South Korea

Despite the fact that South Korea has one of the most advanced information communication technology sectors in the world, online expression remains under the strict legal and technological control of the central government. The country is the global leader in Internet connectivity and speed, but its restrictions on what Internet users can access are substantial.

RESULTS AT A GLANCE

Filtering	No Evidence of Filtering	Suspected Filtering	Selective Filtering	Substantial Filtering	Pervasive Filtering
Political	•				
Social			•		
Conflict and security					•
Internet tools	•				

OTHER FACTORS

	Low	Medium	High	Not Applicable
Transparency			•	
Consistency			•	

KEY INDICATORS	
GDP per capita, PPP (constant 2005 international dollars)	25,493
Life expectancy at birth, total (years)	80
Literacy rate, adult total (percent of people age 15+)	99*
Human Development Index (out of 169)	12
Rule of Law (out of 5)	3.5
Voice and Accountability (out of 5)	3.2
Democracy Index (out of 167)	20 (Full democracy)
Digital Opportunity Index (out of 181)	1
Internet penetration rate (percentage of population)	81.5

*South Korea does not report literacy rate information. In previous years, the United Nations has assumed a literacy rate of 99 percent for the country. See United Nations Development Program, "Human Development Report 2009: Overcoming barriers: Human mobility and development," 2009, http://hdr.undp.org/en/media/HDR_2009_EN_Complete.pdf.

Source by indicator: World Bank 2009, World Bank 2008a, UNDP 2009, UNDP 2010, World Bank Worldwide Governance Indicators 2009, Economist Intelligence Unit 2010, ITU 2007, ITU 2009. See Introduction to the Country Profiles, pp. 222–223.

Background

The Republic of Korea (commonly referred to as South Korea) was established in 1948 and spent most of its first four decades under authoritarian rule. In response to massive protests in 1987, the government eventually enacted a democratic constitution that has endured to this day. South Korea has become one of the most vibrant democracies in the eastern hemisphere, and its human rights record has markedly improved since the 1990s. Today, South Korean citizens enjoy universal suffrage and broad constitutional freedoms, and they choose their leaders in free and fair multiparty elections.

The diplomatic policies of South Korea are heavily influenced by its relationship with the Democratic People's Republic of Korea (commonly referred to as North Korea). South Korea has been technically at war since the two sides fought to a stalemate in 1953. Since then the government has often been intolerant of dissident views, particularly from supporters of communism or of North Korea.[1] The National Security Law (NSL) is the epitome of the government's stance—thousands of South Koreans have been arrested under the anticommunist law since its enactment in 1948.[2] Although prosecutions under the NSL have significantly decreased since the late 20th century, there have been a few recent high-profile investigations using the law. At the start of the 21st century, South Korea attempted a new policy of engagement with

North Korea. Known as the Sunshine Policy, it was enacted by Kim Dae-jung, the 2000 Nobel Prize laureate who served as president from 1998 until 2003.[3] However, the frequent military provocations of North Korea continue to pose ongoing threats to security in South Korea. Today, freedom of expression online in South Korea, with its political and economic complexities, is confronting a new phase of controversy.

Internet in South Korea

South Korea is one of the most connected countries and most penetrated broadband markets in the world: by 2010, more than 81 percent of citizens had access to the Internet,[4] and more than 16 million people subscribed to broadband service.[5] Following heavy investment in broadband infrastructure after the Asian financial crisis in the late 1990s, South Korea now provides its citizens with a national network that carries data at average speeds of 17 Mbps, the highest in the world.[6] Its capital, Seoul, has been named "the bandwidth capital of the world," with its fast yet inexpensive broadband service.[7] Besides Seoul, major cities in South Korea also supply wireless broadband through Wibro and High-Speed Downlink Packet Access technologies. As a result of this broad coverage, over three-quarters of South Koreans use the Internet more than once per day.[8]

As of 2010, there were 126 Internet service providers (ISPs) in the country interconnected through five Internet exchange points (IXPs).[9] However, of these 126 ISPs, three (KT, formerly known as Korea Telecom, Hanaro Telecom, and Korea Thrunet) control almost 85 percent of the broadband market share.[10] KorNet—the largest broadband supplier—provides approximately half of the ADSL lines in the country, making it the largest ADSL supplier in the world.[11]

Legal and Regulatory Frameworks

Despite South Korea's political democracy and extensive Internet connectivity, freedom of online expression has fewer protections than other democracies have. Article 21 of the Korean constitution guarantees that "all citizens shall enjoy freedom of speech and the press," and prohibits censorship of speech and the press.[12] At the same time, Article 21 contains qualifications that "neither speech nor the press shall violate the honor or rights of other persons nor undermine public morals or social ethics."[13] Through Article 21, the constitution empowers the Korean government to regulate expression in news and broadcasting media.[14]

Laying the foundation for all digital and analog content regulation, Article 53(1) of the Telecommunications Business Act (1991) provides that "a person in use of telecommunications shall not make communications with contents that harm the public peace and order or social morals and good customs."[15] Harmful communications are to be determined by presidential decree,[16] and in the original formulation,

harmful communications are referred to as content that aims at or abets a criminal act, aims at committing antistate activities, or impedes good customs and other aspects of social order.[17] Harmful communications can be further restricted by order of the Ministry of Information and Communication (MIC), which delegates this authority to the Information and Communication Ethics Committee (ICEC).[18] The ICEC was established under an amended Telecommunications Business Act (1995) to regulate the content of communications and inform state policy aimed at suppressing subversive communications and "promoting active and healthy information."[19]

