Korea case study on private actors' roles in protecting online human rights

Kyung Sin Park, Open Net Korea[1]

1. Overview of Intermediaries Landscape in Korea

This chapter surveys the special characteristics of the Korean market and regulations.

Some local platforms in areas such as, blogging, search engines, and chatting outperform global ones like Google, WhatsApp, while social networking sites (SNS) are dominated by Facebook and Twitter. As will be seen, domestic intermediaries' behavior differs widely from those of global intermediaries operating in the Korean market.

Local platforms, as opposed to global platforms, are subject to paternalistic regulations. This explains much of the difference in behavior between local and global intermediaries. We will examine some regulations here, while we will examine others in subsequent chapters.

a. Market survey

As of 2013, Korea had a total population of about 48 million people (83% urban) with an Internet penetration rate of 84%, mobile penetration rate of 110%[1], mobile Internet penetration rate of 75%, and a Facebook penetration rate of 27%[2]. See below for a comparison to Japan, U.S., and the world average.

	Korea	Japan	US	World average
Population	48 million	127 million	312 million	
Internet penetration	84%	79%	80%	52%
Mobile penetration	110%	109%	103%	93%
Internet mobile penetration	75%	48%	60%	21%
Facebook penetration	27%	17%	56%	

[2] We Are Social Singapore, "Global Digital Statistics 2014" (January 2014) at 146, online: <http://www.slideshare.net/wearesocialsg/social-digital-mobile-around-the-world-january-2014>.

Korea's major intermediaries for each type are as follows:

(1) Search engines: Naver, the local portal, has maintained 73% of the market share. Daum, the second largest local portal, has about 21%, with Google covering the small remainder of 3% (December 2012).[3]

(2) Micro-blogging: Twitter almost monopolizes the market, but if you include non-micro blogging, some estimates hold that Naver covers 80% of domestic bloggers.[4] In 2007, Naver already topped user visits per month[5] and its dominance has grown since then.

(3) Social Media: 31.3% of all people use SNS (this increased by 7.8% in 2013, and is very fast-growing). Based on the number of accounts, 55.4% use Kakao Story[6], 23.4% use Facebook, 13.1% use Twitter, and as of January 2014[7] 5.5% use Cyworld[8] (SK Communications). However, I personally think that the Kakao Story numbers are exaggerated because users were given the Story accounts by default due to their membership with Kakao Talk, the dominant private messaging service where past postings remain online for future "friends" to see and not really a social "networking" service. Weighing the time spent using the services, I believe that Facebook is by far the most widely used social *networking* service in Korea. This is quite a change from 2010 when Cyworld accounted for 50% of social media users.[9] Not including messaging services, the rankings are as follows:

---

[3] Ministry of Science, ICT and Future Planning and Korea Internet & Security Agency, "2013 Korea Internet White Paper", at 180, online: <http://isis.kisa.or.kr/ebook/WhitePaper2013.pdf>.

[4] There does not seem to be statistics tracking blogging or micro-blogging separately. "80%" is usually tossed around by Internet pundits who seem to derive that number from the search engine market share for the reason that bloggers are likely to expect search engines to promote the blogs on their own services and therefore likely to use the blog platform affiliated with the most popular search engine Naver.

[5] Nielson Korean Click Co., Ltd., "Domestic Blogging Services: Growth and Change" (14 November 2007), online: <http://www.koreanclick.com/information/info_data_view.php?id=189>

[6] An Instagram-like SNS launched by Kakao Talk, the dominant private messaging service.

[7] Korea Information Society Development Institute, KISDI Stat Report "SNS Usage Analysis (SNS 이용추이 분석)" (26 December 2013), online: <http://www.kisdi.re.kr/kisdi/fp/kr/publication/selectResearch.do?cmd=fpSelectResearch&curPage=1&sMenuType=3&controlNoSer=43&controlNo=13270&langdiv=1&searchKey=TITLE&searchValue=sns&sSDate=&sEDate=>.

[8] A My Space-like service launched by the SK conglomerate. This remains the only non-telco intermediary founded by Korean chaebols.

[9] Ministry of Culture, Sports and Tourism, online: <http://m.korea.kr/newsWeb/ml/policyView.do?newsDataId=148703840&currPage=61>.

South Korea SNS 2014: Own an Account (Monthly Active User)
Any SNS 84% (48%)
Facebook 75% (36%)
Twitter 56% (22%)
Google+ 38% (7%)
Me2Day 33% (7%)[10]

(4) Private messaging: Kakao Talk has a 92% market share.[11]

(5) User Created Video Content: YouTube has a 75% market share, but only in video content.[12]

(6) Platform: Google Play has 75.2%, due to the dominance of Samsung (100% of Samsung is Android) in the Korean phone market (Apple 17.9%, Blackberry and Windows each 4%)[13]

As part of the overall Internet economy, the mobile Internet is most often used for search (96.8%), and second most for SNS (50.4%), shopping (36.4%), banking (33.1%), etc. Time-weighted, it is used most for chatting (81.2%), phone calls (visual incl.) (69.7%), texting (69.%), and searches (42.8%).[14]

As expected, the top reasons for use of mobile Internet are not typical revenue-generators like search engines, microblogging sites, social media, messaging, etc., but are game companies. Below are the revenues of the top 10 Internet companies in Korea:

Top 10 Internet companies (by revenue)
Naver (2.3 billion USD)
Nexon (1.6 billion USD)
NCSoft (750 million USD)
NHN Entertainment (640 M)
eBay(640 M)
Daum (530 M)
Net Marle (497 M)
Neo Wiz (443 M)
Smilegate (360 M)
Wemade (227M)[15]

---

[10] *Supra* note 2 at 148.
[11] Newsis, "Kakao Talk's Market Share at 92%...Bandwagon Effects in Mobile Messenger Service, Twice That of Mobile Telecom" (23 September 2014), online: <http://www.newsis.com/ar_detail/view.html?ar_id=NISX20140923_0013187317&cID=10402&pID=10400>.
[12] Newsis, "YouTube, Clearing the Video Market Thanks to Mandatory Identification Rule" (9 October 2013), online: <http://www.newsis.com/ar_detail/view.html?ar_id=NISX20131009_0012419136&cID=10301&pID=10300>.
[13] *Supra* note 3 at 29.
[14] Korea Internet and Security Agency, "Year 2013 Mobile Internet Usage Survey (모바일인터넷이용실태조사)" (15 January 2014), online: <http://isis.kisa.or.kr/board/index.jsp?pageId=040000&bbsId=7&itemId=801&pageIndex=1>.
[15] "2013 Internet Industry, Top 10 Revenue Generators" *Under the Radar* (7 March 7 2014) (Blog), online: <http://undertheradar.co.kr/2014/03/07/114-2013-%EC%9D%B8%ED%84%B0%EB%84%B7%EC%97%85%EA%B3%84-%EB%A7%A4%EC%B6%9C-top10/>.

Notice that out of the 10 companies the majority are game companies. Only Naver and Daum are portals. Facebook, Twitter (SNS), and Kakao are not major revenue-generators, while Google Play revenues are also not significant.

b. Social significance of different intermediaries

In non-economic terms, certain intermediaries are more relevant than others, for example in terms of market share, popularity, usage patterns, and their impact on society. Naver and Daum curate and present news agencies' news on their own pages; and host original user-created discussion pages, blogs (Naver), and cafe pages (Daum), which have become major platforms for political debate. Facebook has become the socializing platform of choice for both conservative and progressive circles. Twitter, the main battleground for political discussions, became even more famous when it was later revealed that National Intelligence Services, the country's intelligence agency, had conducted major public-opinion-manipulation campaigns using Twitter before and during the Presidential election period in 2012.[16]

In late 2014, the Korean intermediary and dominant messenger service provider, Kakao Talk, became the center of public attention when the Prosecutors' Office announced a new campaign to track down and indict postings "causing division in national unity and skepticism of the government" for criminal defamation. The Prosecutors' Office mentioned Kakao Talk as a possible target for such search and seizure, shocking the entire nation, 90% of who use Kakao Talk as a private messenger service. Many users 'migrated' to a foreign service, Telegram, whose server is located overseas and apparently safe from Korean authorities' search and seizure.[17]

c. State paternalism

Indeed, one significant factor affecting online intermediaries is state paternalism, which pervades the country's industrial institutions and practices. For instance, all Internet companies with capital larger than about 100,000 USD are required to register and are given a "value-added telecommunication business" number, which can be taken away if they do not operate in compliance with the government's laws and regulations, or their operation "significantly hurts consumers' interests".[18] This environment creates a cloud under which the domestic companies feel pressure to comply with even extra-legal guidance from the government. For instance, as you will read below, the "temporary take-down" regulation can be read to be only *optional*, but it effectively works as if it is mandatory. This is true of other "optional" regulations, such as the Korea Communication Standards Commission's "correction requests (to take down contents)"[19] and warrantless subscriber data requests, where the compliance rates were respectively almost 100% until

---

[16] "Prosecutors Detail Attempt to Sway South Koran Election" *The New York Times* (21 November 2013), online: <http://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html?_r=0>.

[17] "Why South Koreans are Fleeing the Country's Biggest Social Network" *BBC* (10 October 2014), online: <http://www.bbc.com/news/blogs-trending-29555331>.

[18] *Telecommunications Business Act*, Article 27 Paragraph 2 (Korea).

