.ly/1RsVHER>.

92 Jong-cheol, Shin, “Supreme Court divests a civil servant of his office for defaming Chung Mong-joon and Park Geun-hye” (in Korean), *Law Issue*, December 28, 2015, <http://bit.ly/1QxJl9d>.

Unusually, even foreign reporters came under scrutiny. Japanese journalist Tatsuya Kato of the *Sankei Shimbun* newspaper was indicted for criminally defaming President Park in an August article that cited allegations about the president's whereabouts in the immediate aftermath of the ferry accident, although the same content was first published in a domestic daily, *Chosun Ilbo*, and spread across online media. The journalist was barred from leaving South Korea for eight months, and faced up to seven years in prison,⁹³ but was ultimately acquitted in December 2015.⁹⁴ Beyond national jurisdiction, two U.S.-based journalists received a complaint from the South Korean government for articles criticizing the Park Geun-hye administration's crackdowns on dissent.⁹⁵

At least one similar case was reported after the Middle East Respiratory Syndrome (MERS) broke out in May 2015. At least 184 cases, including 33 deaths, were confirmed by the beginning of July.⁹⁶ On June 3, a 49-year-old man in Gyeonggi province named Lee was arrested on suspicion of defamation and obstructing business for forwarding a list of four hospitals he said were possibly affected by the outbreak to his contacts on the domestic instant messenger Kakaotalk the previous afternoon.⁹⁷ Police said the hospitals were unaffected.

In March 2016, the Supreme Court issued a positive ruling involving a 37-year-old doctor, Kim, who was prosecuted for insulting the Health Insurance Review and Assessment Service on his blog. The court ruled that swearwords do not constitute insults in the context of criticisms of government policies.⁹⁸

Surveillance, Privacy, and Anonymity

The National Intelligence Service (NIS), the country's chief spy agency, has been at the epicenter of surveillance scandals in recent years. In July 2015, documents from the information technology company Hacking Team were leaked online, indicating that the NIS purchased surveillance software from the Italian company to monitor digital activity, especially on domestic mobile devices and Kakaotalk.⁹⁹ The agency acknowledged purchase of the software ahead of the 2012 presidential election, but maintained that it was only used to analyze material related to North Korea. In the wake of the revelations, on July 18, a senior intelligence agent was found dead in an apparent suicide, leav-

93 Roy Greenslade, "South Korea urged to drop libel charges against Japanese journalist," *The Guardian*, October 17, 2014, <http://bit.ly/1xyYbZl>; Nathan Park, "Is South Korea's criminal defamation law hurting democracy?" *The Wall Street Journal*, December 15, 2014, <http://on.wsj.com/16u0CFE>.

94 Sang-Hun Choe, "Court acquits journalist accused of defaming South Korean president," *The New York Times*, December 17, 2015, <http://nyti.ms/1Yn8Z9l>.

95 Whan-woo Yi, "Gov't hit for overreacting to foreign reports," *Korea Times*, December 7, 2015, <http://bit.ly/1So4UDw>; Se-Woong Koo, "War of words over the state of South Korea," *Korea Exposé*, December 10, 2015, <http://bit.ly/1TEjgNx>. The articles in question are: Se-Woong Koo, "South Korea's textbook whitewash," *The New York Times*, November 12, 2015, <http://nyti.ms/1UF3sNu>; Tim Shorrock, "In South Korea, a dictator's daughter cracks down on labor," *The Nation*, December 1, 2015, <http://bit.ly/1NphwAD>.

96 WHO, "Middle East respiratory syndrome coronavirus (MERS-CoV)—Republic of Korea," World Health Organization, July 3, 2015, <http://bit.ly/28QuMjd>.

97 "'Random hospital list' leads to the first arrest for spreading MERS rumors" (in Korean), *Yonhap News*, June 3, 2015, <http://bit.ly/1TYxtHh>.

98 Yonhap News, "According to the Supreme Court, swearing while criticizing government policies does not constitute an insult" (in Korean), March 9, 2016, <http://bit.ly/28O6l5f>.