In June 2002, the Supreme Court struck down the provisions of the Telecommunications Business Act defining "harmful" content and granted the government unlimited authority to regulate harmful Internet content.[20] The court held Article 53(1) to be insufficiently specific and clear, and Article 53(2) to violate the rule against blanket delegation.[21] In December 2002, the National Assembly amended Article 53 to prohibit content that is "illegal" rather than "harmful," while upholding the executive powers of the MIC and the delegated regulatory authority of the ICEC.[22] This provision was ultimately repealed with the 2007 amendment of the Act on Promotion of Information and Communications Network Utilization and Information Protection (Information Act),[23] although the definition referring to "illegal" material remains in place at least functionally.[24] Illegal information included in types of information to be reported continues to be defined as that which infringes on public interests and social order, specifically obscenity, defamation, violence or cruelty, and incitement to gambling.[25]

Specific laws to protect youth, national security, and other national priorities have informed the scope of content that is regulated by government-delegated bodies responsible for filtering. For example, the NSL[26] provides "up to seven years in prison for those who praise, encourage, disseminate or cooperate with antistate groups, members or those under their control."[27] Similarly, the directive to protect the country's youth from "harmful"[28] Internet content, broadly described as "immoral, violent, obscene, speculative and antisocial information,"[29] has been one of the central planks in South Korea's filtering policy. In accordance with the Juvenile Protection Act, ISPs are responsible for making inappropriate content inaccessible on their networks.[30] Web sites carrying adult content must warn visitors and require identification verification for access—measures meant to prevent minors under 19 from accessing pornographic material.[31]

In February 2008, the Korea Communications Commission (KCC) was created to consolidate the MIC and the Korean Broadcasting Commission (KBC). Under South Korea's current legal framework, regulation of Internet content is conducted primarily by two government agencies: the Korean Communications Standards Commission (KCSC; formerly KISCOM)[32] and the National Election Commission (NEC). The KCSC integrated the functions of the KBC and KISCOM[33] in February 2008.[34] Accordingly, the two KCSC subcommissions deal separately with broadcasting and telecommunications standards.[35]

At its inception, the ICEC was empowered to develop general principles or codes of telecommunications ethics, deliberate on and request the "correction" of information declared "harmful" by presidential decree, and operate centers reporting against unhealthy telecommunications activities.[36] The KCSC telecom subcommission continues to make determinations on "requests for correction" with respect to ISPs and Internet content providers (ICPs).[37] Thus the KCSC is empowered to make determinations on information "harmful" to youth under the Juvenile Protection Act,[38] as well as recommend action against Web sites containing "illegal" content, including pornography, information for cyber criminals, and gambling services, and Web sites that express support for communism or for the government of North Korea.[39] The scope of its authority extends to ordering the blocking or closure of Web sites, the deletion of offending messages, and/or the suspension of users identified as posting improper writing.[40] In addition to special advisory committees, the KCSC also mediates disputes over online defamation. The KCSC said it received 156,000 complaints in 2006 about Internet postings considered inaccurate, and 216,000 in 2007.[41]

With President Lee's full support, government ministries proposed a battery of legislation beginning in July 2008 that would create a framework for addressing defamation, "false rumors," and "malicious postings." In July 2008, the KCC introduced the Comprehensive Measures on Internet Information Protection, which instituted 50 changes to communications and Internet regulation.[42] In amendments to the Information Act, the South Korean government further expanded the already-significant regulatory authority of the KCC by adding to online providers' liability for their users' acts. The KCSC was authorized to force providers to delete content or suspend publishing for a minimum of 30 days upon receiving a complaint of "fraudulent" or "slanderous" postings, during which the commission would determine whether disputed articles should be removed permanently.[43] Internet portals that failed to block such postings would be subject to a fine of up to KRW 30 million (just over USD 26,500) or could be forced to shut down,[44] while portals or individuals involved in improperly manipulating Internet search results could be subject to imprisonment for up to one year and a fine of up to KRW 10 million (USD 8,800).[45] In cases of leaked personal information, the KCSC requires the portal to inform the victim of the privacy breach and report the matter to the KCC.

Following an approach taken toward other emergent forms of harmful or illegal content, ICPs have increasingly taken on responsibility for policing slanderous content. Although they were already legally compelled to set up constant in-house monitoring functions,[46] Korea's two largest Internet portals also implemented their own measures to curb postings considered to violate privacy. For example, Naver created a simplified process for users to quickly block "groundless rumors or postings," and Daum required users to click on a different box if they want to read other users' comments.[47]

In July 2008, Minister of Justice Kim Kyung-hwan introduced the crime of "cyber defamation," which punishes those who insult others through the Internet with up to two years imprisonment or a KRW 10 million (USD 8,800) fine.[48] Under this rubric, criminal law applies to defamation and threats, while penalties for cyber defamation and "cyber stalking" will be pursued under information and communication laws.[49] Public figures whose personal information is widely shared on the Internet are often the primary victims of online defamation, as in the cases of Tablo[50] and Choi Jin-sil.[51] Some have called for stronger defamation laws as a result of such incidents.[52]

Government prosecutors also pursued blogger Park Dae-sung on charges of "spreading false data in public with harmful intent" following his popular writings on economic matters during the 2008 economic crisis.[53] Using the pen name Minerva, Park had criticized government economic policy and gained notoriety for accurately predicting the fall of Lehman Brothers and the crash of the won.[54] Park was acquitted in 2009 and saw a subsequent appeal dropped following a December 2010 Constitutional Court ruling that struck down the law prohibiting the spread of "misleading information with the intention of damaging the public interest."[55] The court found that the definition of "public interest" was vague and that the law violated freedom of speech, although the government may still charge individuals with spreading misinformation under the NSL.[56]