[19] K.S. Park, "Administrative Internet Censorship by KCSC" *Open Net (Korea)*, online: <http://opennetkorea.org/en/wp/administrative-censorship>.

a huge judgment came down on the latter in October 2012 in a consumer lawsuit filed by PSPD Law Center.[20]

d. Foreign companies

The regulations, hard and soft, apply in theory equally to Facebook, Twitter, Google, and Microsoft. They all have local offices, but their servers are located overseas, exempting the owners from local income tax liabilities. The extraterritoriality of the servers has also provided a rationalization for the fact that the government has not applied various intermediary regulations to these overseas providers, creating what domestic competitors decry as "reverse-discrimination".[21] The most infamous domestic-only regulation was mandatory identity verification rule, which was only snubbed by overseas providers before it was struck down in 2012 in a constitutional challenge filed by PSPD Law Center.[22]

2. Content removal in response to administrative censorship

- Law: Korean Communication Standards Commission issues more than 100K "correction requests" (takedown requests) each year to platforms and telecoms that are not binding.
- Intermediaries' behavior: "Correction requests" are nearly always complied with. Intermediaries have been questioned on their attitudes toward consumers because of this high compliance rate. Here, we will evaluate the laws on administrative censorship and how the intermediaries' cooperation consummated their censorial effects.
- Civil Society: We will cover recent lawsuits and legislative efforts that have focused on and revealed the de facto binding force of "correction requests" and how to control them.
- Lessons: We will examine questions, such as: Should intermediaries be sanctioned for taking down excessive takedown requests or should be given immunity since they are following government requests? Should intermediaries be required to give posters a chance to rebut before complying with correction requests?

a. Law

Korea Communication Standards Commission (KCSC) is the administrative body that monitors and censors Internet content in Korea. KCSC's Internet censorship is vigorous[23]: it

---

[20] K.S. Park, "Internet Surveillance in Korea 2014" *Open Net (Korea),* online: <http://opennetkorea.org/en/wp/main-privacy/Internet-surveillance-korea-2014>. I had the fortune of initiating and directing the legal campaign for the lawsuit, which is now pending in the Supreme Court.

[21] "'Reverse Discrimination': Korean ICT Companies Suffering from Reverse Discrimination due to Governmental Regulations" *Business Korea* (1 January 2014), online: <http://www.businesskorea.co.kr/article/2274/%E2%80%9Creverse-discrimination%E2%80%9D-korean-ict-companies-suffering-reverse-discrimination-due>.

[22] Constitutional Court's Decision 2010 Hunma 47, 252 (consolidated) announced August 28, 2012; K.S. Park, "Korean Internet Identity Verification Rule Struck Down Unconstitutional; 13 Highlights of the Judgement" (24 August 2014) (Blog), online: <http://m.blog.naver.com/kyungsinpark/110145810944>.

[23] The Internet Sub-Committee draws five Commissioners (three from the ruling party, and two from the opposition) to meet twice every week to deliberate upon 1,000-2,000 websites, webpages, or social media accounts. About 40 people are dedicated to reviewing and preparing the material to be deliberated upon so that

blocked 39,296 web sites or pages based on overseas servers and deleted 17,827 domestic-server-based websites or pages in 2012,[24] ostensibly to protect its 50 million people.[25] The total number of blocking or deleting reached 104,400 in 2013. In comparison, the counterpart Australian Communication and Media Authority (ACMA)[26] has only blocked about 500 web sites or pages each year in 2012-2013[27], in service of its 22 million people. Per capita, KCSC censored about 50 times more than ACMA did in 2012 and 100 times more than ACMA in 2013.

KCSC's reach is broad and comprehensive, covering beyond obscenity/prostitution (19.6%), drugs (35.3%), and gambling (33.6%). It reaches defamation (8.6%)[28] and "any information intended for, aiding or abetting any crime" (2.8%), two categories obviously open to government abuse where, for instance, ACMA's activities focus on child pornography (55%) and almost always relate to sex-related content (99%).[29]

KCSC's censorship is carried out under Article 44-7 of the *Act Regarding Promotion of Use of Information Communication Networks and Protection of Information* (hereinafter, "*Information Communication Network Act"* or "*Network Act"*),[30] which authorizes KCSC to issue "deliberations" on nine categories of unlawful information: obscenity, defamation, stalking, and any information aiding and abetting a crime, etc. It is also carried out under Article 21 of the *Act Establishing Korean Communication Commission* (hereinafter, "*KCC Establishment Act*"),[31] which authorizes KCSC to issue "corrective requests" "when it is necessary for nurturing sound communication ethics." This law freely allows KCSC to censor even lawful content, however, KCSC has relied exclusively on corrective requests and has yet to make a single official take-down decision that triggers KCC enforcement.

KCSC ostensibly tried to concretize the standard of "sound communication ethics" by promulgating the Rules of Deliberation that it claims to abide by during deliberation on particular postings, but the Rules are not helping. What follows are some of the categories of material identified to be fit for takedowns in the Rules for Deliberation:

- Material promoting "superstitions and other unscientific attitudes of life";
- Material "mispresenting school education and clearly harming educational spirits";
- Material clearly capable of "causing social disorders".

Indeed, KCSC's non-binding corrective requests are aimed at content that is not unlawful in

---

the Commissioners can make efficient decisions, spending less than second on each.

[24] Korea Communications Standards Commission, online: <http://www.kocsc.or.kr/02_infoCenter/info_Communition_List.php>.

[25] This number is increasing. The current number is the result of a gradual increase from Lee Myung-Bak's tenure when KCSC issued more than 32,640 corrective requests for about 1.5 year period between May 2008 and December 2009.

[26] Australian Communications and Media Authority, online: <http://www.acma.gov.au/>.

[27] Interview with ACMA official, Jeremy Fenton, on November 2013.

[28] Korea Communications Standards Commission, "Annual Report 2012", online: <http://www.kocsc.or.kr/>.

[29] Australian Communications and Media Authority, *Annual Report 2009-2010* (October 2010) at 87.

[30] *Act on Promotion of Information and Communications Network Utilization and Information Protection*, online: <https://elaw.klri.re.kr/kor_service/lawPrint.do?hseq=18719>.

[31] *Act on the Establishment and Operation of Korea Communications Commission*, online: <https://elaw.klri.re.kr/kor_service/lawPrint.do?hseq=28155>.

any sense other than violating 'sound communication ethics'. There are plenty of examples that can be found on my blog[32], including a parody video of the famous Reza Farazman's <Little Hippo and Little Train>.[33] There are other examples where postings are taken down even when their legitimacy is apparent. KCSC took down certain pages of an elementary student's blog for describing an experiment whereby he tried to obtain propulsion for a projectile, using black powder.[34] Other entries on the student's blog showed that he had aspirations to become an astronaut or a space scientist. His descriptions were very non-technical, similar to cook books describing how many teaspoons of salt you need for a cup of soup and the experiment failed, so there was not even an explosion or propulsion. KCSC decided to take down the blog pages, citing the *Guns Swords and Explosives Control Act* provisions requiring special licenses for handling the named articles and pointing out that the student did not have the requisite license. However, these are experiments routinely done at schools without any license by teachers and students. Another example is when a Twitter account titled 2MB18NOMA was blocked by KCSC for the reason that the phonetic values of the account name closely track an epithet against the then President Lee Myung-Bak. There was no statutory provision claimed by KCSC to have been violated by that Twitter account.[35] In July 2014, KCSC blocked supposed photographs of the dead body of a person identified as the owner of the Sewol ferry that sank tragically taking 300 or so lives.[36] The state's incompetent rescue efforts to the tragedy angered many citizens, who were also skeptical of the state's investigations into the ferry's owners. The photos raised more questions and sparked the vigorous exchange of opinions on their veracity.[37] An administrative lawsuit is pending on those blockings.[38]

b. Intermediaries' behavior

The reason that KCSC exclusively uses non-binding corrective requests and does not make official takedown decisions is to avoid giving due process to the posters. KCSC is required to give the posters and the intermediaries a notice and a hearing before taking official disciplinary action[39] and KCC is also required to give another notice and a hearing before enforcement.[40] However, as long as the intermediaries comply with "corrective requests" (not an official disciplinary action), as they are now, KCSC can bypass all of these procedural safeguards. This allows them to take down content without any opposition, as they are able to hold deliberation meetings outside the eyes of the person most interested in the decision: the poster of the material.

---

[32] K.S. Park, *Naver* (Blog) at "English", online: <http://blog.naver.com/kyungsinpark/>.
[33] K.S. Park, "Censorer's Diary #26 Korean Video Parody of Hippo and Train Taken Down by KCSC" (8 June 2012) *Naver* (Blog), online: <http://blog.naver.com/kyungsinpark/110140161605>.
[34] K.S. Park, *Naver* (Blog), online: <http://blog.naver.com/kyungsinpark/110137736421>.
[35] Harlan, "In S. Korea, A Shrinking Space"; Louisa Lim, "In South Korea, Old Law Leads To Crackdown" (1 December 2011) *National Public Radio (NPR)*, online: <http://www.npr.org/2011/12/01/142998183/in-south-korea-old-law-leads-to-new-crackdown>.
[36] (29 November 2014), online: <http://transparency.or.kr/cases/977>.
[37] "Cause of South Korean Ferry Owner's Death Not Clear" *Business Standard* (25 July 2014), online: <http://www.business-standard.com/article/news-ians/cause-of-south-korean-ferry-owner-s-death-not-clear-114072500343_1.html>.
[38] http://opennet.or.kr/7734
[39] *Supra* note 34 at Article 25.
[40] *Supra* note 33 at Article 44-7, Paragraph 4.

In theory, intermediaries can refuse to comply with corrective requests, but the compliance rate is effectively 100%[41]. Only those corrective request with typological errors (i.e. wrong URLs) are not complied with. The only recorded moment of intermediaries' refusal was in July 2010, when the Korea Internet Self-Governance Organization (KISO, a voluntary alliance of the four major search portals: Daum, Naver, Google, and Nate) publicly announced that it would not comply with KCSC's requests to take down user-created material that raised questions about the government's explanations of the sinking of ROKS Corvette Choenan.