99 Bill Marczak & Sarah McKune, "What we know about the South Korea NIS's use of Hacking Team's RCS," *Citizen Lab*, August 9, 2015, <http://bit.ly/1N5ctvi>; Yu-kyeong Jeong, "Everything you wanted to know about the NIS hacking scandal" (in Korean), *Hankyoreh*, July 23, 2016, <http://bit.ly/23IIA2W>.

ing a note denying that his team had ever used spyware on citizens.¹⁰⁰ An investigation into possible misuse of the equipment was subsequently dropped.

In the context of growing concerns over the NIS's political meddling and lack of accountability, it is anticipated that the new antiterrorism law, passed in March 2016, will further enhance the NIS's position and threaten individual privacy.¹⁰¹ To advance terrorism investigations, the law enables the agency to use military means (Article 2), override any other law (Article 4), access individuals' travel records, financial records, private communications, location data, and any other personal information, on suspicion alone and without judicial oversight (Article 9). It also provides the agency with budgets that are not subject to audit, (Article 11), and allows it to have any items of expression removed from content online and offline, without judicial oversight (Article 12).¹⁰²

In activities not covered by that law, court-issued warrants are required to access the content of private communications. Service providers may "choose" to surrender individuals' metadata to the NIS and other investigative agencies without a warrant under Article 83(3) of the Telecommunications Business Act.¹⁰³ According to an official May 2015 press release, service providers fulfilled 508,511 requests for metadata in the second half of 2014, a six percent increase compared to the same period in 2013.¹⁰⁴ The number of affected citizens corresponds to roughly one fifth of the population.¹⁰⁵ Requests to access the content of private communications decreased, from 132,070 to 127,153 and from 337 to 192 respectively. User rights advocates say these figures may be misleading, since one request can affect many individuals over a long period of time.¹⁰⁶ An amendment to 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.

Service providers are also criticized for not fulfilling their legal duty of informing affected individuals,¹⁰⁷ leading internet users to share among themselves how to retrieve information about disclosures affecting their accounts.¹⁰⁸ Environment activist Lee Heon-seok, civil rights lawyer Yoon Jiyoung, and labor union representatives Park Byeong-woo and Kwak Yi-kyung are among dozens to discover after the fact that they were the subject of government requests to mobile carriers, though they were not under arrest or formal investigation at the time. The NIS and police retrieved Park's meta-

100 Jack Kim, "South Korea spy found dead with note denying agency targeted citizens," *Reuters*, July 19, 2015, <http://reut.rs/1QyBC03>; David Gilbert, "Hacking Team leak linked to South Korean spy suicide," *International Business Times*, July 20, 2015, <http://bit.ly/1QwkU52>.

101 Jun-beom Hwang, "Will passage of anti-terror bill turn the NIS into a monster?" *Hankyoreh*, March 3, 2016, <http://bit.ly/1TUSjY4>.

102 Steven Borowiec, "South Korean lawmakers try first filibuster since 1969 to block anti-terrorism bill," *Los Angeles Times*, February 24, 2016, <http://lat.ms/1QpKNmV>.

103 Metadata includes the user's name, RRN, postal address, telephone number, user ID, and dates of joining or leaving the service.

104 Tae-jin Kim, "Communication information handover increases—500,000 cases in the 2nd half of last year" (in Korean), *ZDNet*, May 21, 2015, <http://bit.ly/1cRDcgu>.

105 Kyung-sin Park, "50 times more frequent than in the US, why the current Korean practice of accessing communicator ID information is unconstitutional" (in Korean), *Slow News*, June 14, 2016, <http://slownews.kr/55068>.

106 Gwang Choi, "The public prosecutors access 67 accounts with one piece of document" (in Korean), *Money Today*, December 3, 2014, <http://bit.ly/1ekA7Gy>.

107 See also a public campaign by Open Net: "Reclaim the right to be informed when telecom companies disclose personal information" (in Korean), <http://bit.ly/1GRAX6e>.