On April 1, 2009, the National Assembly adopted a "three-strikes" approach to copyright infringement, particularly file sharing and downloading movie content.[57] In an amendment to Article 133 of the Copyright Law dealing with the "collection, abandonment, and deletion of illegal reproductions," the Minister of Culture, Sports, and Tourism would be authorized to shut down message boards that refuse to comply with more than three warnings to remove copyrighted content,[58] while users who upload such content may also have their accounts canceled.[59] These punitive measures could be taken regardless of whether a takedown request by a copyright holder has been issued.[60]

Social media sites whose "main purpose is to enable different people to interactively transmit works, etc. among themselves" are treated as "special types of online service providers" under Article 104 of the Copyright Law.[61] Under Article 104, providers are obliged to take "necessary measures" to intercept the illegal interactive transmission of copyrighted works upon the request of rights holders. Article 142(1) lays out fines to a maximum of KRW 30 million (USD 26,000) for these special providers who fail to take necessary measures, while other providers who "seriously damage" copyright enforcement as a result of their failure to take down reproductions or "interactive transmissions" are also subject to fines of up to KRW 10 million (USD 8,800).[62] Under the amended legislation, providers who have been fined under Article 142(1) twice and have failed to take necessary measures can be blocked upon the issuance of a third fine.[63]

South Korea's elections framework allows significant limits to be placed on political speech prior to and during elections in order to prevent corruption, promote equal opportunity, and minimize the "damages caused by distorted election news."[64] Elections are restricted by numerous detailed prohibitions on campaign-related activities that would be standard practice in many other democracies, including elected officials endorsing a candidate,[65] conducting public opinion polls within six days of an election,[66] setting limits on campaign locations, and posting campaign materials.

The election law also extends these restrictions to campaign activities conducted on information and communication networks. Article 93 of the Public Official Election Law makes it illegal for noncandidates to distribute information supporting, recommending, or opposing any political party or candidate.[67] Election commissions that discover such information posted online may demand that the Web site or hosting service delete, restrict, or suspend the relevant information.[68]

The NEC is responsible for controlling all aspects of Korean elections, from counting votes to monitoring the media and tracing campaign contributions.[69] The NEC has used its power to censor online media platforms to remove more than 100,000 election-related articles, comments, and blog entries from the Internet,[70] as well as more than 65,000 movies posted to video-sharing Web sites.[71] The NEC began censoring the Internet in the early 2000s, partly in reaction to the significant role the Internet played in the 2002 presidential election.[72] It currently has two divisions devoted to Internet regulation and censorship: the Internet Election News Deliberation Commission (IENDC),[73] which handles newspaper Web sites and other online media sources (or "Internet press"),[74] and the Cyber Censorship Team (CCT),[75] which monitors personal blogs, videos, message-board comments, and other Web sites.[76]

Violation of the law against advocating a candidate prior to the election period can be punished with a fine of up to KRW 4 million (USD 3,500) or two years in prison.[77] The line between campaigning and normal discussion is extremely vague, and the decision to censor is made at the discretion of the CCT's officers. This vagueness has had a chilling effect on online political discourse, especially on video-sharing sites, whose election-related content has been reduced to little more than videos produced by the campaigns themselves.[78] Between the 2002 and 2007 presidential elections, the total number of deletion requests for early campaigning skyrocketed, from 2,425 to 76,277.[79] Media have also reported that from June 2006 to May 2007, up to 19,000 online election-related messages were deleted, while the authors of 13 messages containing false rumors about candidates faced legal punishment.[80]

Several security incidents in late 2010 also led officials to crack down on the spread of misinformation online. In May 2010, a South Korean warship was sunk, an act widely labeled as North Korean provocation.[81] Despite an international investigation that found North Korea responsible, online discussion forums expressed doubt, suggesting the United States was to blame.[82] Government ministers responded by ordering

a crackdown on the spread of "groundless rumors" online about the incident and charged an individual with libel for criticizing military action before the sinking.[83] In addition, Defense Ministry personnel brought prominent bloggers, Twitter users, and reporters to view the wreckage in an attempt to combat skepticism.[84] South Korean military leaders warned of the potential for cyber attacks from the North during the country's hosting of the G20 Summit in early November 2010.[85] A similar crackdown was launched following the November 2010 North Korean shelling of the South Korean island of Yeonpyeong, with the Supreme Prosecutors Office launching investigations into online rumors and arresting several individuals.[86] The National Police Agency's cybercrime team also expanded their crackdown on online posts sympathetic to North Korea, forcing Web site operators to delete 42,787 messages between January and June 2010.[87]

Surveillance

The South Korean constitution guarantees that the privacy of citizens (Article 17) and the privacy of their correspondence (Article 18) shall not be violated.[88] While most scholars believe that Article 17 forms the basis of a right to privacy,[89] the Supreme Court has also held that together with Article 10, guaranteeing human dignity and the right to pursue happiness, "these constitutional provisions not only guarantee the right to be let alone, which protects personal activity from invasion by others and public exposure, but also an active right to self-control over his or her personal information in a highly informatized modern society."[90]

Internet service providers are generally directed to gather the minimum amount of information necessary and are restricted from disclosing personal information beyond the scope of notification or collecting certain personal information, such as "political ideology, religion, and medical records," that would likely infringe upon the user's privacy without consent.[91] However, these protections do not apply where special provisions apply or other laws specify otherwise.