Most Internet content is being taken down by KCSC without any notice given to the authors of the postings, so that the authors cannot take any action to contest the takedowns before or after. Only the intermediaries receive the notice (domestic Internet companies hosting the material in the case of delete requests, and telecoms in the case of block requests issued against the content on foreign Internet companies' servers). As is the case around the world, the intermediaries usually do not have incentive to contest takedown orders from the government. The reality is that no intermediary has ever challenged a KCSC's decision in court. This is most likely because they do not have interest in individual postings, and also because they do not want to irk the government officials. Very few posters (less than a handful a year out of more than 100,000 posting takedowns) have challenged a KCSC take-down, because they are not notified of the hearing or decision.

The number of objections filed is very small compared to the number of takedowns, less than 0.01%, for the obvious reason that most users do not know when the takedown has taken place. Only a very small number of the people monitoring their postings constantly will have that knowledge. The number is so small that the statistics available on KCSC's website do not even include it, which is not surprising because KCSC's User Rights' Division only maintains statistics on people who filed complaints on the contents,[42] suggesting posters are not considered the users. This means that administrative censorship is conducted unchecked by any other entity, as aspect EFF calls "secret censorship".[43]

There is also content that has been taken down that would have been willingly modified by the poster if they had been properly notified, thereby avoiding the take-down of all the material. For instance, an entire Naver blog maintained by a 60 year old man was shut down by KCSC for the reason that out of 132 entries, about 30% of them included content honoring and encouraging North Korea, which is illegal under the infamous *National Security Act*.[44] About 50% of the entries were photos of his grandchildren and his paintings, music files containing his own compositions and songs, and cooking recipes, accumulated over 3-4 years in probably what people can naturally expect to be his biological final years. Had he been notified, it is likely he would have taken accommodative actions, such as delete all pro-North statements in order to protect the legal content, or at least he would have been able to back-up all the blog content.

---

[41] *Supra* note 31.
[42] http://www.kocsc.or.kr/02_infoCenter/info_UserTrand_List.php
[43] Rainey Reitman and Jillian York, "In South Korea the Only Thing Worse Than Online Censorship is Secret Online Censorship" *Electronic Frontier Foundation* (6 September 2011), online: <https://www.eff.org/deeplinks/2011/08/south-korea-only-thing-worse-online-censorship>.
[44] K.S. Park, (27 August 2011) *Naver* (Blog), online: <http://blog.naver.com/kyungsinpark/110117052953>.

Fortunately, in 2014, the law was changed to require giving notice to the user-authors, but that are many exceptions.[45]

d. Lessons and Analysis

The central pillar of KCSC censorship is the fact that intermediaries comply with corrective requests. If they do not, KCSC would be forced to issue official takedown decisions, which require giving the posters due process. If 1% of the people who were given notice chose to appear for their hearing, about 1,000 people would show up each year, slowing down the process of takedowns considerably. What is more, those faced with takedown notices could challenge, possibly with their lawyers, KCSC's extra-legal standards that they have been warned against twice by the Constitutional Court.

So why do intermediaries comply? Does the fact that the entire phenomenon is voluntary on the part of intermediaries exonerate KCSC? We need clear guidance on this issue. The U.S. Supreme Court did not think so in *Bantam Books v. Sullivan*, which is described by the minority in its successor, *Alexander v. United States*[46]:

> It is a flat misreading of our precedents to declare as the majority does that the definition of a prior restraint includes only those measures which impose a legal impediment, *ante,* at 2771, on a speaker's ability to engage in ***future*** expressive activity. *Bantam Books, Inc. v. Sullivan,* 372 U.S. 58, 70, 83 S.Ct. 631, 639, 9 L.Ed.2d 584 (1963), best illustrates the point. There a state commission did nothing more than warn book-sellers that certain titles **(*already being sold on market)*** could be obscene, implying that criminal prosecutions could follow if their warnings were not heeded. The commission had no formal enforcement powers, and failure to heed its warnings was not a criminal offense. Although ***571** the commission could impose no legal impediment on a speaker's ability to engage in future expressive activity, we held that scheme was an impermissible system of prior administrative restraints. *Ibid.* There we said: We are not the first court to look through forms to the substance and recognize that informal censorship may sufficiently inhibit the circulation of publications to warrant injunctive relief. *Id.,* at 67, 83 S.Ct., at 637638..(*parenthesis and italics added by this author*)

Administrative censorship, even if exercised post-publication, should be deemed to be censorship for the following reasons. Firstly, the administration, almost by definition, does not have the final authority and its decisions are always subject to the risk of reversal as the result of subsequent judicial review.[47] The fact that one can be disciplined by an administrative body without and before judicial review naturally causes a chilling effect on the supposed speaker. One may argue that, as defined, any administrative action will have a

---

[45] *Supra* note 34 at Article 24.
[46] *Alexander v United States*, 509 US 544, 113 S Ct 2766 (1993).
[47] Martin H. Redish, "The Proper Role of the Prior Restraint Doctrine in First Amendment Theory", 70 Va. L. Rev. 53, 58 (1984).

chilling effect, such as if the Food and Drug Administration finds a certain drug dangerous, this will have chilling effects on drug manufacturers and therefore will be banned. However, being chilled from engaging in physical actions because of administrative intervention (e.g. jaywalking being stopped by a police officer) is different from being chilled from speaking, only the latter of which has been considered a constitutional evil. The refrain chilling effects exists only in free speech jurisprudence for a reason.[48] Secondly, the administrative bodies could show bias in favor of the government in disputes concerning the government itself, much more so than the judiciary.[49] The administrative censoring body is not a disinterested party in censorship decisions on content that is critical of the government, for example. Thirdly, administrative bodies usually have the ability to retaliate through other means such as industrial subsidies, licensing schemes, or awards.[50]

The dissenting opinion in *Alexander* was supportive of a more inclusive understanding of censorship:

> As governments try new ways to subvert essential freedoms, legal and constitutional systems respond by making more explicit the nature and the extent of the liberty in question. First in *Near,* and later in *Bantam Books* and *Vance,* we were faced with official action which did not fall within the traditional meaning of the term prior restraint, yet posed many of the same censorship dangers. Our response was to hold that the doctrine not only includes licensing schemes requiring speech to be submitted to a censor for review prior to dissemination, but also encompasses injunctive systems which threaten or bar future speech based on some past infraction.

In France, Hadopi was one of these censorial administrative bodies for copyright protection purposes only, but after the 2009 unconstitutionality decision of the Constitutional Council[51], Hadopi's decisions only attain force only after court approval. The Council had said that basic rights' infringement can take place only through a court of law. In 2014, the Philippines Supreme Court also analogized administrative take-downs to search and seizure and ruled that administrative takedowns violate the warrant doctrine.[52] Also, the number of specialized internet censorship bodies is enlighteningly small among democracies, including Korea's

---

[48] "The Chilling Effect in Constitutional Law" (1969) 69 Columbia L Rev 808 citing *Malone v. Emmett*, 278 F. Supp. 193, 200-01 (M.D. Ala. 1967) which said:

> The Supreme Court in Zwickler, as this Court in Davis did, places free speech and other First Amendment rights in a special category. In this connection see Dombrowski v. Pfister, 380 U.S. 479, 85 S.Ct. 1116, 14 L.Ed.2d 22. In recognizing and emphasizing this 'scale of constitutional values,' on which First Amendment rights enjoy a position at the highest level, the Supreme Court in Zwickler stated:
>
> 'These principles have particular significance when, as in this case, the attack upon the statute on its face is for repugnancy of the First Amendment. In such case to force the plaintiff***201**who has commenced a federal action (at a time when no state court proceedings are pending) to suffer the delay of state court proceedings might itself effect the impermissible chilling of the very constitutional right he seeks to protect.

[49] William T. Mayton, "Toward a Theory of First Amendment Process: Injunctions of Speech, Subsequent Punishment, and the Costs of the Prior Restraint Doctrine" (1982) 67 Cornell L Rev at 245, 250.

[50] Henry P. Monaghan, "First Amendment Due Process" (197) 83 Harvard L Rev 518 at 522-23.

[51] http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf

[52] "Cybercrime Law Constitution – Supreme Court" (21 February 2014) *Rappler*, online: <http://www.rappler.com/nation/special-coverage/cybercrime-law/51197-full-text-supreme-court-decision-cybercrime-law>.

KCSC, Turkey's Information Communications Technology Authority (ICTA)[53], and Australia's ACMA.

3. Content removal in response to private parties' requests

- Law: *Information Communication Network Act* Article 44-2 and *Copyright Act* Article 103 "can be read to" require intermediaries to take down third party contents temporarily upon demand of a private party alleging injury even if those contents may be lawful.
- Intermediaries' behavior: Except the following isolated efforts, intermediaries have chosen to interpret the law as a mandatory requirement. (1) Kiso, a standard-setting self-regulatory body, has twice issued policy decisions protecting postings concerning public interest. (2) Some intermediaries required the posters objecting to the takedown to obtain a favorable decision from KCSC. (3) Other intermediaries kept content down for 30 days, the statutory maximum, at the end of which they could choose to put the content up again.
- Civil Society: We will cover here recent lawsuits and legislative efforts that have focused on the unprecedented 'mandatory' notice and takedown system, and how intermediaries responded to them.
- Lessons: We will cover the places for possible improvement on the part of intermediaries' behaviour and the importance and market share of news portals.

a. Law

In Korea, the idea that the intermediaries must be given exemption from certain limited liability for third party content on the Internet (i.e., "safe harbors") appears to have been misinterpreted. What we have in Korea is not an intermediary liability *exemption* regime, but an intermediary liability *imposition* regime, which only allows for the possibility that damage liability can be reduced or exempted through a prompt removal of problematic content.

What is more important is that the intermediaries are required to take content down. The noncommittal reductions or exemptions of liability do not work as incentives, because intermediaries cannot elect to not to take action that results in the reductions or exemptions of liability. There was a bit of ambiguity in the law, but the Constitutional Court has finally ruled that this takedown obligation applies to information that is claimed by someone to violate their rights through invasion of privacy or defamation, not just to the infringing content.[54]

Contrary to the spirit of intermediary liability regimes around the world aimed at shielding the creators of online space from liability for even lawful content hosted in that space, Korean law goes backward. The law ends up imposing the obligations on the intermediaries to censor lawful material.