108 PPSS, "How to find out whether the NIS and police rummage my mobile phone information?" (in Korean), PPSS, February 26, 2016, <http://ppss.kr/archives/74772>.

data ten times within four months and Kwak's 17 times over a year.¹⁰⁹ In response to requests from users, service providers have refused to provide grounds for complying with these demands.¹¹⁰

The 2014 ferry disaster also prompted accusations of privacy violations and government surveillance. The most telling development was a closed-door meeting that public prosecutors held with major service providers in September 2014 to discuss how to curb rumormongering, including on Kakaotalk, the country's most popular mobile messaging application.¹¹¹ The company dismissed public concern about its cooperation with law enforcement agencies, saying its compliance was prescribed by law.

Public trust in Kakaotalk, however, was undermined in October 2014 during a press conference by Jung Jinwoo, a vice representative of the Labor Party charged with "causing public unrest" during a post-Sewol protest. Jung said prosecutors had accessed two months' worth of his private Kakaotalk conversations, along with the personal details of his 3,000 contacts, as part of the investigation.¹¹² Public prosecutors responded by asking the court to cancel Jung's bail.¹¹³ Yong Hye-in, a university student who initiated a silence protest to show support and solidarity for Sewol victims and their families, also turned out to be subject to surveillance on Kakaotalk.¹¹⁴ In a February 2016 court case, Yong successfully contested the validity of the surveillance warrant executed against her on grounds that she was not appropriately informed, but prosecutors appealed the case to the Supreme Court.¹¹⁵

Some 400,000 users left the service for foreign alternatives perceived to be beyond the influence of the South Korean government, such as Telegram, a Germany-based messaging service that advertises encrypted connections.¹¹⁶ In order to regain user trust, Kakaotalk held a press conference in October 2014, where its CEO, Lee Sir-goo, vowed to reject future data requests from the authorities, even those with warrants.¹¹⁷ The following month, it was reported that seven warrants were pending due to the company's noncompliance. A year later, in October 2015, Kakaotalk announced that it would resume complying with law enforcement requests. More users, including politicians and activists, were reported to be switching messenger clients from Kakaotalk to Telegram, and using iPhones, the only smartphone device known to have failed to meet the NIS requirements,¹¹⁸ after the antiterrorism bill was passed in March 2016.¹¹⁹

109 Hyung-kyu Kim, "NIS digs around the communication records of environmental activists, union representatives, and lawyers" (in Korean), *Kyunghyang*, March 4, 2016, <http://bit.ly/1Sp9n8O>.

110 Junho Bang, "When asked why my 'communication information' was looked at, service providers refuse to answer, saying they have 'no legal obligation'" (in Korean), *Hankyoreh*, March 13, 2016, <http://bit.ly/1Th3R6J>.

111 Jae-seob Kim, "KakaoTalk managers present at prosecutors' meeting on countering 'defamation of the president'" (in Korean), *Hankyoreh*, October 2, 2014, <http://bit.ly/1vzr6Oy>.

112 "Jung Jinwoo: Police surveillance over 3,000 of my family and acquaintances" (in Korean), *JTBC News*, October 2, 2014, <http://bit.ly/1PAH0nY>.

113 "Public prosecutors says Vice rep Jung Jinwoo's 'Kakaotalk press conference' caused public unrest" (in Korean), *Yonhap News*, October 19, 2014, <http://bit.ly/1F5J3lu>.

114 Myeong-soo Seon, "How was Kakaotalk surveillance 'legally' possible?" (in Korean), *Pressian*, October 1, 2014, <http://bit.ly/1LkpBJJ>.

115 Junho Bang, "Kakao chat surveillance victims stage citizens' filibuster," *Hankyoreh*, February 26, 2016, <http://bit.ly/21KAlha>.

116 Sam Judah & Thom Poole, "Why South Koreans are fleeing the country's biggest social network," *BBC News*, October 10, 2014, <http://bbc.in/1MimzBb>.

117 Peter Micek, "South Korean IM app takes bold stand against police abuses," *Access*, October 16, 2014, <http://bit.ly/1Q1as1f>; "Seven warrants for Kakaotalk monitoring still disobeyed and prosecutors looking to enhance law" (in Korean), *Yonhap News*, November 12, 2014, <http://bit.ly/1R9P8JC>.