Real-name registration requirements have been a part of the South Korean Internet landscape since 2003, when the MIC sought the cooperation of four major Web portals (Yahoo Korea, Daum Communications, NHN, and NeoWiz) in developing real-name systems for their users.[92] While implicating deeper privacy concerns, the purported goal of real-name measures is to reduce abusive behavior on the Internet. A number of prominent cases (such as the suicides of a number of actresses) have made this a major issue for the Korean public.[93]

In 2004 election laws began requiring individuals who post comments on Web sites and message boards in support of, or in opposition to, a candidate to disclose their real names.[94] In 2005 the government implemented a rule that required e-mail or chat-service account holders to provide detailed information, including name, address,

profession, and identification number.[95] This policy was tightened further by the MIC in July 2007 when users were required to register their real names and resident identification numbers with Web sites before posting comments or uploading video or audio clips on bulletin boards.[96] In December 2008, the KCC extended its reach to require all forum and chat room users to make verifiable real-name registrations.[97] Furthermore, an April 2009 amendment to the Information Act took effect, requiring Korea-domain Web sites with at least 100,000 visitors daily to confirm personal identities through real names and resident registration numbers.[98] Previously, real-name registration was required for news Web sites with more than 200,000 visitors a day or portals and user-generated content sites with over 300,000 daily visitors.[99] Rather than comply with the new registration system, Google disabled the features on the Korean-language YouTube site (http://kr.youtube.com) for uploading videos and comments.[100] The real-name registration provisions of the Public Official Elections Act were unsuccessfully challenged in July 2010 when the Constitutional Court found that the requirements did not violate principles against prior censorship and that they worked to prevent "social loss and side effects which arise out of the distortion of public opinion."[101]

In 2010, Facebook faced scrutiny from the KCC, which found that "Facebook violates the regulations on protection of privacy in information networks."[102] The KCC required Facebook to submit related documents and make improvements in line with the nation's Information and Communication Law—specifically Article 22 of the Act on Promotion of Information and Communication Network Utilization and Information Protection.[103] This article requires information and communication service providers to gain consent when gathering users' personal data.[104] Facebook indirectly responded by reciting the principle of its company that "the users have control of their personal information."[105]

Amendments to the 2007 Protection of Communications Secrets Act established extensive data retention requirements and expanded the government's surveillance capabilities.[106] These amendments require telecommunications companies and ISPs to retain access records and log files (including online transactions conducted; Web sites visited; time of access; and files downloaded, edited, read, and uploaded) for at least three months, along with date and time stamps, telephone numbers of callers and receivers, and GPS location information for 12 months.[107] The National Human Rights Commission of Korea (NHRCK) criticized these amendments, particularly the use of GPS information to locate users and the imposition of penalties for service providers who refuse to comply with requests for information despite existing provisions that allow gathering of evidence by search and seizure in ordinary investigations.[108]

In 2008, three years after a scandal over the illegal wiretapping of the cell phones of influential political figures forced them to destroy their equipment, the National

Intelligence Service asked for permission to resume the practice.[109] Messages sent by e-mail (after submission and receipt) are already considered by law enforcement authorities as "objects," subject to ordinary search and seizure requirements, rather than "means of communications" requiring wiretapping warrants and notification to parties within 30 days.[110]

ONI Testing Results

OpenNet Initiative testing conducted in 2010 found levels of filtering consistent with those of 2007–2008 testing: filtering in South Korea primarily targets social content and content related to conflict and security, particularly regarding North Korea.

In November 2010, ONI conducted testing on KT Corporation (formerly Korea Telecom), the biggest South Korean ISP. This testing found a select number of blocked Web sites, with the majority of blocked sites focused on issues related to North Korea. Additional blocking occurred with sites focused on dating, pornography, and gambling. These findings are closely consistent with the results of 2007–2008 ONI testing, with a marginal increase in the blocking of sites related to North Korea. New sites that were found to be blocked include North Korea's Twitter feed; however, a North Korea–focused YouTube channel and related Facebook pages were found to be accessible.

The method of blocking used by KT Corporation differed from past test results, although those results included the testing of additional ISPs not tested in this phase. While previous testing showed evidence of IP blocking and DNS tampering, the results of 2010 testing showed that filtering was carried out through HTTP Proxy blocking. Attempts to view these Web sites were redirected to a "block page" jointly hosted by Korea's National Police Agency and the KCSC.

In 2010, ONI testing found results consistent with those seen in 2007–2008, with evidence of filtering social content and content related to conflict and security. Although the overall rate of filtering is generally low, it is primarily targeted at content related to North Korea. In addition, the government's approach to regulating content is far more reliant on other measures, such as real-name registration, takedown orders, and laws prohibiting defamation and libel.

Conclusion

South Korea has one of the most advanced and connected Internet networks in the world. Its Internet speeds are the fastest, and its usage rates the highest. Nevertheless, South Korea's government imposes more constraints on the freedom of online speech than most other democratic countries. The wide range of information blocked, from elections-related discourse to discussion about North Korea, is subject to central

filtering and censorship. South Korea may represent the future of the Internet: it represents a society that is both highly tech savvy and heavily monitored. As more technology is introduced and the hostile confrontation between North and South is prolonged, the paradoxical mix of an expanded base for online expression and the restriction of online voices will continue in South Korea.

Notes

1. "South Korea Country Profile," BBC News, November 23, 2010, http://news.bbc.co.uk/2/hi/asia-pacific/country_profiles/1123668.stm.

2. Reporters Without Borders, *Enemies of the Internet—Countries under Surveillance,* http://www.rsf.org/IMG/pdf/Internet_enemies.pdf.

3. "Kim Dae-Jung: Dedicated to Reconciliation," CNN, June 14, 2001, http://archives.cnn.com/2001/WORLD/asiapcf/east/06/12/bio.kim.daejung/.

4. International Telecommunication Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers," 2009 Figures, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

5. Korea Internet and Security Agency, "2010 Survey on the Wireless Internet Usage Executive Summary," September 29, 2010, http://isis.kisa.or.kr/board/?pageId=060200&bbsId=3&itemId=788; Korea Internet and Security Agency, "Broadband Subscribers," http://isis.kisa.or.kr/eng/sub01/?pageId=010400.