A survey of the world's intermediary liability schemes may be in order:

---

[53] Information and Communication Technologies Authority, online: <http://eng.btk.gov.tr/>

[54] Constitutional Court 2012.5.31 Decision 2010 Hun-ma 88

The following chart shows the relevant provisions at a glance, edited for simplicity, which relate to a third party posting that someone sends a takedown notice to the intermediary hosting it ("noticed posting", hereinafter):

	Liability exemption for "noticed posting"		Liability imposition
Europe: e-Commerce Directive Article 14 (1)[1]	[Upon] obtaining knowledge or awareness of the infringing information	on condition that: the provider acts expeditiously to [take down] the information, the service provider is not liable for the information stored	N.A.
U.S.: DMCA Article 512 (c)[2]	Upon obtaining knowledge or awareness of facts or circumstances of an infringing material or activity; or upon notification of claimed infringement	If the service provider responds expeditiously to [take down] the material claimed to be infringing, the service provider shall not be liable for infringement of copyright.	N.A.
Japan: Provider Liability Law Article 3 (1)[3]	When the relevant service provider knew or there is a reasonable ground for the provider to know [the infringement]	unless it is technically possible [to take down the infringing information], [the service provider] shall not be liable for any loss incurred from such infringement	N.A.
Korea: Copyright Act Articles 102 and 103[4]	If an online service provider (OSP) actually knows of or has received [takedown notice] and thereby learned of the fact or circumstances of an infringement	If OSP immediately takes down the noticed posting, the intermediary shall not be liable for any infringement	In event of a takedown request, OSP must immediately take down (Article 103(2)), in which event OSP may reduce its liability (Article 103(5)).

In-table Note1 http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031
In-table Note 2 https://www.law.cornell.edu/uscode/text/17/512
In-table Note 3
http://www.japaneselawtranslation.go.jp/law/detail/?id=2088&vm=04&re=02&new=1
In-table 4 http://elaw.klri.re.kr/kor_service/lawView.do?hseq=32626&lang=ENG

As you can see from the chart above, it is clear that Korea tried to adopt a provision approximating the safe harbor provisions of the EU, US, and Japan, through *Copyright Act* Article 102.

The problem is the existence of Article 103 of the *Copyright Act*. Other countries' laws consist of just one provision corresponding to Korea's Article 102, but Korea adds the superfluous Article 103, which imposes an on-demand takedown obligation on the intermediaries, which has no equal in other countries' law. While other countries simply grant a safe harbor from liability arising from the infringing posting to those intermediaries that take down all "noticed postings" (thereby "incentivizing" the intermediaries to do so), Article 103 does something more. The law "obligates" intermediaries to take down all noticed postings. Here, "noticed postings" are the third party contents that someone reported as being unlawful.

"Incentivized" intermediaries have freedom to maintain postings that they find lawful. Intermediaries will not have a 'duty' to adjudicate upon the legality of the postings, but will have 'freedom' to do so if they want to maintain lawful postings. "Obligated" intermediaries have no such freedom and must take down postings no matter how lawful they believe the postings are.

The impact of this mandatory notice-and-takedown is clear. The Internet is censored of even lawful contents after anyone's capricious intervention, such as takedown notices, which goes above and beyond the already censorial effects of the current safe harbor notice-and-takedown system.[55] Encouraged, the putative right-holders will intensify campaigns of overbroad takedown notices, which the intermediaries are again obligated to act upon.

The liability-exempting language of Article 103(5), following the obligatory Article 103(2), is meaningless because intermediaries are already legally required to take down the posting. Even without the mandatory takedown, intermediaries already lack any incentive to maintain 'noticed' postings, because they pose a legal threat vis-à-vis the putative right-holder's claims. Given the mandatory takedown, an intermediary who does not comply may risk being held liable for maintaining perfectly lawful content and this risk is too great for the intermediaries.

What is more problematic is that many in Korea overlooked Article 103 and believed the *Copyright Act* was a sound adaptation of the international norm, specifically an adoption of the U.S.'s *DMCA* Section 512. A similar mandatory notice-and-takedown system was replicated in other areas, such as defamation and privacy infringement. For instance, Article 44-2 of the *ICNA*[56] imposes a mandatory notice-and-takedown obligation on intermediaries for any posting that is claimed to be infringing on someone's rights, regardless of its lawfulness (as interpreted by Constitutional Court 2012.5.31.Judgment 2010Hun-ma88). The Internet could therefore be censored not just by unsubstantiated claims of copyright infringement, but also by unsubstantiated claims of defamation and privacy infringement. The ICNA does not even have a genuine liability exemption provision, which constitutes the world's only pure mandatory notice-and-takedown system. This is politically

---

[55] Seltzer and Wendy, "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment" (2010) 24 Harvard J of L & Technology 171, online: <http://ssrn.com/abstract=1577785>.
[56] *Supra* note 33.

very important, because defamation is often used as a legal basis for the powerful to suppress critical opinions of them, as documented in "Korean Intermediary Liability: Not Just Backward but Going Back" (footnote 7) by K.S. Park, Open Net.

	"When notice is given, intermediaries shall not be liable if they expeditiously take down."	"When notice is given, intermediaries must take down. If intermediaries do that, they may reduce their liability."
Europe (all claims)	Applicable	N.A.
U.S. (copyright)	Applicable	N.A.
Japan (all)	Applicable	N.A.
Korea (copyright)	Applicable	Applicable
Korea (defamation)	N.A.	Applicable

b. Intermediaries' behavior

Intermediaries' behavior has been very ambivalent regarding whether they want safe harbors like other countries, or if they do not want to have any discretion on take-down decisions. The idea is that if they are given discretion, all their takedowns will be out of their volition, and they could be held liable to the users for takedown of user created content. The current provisions give the intermediaries no discretion, because the provisions require intermediaries to take down all content upon which they receive a notice of infringement. International literature on intermediary liability rules have passing references to wisdoms such as, "the intermediaries should not be required to pass judgment on the content." These maxims are meant to be an argument for creating safe harbors whereby intermediaries will not be held liable merely for having hosted unlawful content, but the Korean intermediaries seem to have misunderstood these maxims as supporting their position that intermediaries should not be given discretion. What they do not seem to understand is that "safe harbors" are not mandatory, as the laws grant exemptions from liability when intermediaries choose to institute on-demand takedowns, but they do not force them to institute the takedowns.

Indeed, the intermediaries' ambivalence seems to have affected the statutory history of the current provisions. The predecessors of Article 44-2 (Article 44 Paragraphs 1 and 2 of the *Network Act* enacted 2001.7.16, Law No. 6360)[57] simply required the service provider to take down content upon the request of a party injured by that content and did not provide any exemption. Article 44 began as the simple idea that the service provider is at least responsible for infringing content that someone complained about.

---

57 http://www.law.go.kr/lsSc.do?menuId=0&subMenu=2&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D#liBgcolor31

However, many service providers complained that they were not capable of determining whether certain content was infringing or not. They were afraid that, if they over-censored, the users who uploaded content would complain, whereas, if they under-censored, they would violate the law. In response, the law was amended in 2007 (Enacted 2007.7.27 Law No. 8289) into Article 44-2 to create a "temporary (blind) measure" for "border-line" content, which service providers can now resort to.[58] The end result was the current provision, Article 44-2.

There was some ambiguity as to what the new provisions exactly purported to achieve. Intermediaries' wish could have been met by a provision exempting them in case of removal borderline content or another provision deciding for them what to do with the border-line content. It seems that the intermediaries took the second, oppressive reading of the law, which was later confirmed by the 2012 Court.

We will survey the take-down decisions by the intermediaries, but will not look at copyright-related takedown notices, which make up more than 90% of takedown requests in other countries, however the *Korean Copyright Act* sets up a different liability scheme for copyright-related takedown requests. The *Network Act's* liability scheme affects only takedown requests related to defamation, privacy, interference with business, etc. Although the *Network Act's* liability scheme on its face covers copyright as well, the *Copyright Act's* scheme takes precedence in copyright issues in accordance with the rule of implied exception, where the provisions of a general statute yield to those of a special one. Although there will be issues with copyright-related on-demand takedowns, the *Copyright Act's* liability scheme has been quite similar to the American *DMCA* and now more so under the amendment triggered by Korea-US Free Trade Agreement. The amendment closed the final loophole by making the liability exemption mandatory, although there is still room for serious misunderstanding.

Another qualification: There is nothing similar to the Transparency Reports of U.S. OSPs published by Korean intermediaries. There are only statistics occasionally obtained through private sources, along with legislators who exercise their clout through the agencies that can in turn make various disclosure demands on the intermediaries licensed or registered with them. MP Choi Moon-soon obtained relevant data from the top three content host intermediaries through Korea Communications Commission and made the following disclosure in November 2010[59]:

<<Non-copyright-related Takedowns Pursuant to Article 44-2>>

Operators Years	NAVER	DAUM	NATE	**Total**
2008	31,953	27,454	691	**60,098**
2009	37,342	57,712	1,449	**96,503**

58 http://www.law.go.kr/lsSc.do?menuId=0&subMenu=2&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D#liBgcolor20

59 http://moonsoonc.tistory.com/attachment/cfile23.uf@133D7F0F4CE1EF660D3B87.hwp

2010 up to September (estimated year-end figures)	27,914 (37,125)	45,798 (60,911)	956 (1274)	**74,668 (99,310)**

After learning that the number of takedowns executed by the top two content hosts, Naver and Daum, significantly exceeds that of other hosts, MP Nam Kyung-pil obtained similar data on those two content hosts in October 2012[60] shown below:

<<Non-copyright-related Takedowns Pursuant to Article 44-2>>

Operators Years	NAVER	DAUM
2008	70,401	21,546
2009	83,548	50,860
2010	85,573	58,168
2011	123,079	86,431
2012 until July	104,578	40,538

Although the differences in the two tables need some explanation[61], we can make the following points of fact, uncontested:

1. The number of URL takedowns privately requested under Article 44-2 of the *Network Act* for non-copyright purposes has increased over time.
2. The annual number of URLs taken down by Naver hover above 100,000 and Daum takes down about 50-70% of Naver's.