118 Nayoung Shim, "iPhone fails at the NIS's security compatibility assessment" (in Korean), *Asia Economy*, November 12, 2012, <http://bit.ly/1QA7YYy>. The full description of the NIS's Security Verification Scheme can be found here: http://eng.nis.go.kr/EAF/1_7_1_1.do

119 Hyung-kyu Kim, "'2nd wave of cyber exodus' with the anti-terrorism bill now passed. Ruling party members joining too" (in Korean), *Kyunghyang Shinmun*, March 4, 2016, <http://bit.ly/1QA8Ps9>.

In November 2015, Kakaotalk CEO Lee stepped down to face criminal charges for failing to prevent teenagers from sharing lewd photos of themselves on the service, in contravention of Article 17(1) of the Children and Youth Protection Act. Though the charge carries a possible two-year prison sentence, few observers expect him to be convicted, and he took a position with a media group soon after his resignation. Nevertheless, since holding a CEO personally liable for user activity is unprecedented in South Korea, critics suspected that the real goal was “to punish him for resisting government surveillance efforts and refusing to curb users’ opinions critical of the government.”¹²⁰ During a parliamentary filibuster in February 2016, opposition legislator Hong Jong-hak reported that Kakaotalk was subjected to comprehensive tax audits three times within the last seven years, a level of scrutiny reserved for just 0.06 percent of corporate bodies. According to Hong, the audits took place during periods of heightened public criticism of the government, including after the Sewol ferry disaster in 2014 and the MERS outbreak in 2015. The 2015 audit lasted 137 days, three times longer than the average 36 days.¹²¹

Within South Korea, anonymous communication was long compromised by the so-called “internet real-name system” first adopted in 2004 as part of an amendment to the Public Official Election Act.¹²² Users were required to verify their identities by submitting their Resident Registration Numbers (RRNs) to join and contribute to web portals and other major sites. An RRN is a 13-digit number uniquely assigned to a Korean citizen at birth. In 2007, the real-name system was expanded to apply to any website with more than 100,000 visitors per day under Article 44(5) of the Information and Communications Network Act.

In 2012, the Constitutional Court ruled Article 44(5) of the Network Act unconstitutional, citing privacy vulnerabilities from cyberattacks among other factors.¹²³ In 2011, a cyberattack allegedly originating from China targeted the popular portal Nate and its social networking service Cyworld. Hackers reportedly stole the personal details of 35 million users, equivalent to 70 percent of the population, including names, passwords, RRNs, mobile phone numbers, and email addresses. The portal’s parent company, SK Communications, said RRNs and passwords were encrypted,¹²⁴ but the incident renewed public concern about internet users’ right to privacy.¹²⁵

The Personal Information Protection Act was amended in 2013 to reflect the Constitutional Court’s 2012 ruling. Website administrators are now prohibited from collecting users’ RRNs, and must destroy those already on record. Effective from August 2014, failure to protect an individual’s RRN is punishable by fines of up to KRW 500 million (US\$455,000).¹²⁶ Mobile service providers still require users to provide their RRNs.

Other laws, such as the Public Official Election Act, the Children and Youth Protection Act, the Game Industry Promotion Act, and the Telecommunications Business Act, separately require internet users

120 “South Korea targets dissent,” *The New York Times*, November 19, 2015, <http://nyti.ms/1jah3N0>; Simon Mundy, “Freedom fears as South Korea targets chat app chief,” *Financial Times*, November 17, 2015, <http://on.ft.com/1QVI2p4>.

121 Slides that he used during his speech on February 29, 2016, are available for downloads at his official blog: <http://bit.ly/1L7u4ol>.

122 The amendment became Article 82, Provision 6.

123 Kyung Sin Park, “Korean internet identity verification rule struck down unconstitutional; 12 highlights of the judgment,” *K.S. Park’s Writings* (blog), August 25, 2012, <http://bit.ly/1nevLB7>.

124 AP, “Nate, Cyworld hack stole information from 35 million users: S Korea officials,” *Huffington Post*, July 28, 2011, <http://huff.to/1k9aiaf>.