6. Darren Allen, "South Korea Tops Akamai Broadband Averages with 17 Mbps," TechWatch, October 21, 2010, http://www.techwatch.co.uk/2010/10/21/south-korea-tops-akamai-broadband-averages-with-17mbps.

7. J.C. Hertz, "The Bandwidth Capital of the World," *Wired,* October 12, 2010, http://www.wired.com/wired/archive/10.08/korea.html.

8. National Internet Development Agency of Korea, "Survey on the Computer and Internet Usage," September 2008, http://isis.nida.or.kr.

9. National Internet Development Agency of Korea, "Korea Internet White Paper," 2010, http://isis.nida.or.kr/eng/ebook/ebook.html.

10. Paul Budde Communications Pty., Ltd., "South Korea Broadband Market—Overview and Statistics," July 24, 2010, http://www.budde.com.au/Research/South-Korea-Broadband-Market-Overview-Statistics-and-Forecasts.html.

11. Ibid.

12. Constitutional Court of Korea, Constitution of the Republic of Korea, Article 21, October 29, 1987, http://english.ccourt.go.kr/home/att_file/download/Constitution_of_the_Republic_of_Korea.pdf.

13. Ibid.

14. Ibid.

15. Telecommunications Business Act, wholly amended by presidential decree no. 13558 on August 10, 1991, Decisions of the Korean Constitutional Court, Opinion 14–1 KCCR 616, 99Hun-Ma480, June 27, 2002.

16. Ibid., Article 53(2).

17. Enforcement Decree of Telecommunications Business Act, Article 16, wholly amended by presidential decree no. 13558 on December 31, 1991, Decisions of the Korean Constitutional Court, Opinion 14–1 KCCR 616, 99Hun-Ma480, June 27, 2002, http://english.ccourt.go.kr/home/english/decisions/mgr_decision_view.jsp?seq=224&code=1&pg=1&sch_code=&sch_sel=sch_content&sch_txt=99Hun-Ma480&nScale=15.

18. Ibid.

19. Telecommunications Business Act, Law 4903, Article 53–2, January 5, 1995, http://www.itu.int/ITU-D/treg/Legislation/Korea/BusinessAct.htm.

20. "Decisions of the Korean Constitutional Court, Opinion 14–1 KCCR 616, 99Hun-Ma480," June 27, 2002, http://english.ccourt.go.kr/home/english/decisions/mgr_decision_view.jsp?seq=224&code=1&pg=1&sch_code=&sch_sel=sch_content&sch_txt=99Hun-Ma480&nScale=15.

21. Ibid.

22. Act on Promotion of Information and Communications Network Utilization and Information Protection, Law No. 8289, January 16, 2007, http://eng.kcc.go.kr/download.do?fileNm=TELECOMMUNICATIONS_BUSINESS_ACT.pdf; Privacy International and the GreenNet Educational Trust, "Silenced: An International Report on Censorship and Control of the Internet," September 2003, https://www.privacyinternational.org/survey/censorship/Silenced.pdf.

23. Ibid.

24. On its Web site, the Korea Communications Standards Commission defines illegal information as "all sorts of information against the positive law of the Republic of Korea, that is, information infringed upon the public interests and social orders." Korea Communications Standards Commission, "Subject of Report," http://www.singo.or.kr/eng/02_report/Subject_Report.php.

25. Ibid.

26. The NSL has been used to criminalize advocacy of communism and groups suspected of alignment with North Korea, although arrests under the NSL have become much less frequent in recent years. Nevertheless, the law continues to have a chilling effect on public discussion of North Korea and provides a justification for censorship of Web sites related to North Korea and communism. See Ser Myo-ja, "Security Law Marks 60 Years of Strife," *Korea JoongAng Daily*, September 1, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2894346; Human Rights

Watch, "Retreat from Reform: Labor Rights and Freedom of Expression in South Korea," November 1, 1990, http://www.hrw.org/en/reports/1990/11/01/retreat-reform; Brad Adams, "South Korea Should Act Like It Knows," Human Rights Watch, April 13, 2006, http://www.hrw.org/en/news/2006/04/12/south-korea-should-act-it-knows; Brad Adams, "South Korea: Defend Human Rights," Human Rights Watch, January 15, 2008, http://www.hrw.org/en/news/2008/01/22/south-korea-defend-human-rights.

27. National Security Law, Article 7(1). Unofficial English translation is available at: http://www.hartford-hwp.com/archives/55a/205.html.

28. The standard of harm in the Enforcement Decree of the Juvenile Protection Act (JPA) was developed from "criteria for deliberation of media materials harmful to juveniles," which include provocative, obscene, antisocial, violent, or unethical materials that may harmfully affect youths' mental and physical health. See http://www.ccourt.go.kr/home/english/decisions/mgr_decision_view.jsp?seq=224&code=1.

29. Adams, "South Korea: Defend Human Rights."

30. Act on Promotion of Information and Communication Network Utilization and Information Protection (2001), Article 42.

31. Act on Promotion of Information and Communication Network Utilization and Information Protection (2001), Article 42; *Korea Herald*, "45 Websites Violate Youth Law," March 31, 2009.

32. Korea Communications Standards Commission (KCSC), http://www.singo.or.kr/eng/01_introduction/introduction.php.

33. KISCOM's mandate was originally established through the creation of the ICEC in 1995. See http://www.itu.int/ITU-D/treg/Legislation/Korea/BusinessAct.htm.

34. KCSC, "Chronology," http://www.icec.or.kr/eng/01_About/Chronology.php.

35. Telecommunications Business Act (1995), Law 4903, Article 53–2, January 5, 1995, http://www.itu.int/ITU-D/treg/Legislation/Korea/BusinessAct.htm.

36. Ibid.

37. For an explanation of the reporting process of suspected illegal content, see KCSC, "Report Process," http://www.singo.or.kr/eng/02_report/Process.php.