How serious is this? There is nothing here that we can compare to the situation in the U.S. because Section 230 of the *Communications Decency Act* insulates the intermediaries from liability for defamation and other non-copyright related laws. However, we can compare these Korean numbers to government-originating takedowns in other countries. Google received only about 4,000 takedown requests in 2012 from the whole world, only about half of which Google complied with.[62] Therefore, while 2,000 takedown requests were complied with by Google, 100,000 were in Korea. As another example, the Korean government's censorship body, the Korean Communication Standards Commission, issued 54,385 takedown requests to various intermediaries in 2011, out of which only 668 were related to

---

[60] (8 October 2012) online: <http://www.ggetv.co.kr/news/articleView.html?idxno=16781>.

[61] Naver's numbers in the first table represent the number of requests, which can cover more than one URL, while the Naver numbers in the second table represent the number of URLs taken down. Daum's numbers in the first table include both permanent removals and temporary measures, such as blinds, while Daum's numbers in the second table include only temporary measures. Daum's numbers in the second table represent the total number of takedowns as Daum cancelled its policy of undoing the blinds after 30 days, therefore all temporary measures became permanent.

[62] Google Transparency Report, "Government Requests to Remove Content", online: <https://www.google.com/transparencyreport/removals/government/>.

defamation and other rights infringement.[63] Although the number of URLs is usually greater than the number of requests (for each request may cover more than one URL), the rights-infringement category of KCSC activities usually covers less than 10 URLs. That means that private censorship through Article 44-2 is underlying more than 10 times the number of rights-infringement takedowns executed by the Korean government.

It is not just the volume of censorship that is problematic. Politicians and government officials often make the takedown requests on postings that are critical of their policy decisions, which are clearly lawful, as illustrated below:

- A posting[64] critical of a Seoul City mayor's ban on assemblies in the Seoul Square;
- A posting[65] critical of a legislator's drinking habits and introducing his social media account;
- Clips of a television news report on Seoul Police Chief's brother who allegedly runs an illegal brothel-hotel;[66]
- A posting critical of a politicians' pejorative remarks on the recent deaths of squatters and police officers in a redevelopment dispute;[67]
- A posting calling for immunity from criminal prosecutions and civil damage suits on labor strikes; and[68]
- A posting by an opposition party legislator questioning a conservative media executive's involvement in a sex exploitation scandal related to an actress and her suicide.[69]

c. Civil Society and Dynamics

Korea has failed to institute intermediary immunity regimes such as the United States' *CDA* Section 230 or *DMCA* Section 512 that shields intermediaries from liability for even unlawful content. Korea's law actually chills the intermediaries into taking down even lawful content as evidenced by the examples above. The PSPD Public Interest Law Center and others filed a constitutional challenge against Article 44-2 of the *Network Act*, but this was rejected by the Constitutional Court:

> When another's personal rights such as privacy or reputation are infringed or are anticipated to be infringed, a need to temporarily block the infringing information is greater than the need to guarantee the temporal pertinence of the information. The fact that the content was disclosed may be further propagated through other means, and may cause privacy-infringement and defamation to an equal extent. In such situation, publishing a rebuttal by the infringement complainant, blocking of the links, search restrictions, expeditious dispute resolution, etc., cannot be effective alternatives to accomplish the legislative purpose. [70]

---

[63] https://www.kocsc.or.kr/02_infoCenter/info_Communition_View.php?ko_board=info_Communition&ba_id=4909

[64] http://blog.ohmynews.com/savenature/199381

[65] http://wnsgud313.tistory.com/156 (the original posting was taken down)

[66] http://www.hani.co.kr/arti/society/society_general/300688.html

[67] (30 April 2009), online: <http://blog.jinbo.net/gimche/?pid=668>.

[68] (3 September 2007), online: <http://blog.jinbo.net/gimche/?pid=492>.

[69] http://bbs1.agora.media.daum.net/gaia/do/debate/read?bbsId=D115&articleId=610524

[70] *Supra* note 69.

c. Analysis and Lessons

The innocuous rule that intermediaries must take down unlawful content that they receive notices for, and the intermediaries' ambivalent attitude has resulted in the current provisions, which set up the world's only mandatory notice-and-takedown regime.

The intermediaries' ambivalence results, I believe, from (1) the fact that the top intermediaries' marginal output of one posting (i.e., output increase originating from one more user-created content) is not great; and (2) the top intermediaries usually dominate over the voices of all the intermediaries, including the small ones. There must be inclusion in the intermediary liability dialogue of smaller intermediaries who rely on individual user-created content for the success of their business.

Also, we need to set a clear stance on the rule that Internet intermediaries should not be subject to discriminatory rules where they are required to take down perfectly lawful content, which newspaper publishers, film studios, and any other intermediary are not required to do. "What is protected offline should be protected online as well." The Manila Principles of Intermediary Liability is one such attempt (www.manilaprinciples.org) that many NGOs and individuals have subscribed to. Manila Principles Article 1.d. states that intermediaries should not be required to monitor content proactively; Article 2.a. states that "Intermediaries must not be required to restrict content unless an order has been issued by an independent and impartial judicial authority that has determined that the material at issue is unlawful"; and Article 1.c. states that "Intermediaries must not be held liable for failing to restrict lawful content." Almost identical recommendations were made in a study titled "Good Practice for Online Intermediaries"[71] commissioned by the Network of Centers, a network of 50 research centers around the world, including Harvard University's Berkman Center and Humboldt Institute.

4. Responding to surveillance requests

- Law: Korean laws are in general not dissimilar from other countries except that the state notifications to those under surveillance are delayed until the end of the investigation and after the indictment decisions are made. Also, overbroad surveillance requests are often filed.
- Intermediaries' behavior: Surveillance requests are usually mandatory on intermediaries, so there is not much they can do. However, some intermediaries over-produce data to the intermediaries due to the inability to narrow the scope of data production without reviewing the contents themselves (which would never be done in order to avoid the data subjects' wrath). In the face of the October 2014 exodus from Kakao Talk to Telegram, Daum Kakao announced that it will not fill wiretapping orders and they, along with Naver, began publishing transparency reports.
- Civil Society: The October 2014 fiasco regarding Kakao Talk and Telegram will be

[71] K.S. Park and Alexandra Kuczerawy, "The Online Intermediaries Research Project: Good Practice Document" Global Network of Internet and Society Resarch Centers, online: <https://publixphere.net/i/noc/page/Online_Intermediaries_Research_Project_Good_Practice_Document>.

examined here

- Lessons: How much should intermediaries cooperate in narrowing the scope of data production? What meaning will the Kozinski rule have on these questions?

a. Law

There are four types of surveillance procedures used by the investigative authorities in Korea: (1) wiretapping; (2) search and seizure; (3) acquisition of communication metadata; and (4) acquisition of subscriber identity data.

In 2011 in Korea, out of a total population of about 50 million people, the law enforcement wiretapped 7,167 phones; seized communication metadata [72] from 37.3 million communication facilities (phone numbers, email addresses or other accounts); and seized the subscriber-identifying information for 5.84 million facilities.[73] That was just for one year.

Per capita, the number of phones wiretapped in Korea was about 9.5 times the amount wiretapped in the United States, including those issued by the Foreign Intelligence Surveillance Court (2,732[74] + 1,789[75] = 4,521) and about 800 times the number wiretapped in Japan (25[76]) in the same period. As we will see, the comparison of other methods of communication surveillance does not fare any better.

Although there are laws in place and, as in other developed countries, an enhanced court approval is required for wiretapping[77], the sheer volume of communications surveillance conducted by the Korean government needs a lengthy explanation. The rejection rate for wiretapping applications in Korea (4%[78]) is much higher than the U.S. court's rate of 0.03%[79].

---

[72] Communication metadata is the information about communication that includes the identifying information of the communicating devices and the time and duration of the communication, but does not include the content of the communication.

[73] http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=3&boardSeq=34922.

[74] United States Courts, *Wiretap Report 2011*, online: <http://www.uscourts.gov/Statistics/WiretapReports/WiretapReport2011.aspx, *summarized here* http://epic.org/privacy/wiretap/>.

[75] Electronic Privacy Information Centre, *Foreign Intelligence Surveillance Act Court Orders 1979-2014*, online: <http://epic.org/privacy/wiretap.stats/fisa_stats.html>.

[76] Nishiyama Takaaki, "Interception of phone calls by the police is doubled to 64 numbers, tapping occurring over 19000 times," *Asahi News* (7 February 2014), online: <http://www.asahi.com/articles/ASG263RKWG26UTIL00D.html> (Japanese).

[77] *Protection of Communication Secrets Act*, Act. No. 12960, Article 5 (6 January 2015).

> "The communication-restricting measures shall be allowed only when there is a substantial reason to suspect that a crime under each of the following subparagraphs is being planned or committed or has been committed, and it is difficult to prevent the committing of the crime, arrest the criminal or collect the evidence through other measures."

[78] Byungchul Kim, "Gugjeongwon Gamcheong Yeongjangeun Mujogeon Balbudoenda? [The warrant for NIS wiretapping is issued unconditionally?]", *Media Today* (30 October 2013), online: <http://www.mediatoday.co.kr/news/articleView.html?idxno=112807>.