125 Eric Pfanner, “Naming names on the internet,” *The New York Times*, September 4, 2011, <http://nyti.ms/1ffDiLz>.

126 Yun-ji Kang, “Hide your RRN away! Ban on online collection of user RRNs” (in Korean), *Policy News* (blog by the Ministry of Culture, Sports and Tourism), February 21, 2013, <http://bit.ly/1eefGaD>.

to verify their identities.¹²⁷ In July 2015, the Constitutional Court confirmed that it is appropriate for the Public Official Election Act to require people to use their real names online during election periods (22 days before a presidential election and 13 days before a general election).¹²⁸

To ensure compliance with these laws, the KCC is exploring other identity verification methods, such as Internet Personal Identification Numbers (i-PINs, overseen by the Ministry of Government Administration and Home Affairs), authenticated certificates (issued by banks and other organizations permitted to collect RRNs by Article 23 of the Network Act), and SMS verification. However, large-scale hacking attacks into the i-PIN system in February 2015, generating 750,000 counterfeit numbers, called for rethinking of the security framework at a more fundamental level.¹²⁹

Following the 2011 Cyworld hack, around 2,900 users together filed suit for damages, but the Seoul High Court ruled in favor of the company in March 2015.¹³⁰ Fifteen citizens also filed a lawsuit to change their RRNs, but the Seoul Administrative Court and the Seoul High Court ruled against them. However, in December 2015, the Constitutional Court ruled that disallowing people to change their RRNs was unconstitutional and advised that the Resident Registration Act be revised accordingly by December 31, 2017.¹³¹

Intimidation and Violence

There have been no reports of physical violence against online users in South Korea.

Technical Attacks

Reported violations of electronic data tripled between 2010 and 2013, from 54,832 incidents to 177,736, but decreased to 152,151 in 2015, according to official statistics.¹³² Local officials alleged that the North Korean government was behind the attacks on major banks and broadcasting stations in March 2013,¹³³ those on nuclear power plants in December 2014,¹³⁴ and remote controlling of a large university hospital network over 8 months between 2014 and 2015,¹³⁵ among many other such threats,¹³⁶ which highlight vulnerabilities in the country's ICT infrastructure. Attacks were ongoing during the reporting period, though they did not succeed in disabling as many high-profile institutional targets.

127 Bora Jeong, "Internet real-name system and its lingering remains" (in Korean), *Bloter.net*, September 13, 2013, <http://bit.ly/1jKR4Hx>.

128 Kyung-min Lee, "Online real name system during election periods constitutional: court," *The Korea Times*, July 30, 2015, <http://bit.ly/28QNHnH>.

129 Sang-wook Ahn, "Hacking attacks result in 750,000 counterfeit public i-PINs" (in Korean), *Bloter*, March 5, 2015, <http://bit.ly/1AoxYne>.

130 Jihoon Kim, "Court says SK Comms has no responsibility to compensate users for Cyworld personal information hack" (in Korean), *Newsis*, March 20, 2015, <http://bit.ly/1F1vB5o>.

131 Hyun-ju Ock, "Court allows changes to national IDs," *Korea Herald*, December 23, 2015, <http://bit.ly/1OVgcZ8>.

132 Statistics Korea, "Incidents of personal information violation" (in Korean), *e-National Indicators*, <http://bit.ly/1fcGxBK>.

133 Agence France-Presse, "S. Korea probe says North behind cyber attack," *The Straits Times*, April 10, 2013, <http://bit.ly/1jKAUAa>; CrowdStrike, *CrowdStrike Global Threat Report*, January 22, 2014, p.25, <http://bit.ly/1ffcUUB>.

134 Jeyup S. Kwaak, "North Korea blamed for nuclear-power plant hack," *Wall Street Journal*, March 17, 2015, <http://on.wsj.com/1EYLbnB>.

135 Chang-wook Kang, "North Korea's remote controlling over the entire network of a large university hospital in Seoul goes unnoticed for 8 months" (in Korean), *Kukmin Ilbo*, August 13, 2015, <http://bit.ly/1RMH2XU>.

136 Ju-min Park & Jack Kim, "South Korea says suspects North Korea may have attempted cyber attacks," *Reuters*, January 26, 2016, <http://reut.rs/1QBm7rW>.