38. KCSC, "Committees," http://www.icec.or.kr/eng/02_Operation/Committees.php.

39. KCSC, "Subject of Report," http://www.singo.or.kr/eng/02_report/Subject_Report.php; Reporters Without Borders, *South Korea—2004 Annual Report* (2004), http://en.rsf.org/report-south-korea,59.html.

40. "Decisions of the Korean Constitutional Court, Opinion 14–1 KCCR 616, 99Hun-Ma480," June 27, 2002, http://english.ccourt.go.kr/home/english/decisions/mgr_decision_view.jsp?seq=224&code=1&pg=1&sch_code=&sch_sel=sch_content&sch_txt=99Hun-Ma480&nScale=15.

41. Kim Hyung-eun, "Do New Internet Regulations Curb Free Speech?" *Korea JoongAng Daily*, August 13, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2893577.

42. Jung Ha-won, "Internet to Be Stripped of Anonymity," *Korea JoongAng Daily*, July 23, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2892691.

43. Michael Fitzpatrick, "South Korea Wants to Gag the Noisy Internet Rabble," *Guardian*, October 8, 2008, http://www.guardian.co.uk/technology/2008/oct/09/news.internet; Kim Tong-hyung, "Cabinet Backs Crackdown on Cyber-bullying," *Korea Times*, July 22, 2008, http://www.koreatimes.co.kr/www/news/biz/2008/07/123_28003.html.

44. Park Sung-woo, "Court Says Web Portals Are Responsible for Comments," *Korea JoongAng Daily*, April 18, 2009, http://joongangdaily.joins.com/article/view.asp?aid=2903746.

45. Lee Sang-bok, "New Regulations Proposed for Internet Postings," *Korea JoongAng Daily*, August 21, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2893939.

46. Kim Hyung-eun, "Do New Internet Regulations Curb Free Speech?"

47. Sung So-young, "Portals Beef Up Measures against Malicious Postings," *Korea JoongAng Daily*, October 23, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2896433.

48. Ser Myo-ja, "GNP Files Bills to Alter the Nation's Media Landscape," *Korea JoongAng Daily*, December 4, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2898166.

49. Lee Sang-eon and Chun In-sung, "Cyber Terror Sleuths Planning Internet Crackdown," *Korea JoongAng Daily*, October 6, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2895724.

50. In 2010, Tablo, the leader of a Korean hip-hop band called Epik High, faced months-long doubt and accusation over the accuracy of his school records. An Internet group called "We Urge Tablo to Tell the Truth (Tajinyo)" raised suspicion in a television documentary produced to reveal the truth of Tablo's Stanford degree. Although his graduation from Stanford University was later verified, in August 2010 Tablo filed a libel suit against the bloggers, and a police investigation was opened. See Park Si-soo, "Tablo-Bashing Website Shut Down," *Korea Times*, October 22, 2010, http://www.koreatimes.co.kr/www/news/nation/2010/10/117_75055.html; *Korea Herald,* editorial, "Virus of Distrust," October 17, 2010, http://www.koreaherald.com/opinion/Detail.jsp?newsMLId=20101010000069; Park Si-soo, "Police Confirm Singer Tablo Graduated from Stanford," *Korea Times*, October 8, 2010, http://www.koreatimes.co.kr/www/news/nation/2010/10/117_74232.html; Kim Yoon-mi, "Tablo's Diploma Confirmed," October 8, 2010, http://www.koreaherald.com/entertainment/Detail.jsp?newsMLId=20101008000688.

51. In 2008, actress Choi Jin-sil committed suicide after suffering online harassment. See Choe Sang-hun, "Korean Star's Suicide Reignites Debate on Web Regulation," *New York Times*, October 12, 2008, http://www.nytimes.com/2008/10/13/technology/internet/13suicide.html.

52. "A Law for Choi Jin-sil," *Korea JoongAng Daily,* October 4, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2895644.

53. Choe Sang-hun, "South Korea Frees Blogger Who Angered Government," *New York Times*, April 20, 2009, http://www.nytimes.com/2009/04/21/world/asia/21blogger.html; Oh Byung-sang, "After Minerva: Gaining Balance," *Korea JoongAng Daily*, April 24, 2009, http://joongangdaily.joins.com/article/view.asp?aid=2903946.

54. Ser Myo-ja, "Prognosticator 'Minerva' Is Acquitted by a Seoul Court," *Korea JoongAng Daily*, April 21, 2009, http://joongangdaily.joins.com/article/view.asp?aid=2903837.

55. Bae Ji-sook, "Prosecution Confirms 'Minerva' Innocent," *Korea Herald*, January 4, 2011, http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110104000750.

56. Song Jung-a, "South Korean Court Rules on Internet Law," *Financial Times*, December 28, 2010, http://www.ft.com/cms/s/0/38b354a4-126d-11e0-b4c8-00144feabdc0.html.

57. "South Korea Passes Three-Strikes Internet Piracy Law," IP World, April 15, 2009, http://www.ipworld.com/ipwo/doc/view.htm?id=217097&searchCode=H. http://news.softpedia.com/news/File-Sharers-Cornered-Again-84010.shtml.

58. Proposed Amendment to Copyright Law of Korea, July 2008, Article 133–2(3). Unofficial English translation is available at http://ipleft.or.kr/bbs/view.php?board=ipleft_5&id=488&page=1&category1=3.

59. Ibid.

60. Nate Anderson, "South Korea Fits Itself for a '3 Strikes' Jackboot," Ars Technica, April 15, 2009, http://arstechnica.com/tech-policy/news/2009/04/korea-fits-itself-for-a-3-strikes-jackboot.ars.