[79] Tim Cushing, "US Courts' Wiretap Report Shows Wiretaps are for Drugs and Warrants are rejected only 0.03% of Times" *Techdirt* (7 July 2014), online: <https://www.techdirt.com/articles/20140703/10502127773/us-courts-wiretap-report-shows-wiretaps-are-drugs-law-enforcement-warrants-rejected-only-03-time.shtml>.

The last of the four measures, seizure of the identity data of the parties to communication, will be discussed in the next chapter.

The number of devices targeted to be wiretapped in one wiretapping application varies a great deal between U.S. and Korea. The U.S. applications are filed more or less for one-application-for-one-device basis, but a typical Korean application covers 10 to 15 devices. Also, unlike the U.S., there is no limit on the number of counterparts whose conversation can be wiretapped in Korea, which increases the investigatory value of wiretapping for the authorities. This means that if a suspect spoke to 1,000 people during the wiretapping period, all 1,000 people's conversations, related or unrelated to the crime being investigated, become part of the investigatory file maintained by the authorities. This fact played an important role in one intermediary's response to wiretapping orders, to be discussed in a later chapter.

As to the search and seizure of stored information, such as e-mail, volume has not been identified as the reason for why courts or prosecutors do not keep a tally of warrants aimed at electronic communications, but rather quality is the problem. However, during the July 2008 local Educational District head election, an investigation of a progressive candidate's election campaigning spanning less than a couple months resulted in the seizure of seven years' worth of his email.[80] In a defamation investigation for critical reports of a government policy on American beef import, six television producers were subjected to the search and seizure of seven months' worth of their emails. [81] Also, in an investigation on a strike launched to block the appointment of the then President Myung Bak Lee's crony as the broadcasting company's CEO, about 20 union leaders of a broadcasting union had nine months' worth of their emails seized. [82] Search and seizure of stored information is also problematic because it involves eavesdropping on "innocent third parties," who happen to be in communication with the suspect.

The reason for the high volume of transactional metadata acquisitions is "cell tower dumps". The law requires a certificate of a "need to investigate" approved by the court for a law enforcement acquisition,[83] just as the U.S. law requires.[84] However, the sting of the numbers

---

[80] Sukjae Hong, "Geomchal, Ju Gyeongbok E-mail 7 Nyeonchi Tongjjae Dwijyeo [Prosecutors searched the whole 7-years worth of Gyeongbok Ju's e-mail]" *Hankyoreh Newspaper* (23 April 2009), online: <http://www.hani.co.kr/arti/society/society_general/351489.html>.

[81] Jinhwan Suk, Jungae Lee and HyunCheol Park, "Sasaenghwal Yeosbogo Deulchugo . . . Geomchal E-mail Gongantongchit [Peeking into and Searching private life, E-mail Public Security Rule by the Prosecution]" *Hankyoreh Newspaper* (19 June 2009), online: <http://www.hani.co.kr/arti/society/society_general/361387.html>.

[82] Kyunghee Woo, "Gyeongchali YTN Nojo E-mail Absususaeg 'Nonlan' [Controversy over the police seizure of the e-mail of the YTN Labor Union]" *Asia Economy* (1 July 2009), online: <http://www.asiae.co.kr/news/view.htm?idxno=2009070121394542118&sp=EC>.

[83] *Supra* note 95 at Art 13 "Procedures for Provision of Communication Confirmation Data for Criminal Investigation"*:*

> "(1) Any prosecutor or any judicial police officer may, when he deems it necessary to conduct any investigation or to execute any punishment, ask any operator of the telecommunications business under the Telecommunications Business Act (hereinafter referred to as the "operator of telecommunications business") for the perusal or the provision of the communication confirmation data (hereinafter referred to as the "provision of the communication confirmation data"). (2) Any prosecutor or any judicial police officer shall, when he asks for the provision of the communication confirmation data under paragraph (1), obtain permission therefore from the competent district court (including a general military court; hereinafter the same shall apply) or branch court with a document in which the reason for such asking, the relation with the relevant subscriber, and the scope of necessary data are entered: *Provided*, That if the urgent grounds exist that make it impossible to

is exactly in that law: 37 million people, more than half the total population of Korea, "needed to be investigated" in one year?

Admittedly, the reason for the large number is that the Korean police conduct massive indiscriminate surveillance, which intercepts the metadata of a huge number of communications among unidentified people. The big data can be analyzed to identify targets for deeper investigations. The metadata are usually equivalent to the 'pen register/trap and trace' data in the U.S. investigative parlance, which include the phone numbers/IP addresses called from and the specific phone number/IP address being called. In Korea, instead of requesting metadata on communications *originating or terminating at* a specified phone number, the Korean police cleverly requested the metadata on a specific cell tower and obtained the called/calling phone numbers for all the calls *going through* that cell tower. It is not clear whether they also obtained the phone numbers of the phones that made 'sleep mode' calls to the cell towers as the United States does. It is this "cell tower investigation" that accounts for 98.6% of communication metadata obtained, leaving only 235,716 requests to be individually-targeted.[85] In other words, 4,616 cell tower searches were conducted in 2011 and each cell tower produced about 7 to 8,000 phone numbers,[86] explaining the 37 million phone numbers. For comparison, in 2012, about 9,000 'cell tower dumps' were conducted by the federal and state governments of the United States.[87] Per capita, 4,616 cell tower searches conducted by the Korean government in 2011 is about 3 times more than everything the American authorities did in 2012.

This author believes that the main reason for the large volume or broad scope of the surveillance is the lack of proper user notification, which would bring many of these requests under scrutiny and give proper signals to the judiciary deliberating upon the approvals.

Under the constitutional principle of due process, when a state violates a private individual's right, whether by surveillance or other actions, the state, at minimum, must notify the individual that the state is doing so.[88] That the police have a warrant does not mean that the warrant can be executed surreptitiously and the police cannot steal something just because they have a warrant for it. The person searched should know the fact that his or her premises are being searched. Korean surveillance laws are indeed very weak on user notifications across the board.

---

obtain permission from the competent district court or branch court, he shall obtain permission immediately after asking for the . . . "

[84] 18 U.S.C. § 3123 (2009) (for prospective transactional data) and 18 U.S.C. §§ 2703 (c), (d) (2011) (for stored information on the communications that already have taken place, which include 'retrospective' transactional data). The standards differ, depending on whether they are prospective ("if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is *relevant* to an ongoing criminal investigation") or retrospective (when the Government offers "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records . . . sought are *relevant and material* to an ongoing criminal investigation.").

[85] National Human Rights Commission of Korea, *Recommendation on Telecommunications Act's Communications Data and Protection of Communications Privacy Act's Communications Metadata*, (2014).

[86] *Ibid.*

[87] Ellen Nakashima, "Agencies collected data on Americans' cellphone use in thousands of 'tower dumps'" *Washington Post* (9 December 2013), online: <http://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html>.

[88] *Goldberg v Kelly*, (1970) 397 US 254.

The wiretap and communication metadata provisions require notification to be given to the target, as the U.S. law does, but only 30 days *after a decision on whether to indict has been made by the prosecutors.*[89] (Japan requires the notice to be given 30 days *after the wiretap is complete*,[90] just as the United States requires the notice to be given 90 days *after the wiretap is complete*.[91]) This means that, if an investigation continues for and ends in 2 years with a decision on indictment, one will have lived as if nothing had happened for that 2 years. Those not indicted are unlikely to make an issue of what happened long ago. Most indicted individuals receive the notification only after they have been indicted and sometimes only find out they have been wiretapped at the trial when the prosecutors present the wiretrap transcript as evidence. By then, the privacy breach may not be as important as the other charges the individual is facing, "justice delayed is justice forgotten".

This notice can be deferred not by judges, but by the heads of the local prosecutors' office,[92] in complete contravention of the warrant doctrine.

Notification for search and seizure of electronic transmissions is also governed by similar provisions as the ones governing wiretapping, for example notification is not required until 30 days after the indictment decision.[93] However, the delayed notification for search and seizure of electronic content raises yet another dimension. Korean laws on ordinary search and seizure are very strict and suspects must be notified in advance of the warrant's execution,[94] and the delay in notification for search and seizure of emails is not justified.

---

[89] *Protection of Communication Secrets Act*, Act. No. 6546, Article 9-2 (December 12, 2001).

[90] *Act Concerning Interception of Communications for the Purpose of Criminal Investigations* at Article 23, online: <http://law.e-gov.go.jp/htmldata/H11/H11HO137.html> (犯罪捜査のための通信傍受に関する法律(平成十一年八月十八日法律第百三十七号)제23조).

[91] Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2518 (1998):

> "Procedure for interception of wire, oral, or electronic communications: (8)(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of. . .".

[92] *Supra* note 112, "Notice on Execution of Communication-Restricting Measures":

> "(4) Notwithstanding the provisions of paragraphs (1) through (3), in the event that the grounds falling under each of the following subparagraphs accrue, the notice may be deferred until such grounds cease to exist:
>
> 1. When the notice of the communication-restricting measures is seriously feared to endanger the national security and disrupt the public safety and order; and
>
> 2. When the notice of the communication-restricting measures is feared to result in dangers to lives and bodies of people.
>
> (5) Any prosecutor or any judicial police officer shall, when he intends to defer the notice in accordance with paragraph (4), obtain approval therefor from the head of the District Public Prosecutor's Office after filing an application therefor, accompanied by the material establishing a prima facie case, with the District Prosecutor's Office: *Provided*, That in the event any public prosecutor or any military judicial police officer intends to defer the notice in accordance with paragraph (4), he shall obtain approval therefor from a senior prosecutor of the competent Public Prosecutor's Office after filing an application therefor, accompanied by the material establishing a prima facie case, with such Public Prosecutor's Office.".

[93] *Supra* note 95.