61. Copyright Law of Korea, Article 104, http://eng.copyright.or.kr/law_01_01.html.

62. Ibid., Article 142(1).

63. Proposed Amendment to Copyright Law of Korea, Article 133–2(4)(1).

64. National Election Commission, "About IENDC," http://www.nec.go.kr/engvote/about/iendc.jsp.

65. Public Official Election Law, Act No. 8879, February 29, 2008, Article 86, http://www.nec.go.kr/english/NEC/Public_Official_Election.zip. Former President Roh Moo-hyun was charged by the NEC and impeached for violating this law. He was later reinstated as president. See "Obituary: Roh Moo-hyun," BBC News, May 23, 2009, http://news.bbc.co.uk/2/hi/asia-pacific/2535143.stm.

66. Public Official Election Law, Article 108.

67. Ibid., Article 93.

68. Ibid., Articles 82–84 (3–5).

69. ONI interview with an official from the IENDC.

70. National Election Commission, "The Overview of Cyber Crackdown Service Related to the 18th National Election."

71. Bruce Wallace, "Emotions Don't Reach S. Korea Voters," *Los Angeles Times*, December 15, 2007, http://articles.latimes.com/2007/dec/15/world/fg-korea15.

72. "The 2007 Korean Presidential Elections and Internet Censorship," Internet and Democracy Blog, January 16, 2008, http://blogs.law.harvard.edu/idblog/2008/01/16/the-2007-korean-presidential-elections-and-internet-censorship/.

73. The IENDC's mission is to ensure that newspaper Web sites, online news agencies, and other semiofficial online news sources are impartial in their campaign coverage and do not violate election laws. The IENDC has a great deal of discretion to decide what constitutes a violation of these rules and to censor the Internet press accordingly. Generally, it does so by contacting the relevant Internet press organizations and telling them to change their content or to issue a correction. See National Election Commission Web site, "About IENDC," http://www.nec.go.kr/english/NEC/nec_IENDC01.html.

74. Public Official Election Law, Article 8–5(1). According to the NEC, IENDC bans the Internet media from doing the following: (1) Reporting on public opinion polls during the two- to three-week election period, or reporting on polls during any other period in a way the IENDC considers biased or inaccurate; (2) using headlines that "reduce, overstate or distort" election-related news; (3) reporting "distorted or false" news by "overstating, highlighting, cutting or hiding important facts that may have substantial impacts on the decisions of voters"; (4) falsely attributing any statements or other actions to candidates or political parties; (5) misinforming voters with reports on election results estimated without any reasonable basis; (6) failing to draw a sharp line between facts and opinions; (7) failing to equally represent different points of view when asking candidates or other people for their opinions; (8) modifying pictures or videos to create a negative portrayal of a candidate; (9) allowing opinion advertisements that support or oppose a particular party or candidate. See National Election Commission Web site, Internet Election News Deliberation Commission Regulation No. 1, Articles 1–18.

75. Since it started in 2002, the CCT polices blogs, personal Web sites, video postings, and message boards. Its three main tasks are to prevent damaging and untrue statements about candidates during an election, to maintain the prohibition against campaigning outside of election periods, and to ensure that all users make comments during an election with only their full, real names. All three tasks are usually executed by requesting that the Web site's hosting service delete or change offending content, potentially opening an investigation, and pressing charges if the hosting service refuses (ONI interview with an official from the Cyber Censorship Team). Monitoring is carried out by about 1,000 part-time workers who are hired nationwide 120 days before every election to run a search program to find and flag suspicious content (ONI interview with IENDC official).

76. ONI interview with an official from the Cyber Censorship Team.

77. Offending acts include posting long opinions of political parties on Web portals and Web sites, posting comments on online news articles, or any similar acts on personal Web sites or

blogs. However, the NEC has stated that "there is small chance that citizens will face legal charges for posting their opinion as they will be viewed flexibly in actual crackdowns." See Shin Hae-in, "Korea: Controversy Mounts over Ban on Internet Election," *Korea Herald*, June 25, 2007, http://www.asiamedia.ucla.edu/print.asp?parentid=72445.

78. Wallace, "Emotions Don't Reach S. Korea Voters."

79. Yoo Jae-il, Sohn Byung-kwon, et al., 'The 18 Political Scientists' Participatory Observation of the 18th Korean National Assembly Election in 2008," Purungil.

80. Shin Hae-in, "Korea: Controversy Mounts."

81. "Times Topics—he Cheonan (Ship)," *New York Times*, May 20, 2010, http://topics.nytimes.com/top/reference/timestopics/subjects/c/cheonan_ship/index.html.

82. Christian Oliver, "South Koreans Fear Unmasking of Online Critics," *Financial Times*, July 8, 2010, http://www.ft.com/cms/s/0/af902db6-8aac-11df-8e17-00144feab49a.html.

83. Bae Ji-sook, "Government Warns against 'Groundless Rumors,'" *Korea Times*, May 20, 2010, http://www.koreatimes.co.kr/www/news/nation/2010/05/117_66222.html.

84. Christian Oliver and Kang Buseong, "Seoul Turns to Twitter to Combat Skeptics," *Financial Times*, May 31, 2010.

85. Jung Sung-ki, "Military Leaders Warn of NK Cyber Attack," *Korea Times*, June 8, 2010, http://www.koreatimes.co.kr/www/news/nation/2010/06/113_67314.html.

86. Bae Ji-sook, "Prosecution Investigates Groundless Rumormongers," *Korea Times*, November 24, 2010, http://www.koreatimes.co.kr/www/news/nation/2010/11/117_76912.html.

87. Lee Tae-hoon, "Censorship on Pro-NK Websites Tight," *Korea Times*, September 9, 2010, http://www.koreatimes.co.kr/www/news/nation/2010/09/113_72788.html.