[94] Criminal Procedure Code, Act. No. 341, Article 121 "Execution of Warrant and Presence of Parties" (September 23, 1954): "A public prosecutor, the defendant or his defense counsel may be present when a warrant of seizure or of search is being executed." Criminal Procedure Code, Act. No. 341, Article 122 *Execution of Warrant and Notice of Presence* (September 23, 1954). "In cases where a warrant of seizure or of search is to be executed, the persons listed in the preceding Article shall be notified of the date and place of

Delayed notification for a wiretap is justified by the fact that the contents of phone communications are usually not recorded, so the investigators have to listen in on the conversation real-time, so as the communications are taking place. In this context, if the parties to the communication are notified of the fact that they are being eavesdropped, the whole project will be frustrated. However, there is no such justification for stored communications, such as emails;[95] therefore, seizure should be notified as soon as possible to the email accountholders, just as seizure of a notebook will necessitate contemporaneous presentation of a warrant.

However, as the notification is delayed past the indictment decision, the person being searched often does not find out about the seizure of their emails until the prosecutors present it as evidence against them in court. In response to a pertinent suit filed by the PSPD Law Center in October 2010,[96] the court approved the delaying practice by ruling that the search and seizure of emails qualifies under an "urgency" exception to prior notification requirement, because the person notified may erase the emails.[97]

Such judgment turns a blind eye to the technically immovable fact that erasing emails on one's email account works in the way of cutting off the connection between the e-mail account and the data, which will remain on the server for an indefinite amount of time until the server's hard disk slot is 'written over' and the hard disk accepts more data. Also, it ignores the possibility that, since the law requires notification in advance only of execution of the warrant, the investigators can take pre-emptive measures, such as requesting the email service provider to shut off the suspect's access to the account, before executing a properly-notified warrant.

The court's decision also contravenes the National Human Rights Commission's August 19, 2010 Recommendation that specifically requires prior notification for email search and seizure and post-execution notification is only allowed in exceptional situations.[98] As a result of these efforts, the law has been amended in July 2011 to require immediate notification to "data subjects" upon seizure of the data storage device.[99] However, e-mail

---

execution in advance: *Provided*, That this shall not apply to the case where a person prescribed in the preceding Article, clearly expresses his will in advance to the court that he does not desire to be present or to the case of urgency;" Act. No. 10864, Article 219 "Mutatis Mutandis Applicable Provisions" (July 18, 2011): "The provisions of Articles 106, 107, 109 through 112, 114, 115 (1) (main sentence) and (2), 118 through 135,140, 141, 333 (2) and 486 shall apply *mutatis mutandis* to seizure, search or inspection of evidence by a public prosecutor or judicial police officer as prescribed in the provisions of this Chapter (Suspects).".

[95] The same is true for pen register data, but this will not be discussed here. The problem of not distinguishing real-time pen register data and retroactive data seems ubiquitous in other countries.

[96] Junhee Bae, "Chamyeoyeondae, E-mail Absususaeg Mitongjihan Guggae Sonbaeso [PSPD files litigation charges against the government for not notifying the seizure and search of personal E-mails]" *Money Today News* (12 October 2010), online: <http://news.mt.co.kr/mtview.php?no=2010102171123707 54>.

[97] Seoul District Court, 2012Na46780, July 5, 2013 (certiorari denied by the Supreme Court).

[98] National Human Rights Commission of the Republic of Korea, "전자우편", online: <http://www.humanrights.go.kr/03_sub/body02_2.jsp>.

[99] *Supra* note 120 at Act No. 10864, Article 106 "Seizure" (July 18, 2011):

> "(1)When it is necessary, a court may seize any articles which, it believes, is related to the defendant's case and may be used as evidence, or liable to confiscation: *Provided*, That the same shall not apply to the cases where there exist other provisions in Acts. (2) A court may designate articles to be seized and order the owner, possessor, or custodian thereof to produce such articles. (3) In case the object of seizure is computer disk and other similar data storage devices, the court shall receive in printouts or duplicates only the part of data storage that it has specified: Provided, That in case the court may seize the data storage device such printing or copying of specific scope is impossible or is significantly

account holders are still not notified of search and seizure,[100] because the new provision on the data storage device is applied only to the seizure aimed at the device itself, whereas email search and seizure is aimed at a certain email account, a technologically defunct distinction.

In the end, the amount of subscriber data disclosures is high, at around 60 times the United States' disclosures per capita. Wiretapping takes place 9.5 times more per capita than the United States and acquisition of non-content metadata is at least more than two times the United States, despite the laws in Korea being very similar as those in the United States. As to the number of search and seizures of electronic emails, there is no reliable data in Korea or any other country that this author has identified so far.[101] However, it is not just the number of surveillances, but the broadness of each surveillance measure that has become a major problem.[102]

b. Intermediaries' behavior and civil society

To address the overbroadness of the search and seizure warrants, the PSPD Law Center filed a suit against the Prosecutors' Office and won around US$7,000 in damages for the overbroad execution of the warrant. The warrant was limited to "information related to the election campaigning," however had been used for the seizure of seven years' worth of emails.[103] The court opined that "given the time spanned by election campaigning, the search should have been limited even at most less than a one (1) year period before the election date."

When the lawsuit began, it attracted public attention to how broad email search and seizures were in Korea. This caused a phenomenon referred to as "cyber-asylum," where people left domestic services for foreign services outside the reach of Korean warrants,[104] such as Gmail. The phenomenon was accelerated by Google's decision to delocalize Youtube's uploading function in April 2009 in an apparent protest to the real name law. This reminded people that domestic emails are easily trackable to their authors due to domestic email providers' policy of obtaining the users' real names with their resident registration numbers upon enrollment.[105]

After the judgment, the intermediaries claim that they are careful not to accept warrants with an overbroad scope.

---

insufficient for achieving the purpose of seizure.).(4) The court shall notify the data subject as defined by Article 2 Item 3 of the Personal Data Protection Act immediately that it has received the data according to paragraph 3.".

[100] Junghwan Lee, "Dangsindo Moleuge Dangsinui Meilgwa Mesinjeoga Teolligo Itda [Your e-mails and messages are being wiretapped without your realizing]" *Media Today* (2 January 2014), online: <http://m.mediatoday.co.kr/articleView.html?idxno=114043>.

[101] It is difficult for courts and governments to create separate statistics for that category of surveillance, because once the mail reaches their destination, it becomes a stationary object subject to the normal search and seizure process applicable to non-digital items.

[102] K.S. Park, "Communications Surveillance in Korea" *Open Net Korea*, online: <http://opennetkorea.org/en/wp/main-privacy/internet-surveillance-korea-2014>.

[103] Seoul Civil Court, 2012Na4678 (July 5, 2013).

[104] Bonkwon Koo, "Cyber Mangmyeongi Neunda [Increase of Cyber Asylum]" *Hankyoreh Newspaper* (25 April 2009), online: <http://www.hani.co.kr/popups/print.hani?ksn=351553>.

[105] Email services are not subjected to the identity verification requirement. However, domestic portals, in order to minimize inconvenience and costs involved with requesting the identity information multiple times, often request all the identity information upon enrolment if any part of their services is subject to the identity verification requirement, an abhorrent trend continued to date.

To address the wiretapping problem, the Constitutional Court reviewed a National Security Law investigation in 2010. The investigation had involved 14 consecutive extensions of a wiretapping warrant for a lawsuit filed by Jinbo Net. The maximum period for an extension is 2 months, therefore this warrant was extended for up to 30 months. In an unprecedented advance beyond any international norm, the Court struck down the provision that allowed unlimited renewals[106] of warrants. Even the American ECPA does not set such limits on the extension of warrants.[107] The reasoning of the Court was more surprising: "we need a statutory limit because it will be difficult for judges to refuse extensions",[108] however, the Court did not explain why this was case. This defeatist confession is more worrying than the result is encouraging, as the judge helplessly looks to the legislature for help in a situation that is actually in his or her power. The judge is split between the lack of "concrete awareness" of pervasive surveillance (probably due to the poor notification regime) and a sense of obligation to respond to large number and length of surveillance.

Another flashpoint took place in September 2014, when the government announced the creation of the Cyber Defamation Special Taskforce to conduct defamation investigations on online content. The Prosecutors' Office announced that it will initiate defamation proceedings pre-emptively, so before anyone alleges an injury, on content that "causes division in public opinion and distrust of government," even if the content is true. What was most surprising was a reference to its intention to search and seize the messages of Kakao Talk, the leading chat app in Korea that has 90+% market share. The idea that these private messages could be searched and seized for investigating messages of public interest caused concern among Kakao Talk's users, who migrated to a foreign chat app, Telegram. Telegram has device-to-device encryption, so surveillance through the chat app server is not possible. The "cyber-asylum" reached its height when it was revealed that in a search and seizure of an opposition party officials' Kakao Talk account, many innocent Kakao messages he had with more than 2,000 'friends' were also obtained. The friends' identity data was also obtained, despite most of the messages being unrelated to the crime under investigation. This is a result of the overbroadness of search and seizure, especially the lack of limiting the number of communication partners that are subject to the surveillance.

As the number of "cyber-asylum" seekers grew, Daum-Kakao, the operator of Kakao Talk, announced in October 2014 that it will no longer comply with any wiretap order for chat messages on the ground. Under the current technology, surveillance on chat messages can never be done on a real-time basis, the supposed hallmark of wiretapping in the Supreme Court's interpretation. The only way to emulate wiretapping is for the chat operators to save all the chat messages and turn them over to the police, but that is not strictly "real-time," according to the Court. The wiretap order on chat messages is like a square circle, it refers to something that does not exist, and therefore, is impossible to comply with. Although this

---

[106] *Supra* nota 95, at Act. No. 6546, Article 6 "Procedures for Authorization of Communication-Restricting Measures for Criminal Act Investigation" (December 29, 2001):

> "(7) The period of communication-restricting measures shall not exceed 2 months and in the event that the objective of the communication-restricting measures is attained during the period, such communication-restricting measures shall be immediately discontinued: *Provided*, That if the requirements for permission under Article 5 (1) are still valid, a request for extending the period of communication-restricting measures pursuant to paragraphs (1) and (2) may be filed, within the limit of 2 months and such request shall be appended by material establishing a prima facie case.".