88. Constitution of the Republic of Korea, Articles 17–18, http://english.ccourt.go.kr/home/att_file/download/Constitution_of_the_Republic_of_Korea.pdf.

89. Soon Chul Huh, "Invasion of Privacy v. Commercial Speech: Regulation of Spam with a Comparative Constitutional Point of View," *Albany Law Review,* 2006, *70 Alb. L. Rev. 181.*

90. 96 Da 42789 (S. Korea 1998).

91. Act on Promotion of Information and Communications Network Utilization and Information Protection, Articles 22–24.

92. Winston Chai, "Real User IDs on Chat Groups: Korean Govt," ZDNet Asia, May 23, 2003, http://www.zdnetasia.com/real-user-ids-on-chat-groups-korean-govt-39133165.htm.

93. Choe Sang-Hun, "Web Rumors Tied to Korean Actress's Suicide," *New York Times*, October 2, 2008, http://www.nytimes.com/2008/10/03/world/asia/03actress.html.

94. Public Official Election Law, Article 82–6.

95. "Internet Real-Name System Boosts Cyber Security in S Korea," Xinhua, April 24, 2008, http://news.xinhuanet.com/english/2008-04/24/content_8039953.htm.

96. "Web Identification System Not Effective," *Korea Herald,* July 3, 2007.

97. Brian Lee, "What Happens When Intelligence Fails," *Korea JoongAng Daily,* September 28, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2895216; Fitzpatrick, "South Korea Wants to Gag the Noisy Internet Rabble."

98. Antone Gonsalves, "Google Scales Back YouTube Korea," *Information Week*, April 13, 2009, http://www.informationweek.com/news/internet/google/showArticle.jhtml?articleID=216500489; Martyn Williams, "Google Disables Uploads, Comments on YouTube Korea," *PC World*, April 13, 2009, http://www.pcworld.com/article/162989/google_disables_uploads_comments_on_youtube_korea.html.

99. Kim Hyung-eun, "Do New Internet Regulations Curb Free Speech?" *Korea JoongAng Daily,* August 13, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2893577.

100. Gonsalves, "Google Scales Back YouTube Korea."

101. Constitutional Court of Korea, "Real Name Verification of the Internet News Site Case," February 25, 2010, http://www.ccourt.go.kr/home/english/decisions/rcnt_decision_view.jsp?seq=513&pg=1&sch_sel=&sch_txt=&nScale=15&sch_code=9.

102. Martyn Williams, "Facebook in Breach of Korean Privacy Laws, Says Regulator," *Computer World*, December 8, 2010, http://www.computerworld.com/s/article/9200458/Facebook_in_breach_of_Korean_privacy_laws_says_regulator.

103. Act on Promotion of Information and Communications Network Utilization and Information Protection, Article 22, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf; Lee Min-hyung, "The KCC's Facebook Tackling," Digital Daily, December 14, 2010, http://www.ddaily.co.kr/news/news_view.php?uid=72089.

104. Ibid.

105. Jung Yuni, "Youtube, Facebook Sweating Hard Due to the Korean Market," ZD NET Korea, December 14, 2010, http://www.zdnet.co.kr/ArticleView.asp?artice_id=20101214153147.

106. "PHR2006—Republic of (South) Korea," Privacy International, December 18, 2007, https://www.privacyinternational.org/article/phr2006-republic-south-korea.

107. Asian Legal Resource Centre, "South Korea: Concerns about the Freedom of Expression and the Possible Resumption of Executions," June 4, 2009, http://www.alrc.net/doc/mainfile.php/alrc_st2009/562/http://www.humanrights.go.kr/english/activities/view_01.jsp?seqid=713&board_id=Press%20Releases.

108. National Human Rights Commission of Korea, "NHRCK Announces Opinion on Proposed Amendments to the Protection of Communications Secrets Act," January 30, 2008, http://www.humanrights.go.kr/english/download.jsp?board_id=Press%20Releases&filename=Communications%20Secrets%20Act.doc.

109. Brian Lee, "What Happens When Intelligence Fails," *Korea JoongAng Daily,* September 28, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2895216; "S. Korean Spy Agency Admits Conducting Illegal Wiretapping," *People's Daily*, August 5, 2005, http://english.people.com.cn/200508/05/eng20050805_200519.html.

110. "Prosecutors Have Indiscriminate Access to Personal Email Communications," The Hankyoreh, April 24, 2009, http://english.hani.co.kr/arti/english_edition/e_national/351496.html.

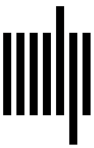
Access Contested

Security, Identity, and Resistance in Asian Cyberspace

Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

Citation:

Access Contested: Security, Identity, and Resistance in Asian Cyberspace
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/9780262016780.001.0001
ISBN (electronic): 9780262298919
Publisher: The MIT Press
Published: 2011



The MIT Press

The online edition of this work is available from IDRC and at http://www.access-contested.net.

International Development Research Centre
PO Box 8500, Ottawa, ON K1G 3H9, Canada
info@idrc.ca / www.idrc.ca <http://www.idrc.ca>
ISBN 978-1-55250-507-6 (IDRC e-book)

This book was set in Stone Sans and Stone Serif by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access contested : security, identity, and resistance in Asian cyberspace / edited by Ronald Deibert . . . [et al.].
p. cm. — (Information revolution and global politics)
Includes bibliographical references and index.
ISBN 978-0-262-01678-0 (hardcover : alk. paper) — ISBN 978-0-262-51680-8 (pbk. : alk. paper)
1. Cyberspace—Government policy—Asia. 2. Computer security—Asia. 3. Computers—Access control—Asia. 4. Internet—Government policy—Asia. 5. Internet—Censorship—Asia. I. Deibert, Ronald.
HM851.A253 2011
303.48′33095—dc23

2011031273

10 9 8 7 6 5 4 3 2 1