[107] 29 U.S.C. § 2518 (5) (1998).

[108] Constitutional Court 2010.12.28 Decision 2009 Hun-ga 30.

move was not related to the overbroadness problem that intensified the migration, it was a great publicity stunt that restored the intermediary's reputation and therefore, their business. It was a great display of Kakao's commitment to user privacy, although the crux of the cyber asylum was less about wiretapping, because wiretapping can be used for other serious crimes that are unrelated to defamation. Kakao Talk continues to dominate the market, with 90+% of the shares, even after Kakao Talk retracted their non-compliance announcement one year later. They cited an improved privacy policy for the identification data of the chat partners. Whereas previously the identification data of *all* chat partners was given away upon a single wiretapping order, the new two-step policy only allows the chat partners selected after analyses of the chat messages by the investigatory authorities to be released.

Kakao's two-step policy is still short of full application of the warrant doctrine to the procedure of forcefully obtaining the identity data of the parties to communication. However, it is an attempt to limit the disclosure of identity data.

c. Lessons

From the unusual frequency and breadth of communications surveillance in Korea, we can only conclude that judges and prosecutors do not exercise much restraint in applying for and granting wiretaps and communication metadata. This mind-set is extended to the law enforcement agencies that issue user identification requests, which do not involve the warrant process. I believe one of the reasons for this mind-set is the general lack of awareness of the volume and threat of the surveillance being conducted. This is a unique danger associated with surveillance, because many forms of surveillance take place secretly. If the general populace does not know if they are under surveillance and therefore, do not vocalize and convey their fears thereof, the judges approving this surveillance will not realize the effect of the surveillance on the individuals and are not likely to weigh the users' privacy carefully.

One way to address this lack of awareness is the publication of 'transparency reports' both by the government and the companies. Another way is to enhance user notifications. Despite the huge number of people under surveillance, only a very small number of people actually receive notice of surveillance due to the poor notification laws. For instance, none of the 37 million people caught in cell tower dumps in 2011 were notified. The lack of notification results in the moral hazard of approval-issuing judges, whose attitudes are unlikely to change unless they acquire a "real-like understanding" of an overbroad search and seizure, such as a close friend or family member being wiretapped.

Also, we need to establish a clear stance on surveillance that is not based on individualized suspicion ("mass surveillance"). Why would the police do the cell tower search? There are times when the only way for the police to find suspects is to interrogate people who were at the supposed crime scene. The police will acquire the metadata on all the calls going through all the cell towers covering the area of the crime scene (several thousands of phone calls each hour, per cell tower in metropolitan areas) and then narrow down to a smaller number of the phone numbers of which the owners exhibited pertinent communicative or locational behavior, such as made multiple phone calls to the known phone numbers or remained in the area for a sufficiently long time as evidenced by the calls made there.

Some believe that cell tower dumps require a "warrant"[109] if it acquires geolocation information, rather the low-level court order applicable to historical call records. The

[109] In the Matter of the Application of the United States of America for an ORDER PURSUANT TO 18 U.S.C.

question remains that even if it can be issued under the lower standard, can it can be issued to such a large number of people, most of whom are innocent? It may be comforting to some to know that these metadata requests are not based on stigmatizing suspicions that some phone users are probable criminals. However, the police do *treat* all other innocent people as probable criminals. If your communicative behaviour is revealed to law enforcement officers, the infringement is constant and its implications are far-reaching, regardless of their intent. The cell tower investigation is none other than suspicion-less, dragnet surveillance of people around certain areas for the simple reason that they are there, which is the reason that NSA's mass surveillance is criticized by both the UN Office of High Commissioner and the UN Special Rapporteur on Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism.[110] It is also the reason that the indiscriminate retention of DNA data has been criticised by the European Court of Human Rights.[111] In an amicus brief submitted against the American government's application for a 4.5 hour-long cell tower dump planned for New York's Manhattan area in 2014, the American Civil Liberties Union (ACLU) argued persuasively:[112]

> [T]he intentional targeting of large numbers of non-suspects is inherently unreasonable under the Fourth Amendment and raises the concerns animating the longstanding prohibition on "general warrants . . . Allowing the government to obtain tower-dump data risks sanctioning the sort of "general warrant" that the Fourth Amendment's framers so reviled. *See Stanford v. Texas*, 379 U.S. 476, 481–82 (1965). As the Ninth Circuit observed, requests by "law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam); *accord United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). Surely, a reported gunshot in a residential neighborhood would not allow nonconsensual searches of every home in a several-block radius in hopes of identifying a suspect. Likewise, a theft in Times

---

§ 2703(D) Directing Providers to Provide Historical Cell Site Locations Records, *930 F.Supp.2d 698* (S.D. Tex. 2012); Hon. Brian L. Owsley, "The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance", 16 U Pa J Const L 1, at 17–23 (2013).

[110] Office of the UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age,* A/HRC/27/37 (30 June 2014), online: <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>:

> "Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate";

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, OHCHR, 2014, A/69/397, online: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement>:

> "[Mass surveillance] amounts to a systematic interference with the right to respect for the privacy of communications, . . . it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately."

[111] *S and Marper v United Kingdom,* Nos 30562/04 and 30566/04, [2008] ECHR 1581, 48 EHRR 50.

[112] American Civil Liberties Union, "Response to Government Application for Historical Cell Site Data from Cell Towers in the Vicinity of One Location During a Four-and- One-Half-Hour Time Period," as Amicus Brief, (20 May 2014), online: <https://www.aclu.org/sites/default/files/assets/5.20.2014_aclu_tower_dump_brief_to_m.j._francis.pdf>.

> Square would not permit frisks and bag searches of every person walking along Broadway. Dragnet searches are no more permissible when carried out using electronic means; a claim by the government that a criminal suspect whose email address it does not know sent a potentially incriminating email on a particular day would never authorize it to ask Google or Yahoo to produce a catalogue of every email sent from a New York City internet protocol address on that day.

In response to ACLU's argument, Magistrate Judge James C. Francis V ruled:[113]

> I will . . . require the Government to submit an amended application that i) provides more specific justification for the time period for which the records will be gathered and ii) outlines a protocol to address how the Government will handle the private information of innocent third parties whose data is retrieved. See In re S.D. Tex. Application, 930 F. Supp. 2d at 702 ("[I]n order to receive such data, the Government at a minimum should have a protocol to address how to handle this sensitive private information."); see also In the Matters of the Search of Cellular Telephone Towers, 945 F. Supp 2d 769, 771 (S.D. Tex. 2013) (issuing warrant for cell tower records but requiring, among other things, that "any and all original records and copies . . . determined not to be relevant to the investigation" be returned to cell service providers.)".

Regarding another 2-hour long cell tower dump application for one hour before and one hour after a crime, another Magistrate, Judge Brian Owsley, ruled:[114]

> Finally, there is no discussion about what the Government intends to do with all of the data related to innocent people who are not the target of the criminal investigation. In one criminal investigation, the Government received the names, cell phone numbers, and subscriber data of 179 innocent individuals. *See United States v. Soto,* No. 3:09CR200 (D. Conn. May 18, 2010) (Memorandum in Support of Motion to Suppress). Although the use of a court-sanctioned cell tower dump invariably leads to such information being provided to the Government, in order to receive such data, the Government at a minimum should have a protocol to address how to handle this sensitive private information. Although this issue was raised at the hearing, the Government has not addressed it to date. This failure to address the privacy rights for the Fourth Amendment concerns of these innocent subscribers whose information will be compromised as a request of the cell tower dump is another factor warranting the denial of the application."

A fatal flaw of mass surveillance from a human rights perspective is that it can be used to search for a suspect. Surveillance is meant to be used once a suspect has already been identified, for example when there are specific individuals suspected of criminal involvement.

---

[113] In the Matter of the Application of the UNITED STATES of America for an ORDER PURSUANT TO 18 U.S.C. §§ 2703(C) and 2703(D) DIRECTING AT & T, SPRINT/NEXTEL, T–MOBILE, METRO PCS and VERIZON WIRELESS to Disclose Cell TowerLog Information, --- F.Supp.2d ----, 2014 WL 4388397 (S.D.N.Y.), online: <https://www.aclu.org/sites/default/files/assets/sdny__mj_francis__tower_dump_order.pdf>.

[114] In the Matter of the Application of the UNITED STATES of America for an ORDER PURSUANT TO 18 U.S.C. § 2703(D) Directing Providers to Provide Historical Cell Site Locations Records, *930 F.Supp.2d 698* (S.D. Tex. 2012).

In fact, the *NSA* was not looking for suspects of a specific crime that took place, but was searching for people who may have committed crimes that the *NSA* does not know about, or people who may commit a crime. This standard potentially turns all individuals into potential targets.

An argument can be made that the privacy interest associated with communication metadata is not significant when the police do not know *whose* communication metadata they are getting. It is true that privacy cannot be infringed when we know *whose* privacy is being infringed, however, as we shall discuss later, other laws enable the authorities to gain identities easily, such as through the warrantless seizure of subscriber identification data.

5. Responding to user identity requests and related users' inspection rights issues

- Law: *Telecommunications Business Act* Article 83-3 allows intermediaries to release subscriber-identifying data to the investigative authorities without a warrant and without any notification to the subscribers.
- Intermediaries nearly always comply, even though it is not mandatory; Telecoms' refusal to allow users' inspections on data disclosure in relation to Article 83-3.
- In transition: Will cover a series of lawsuits and campaigns responding to the state of affairs above: the 2012 Naver High Court decision and the 2015 Telecoms High Court decision.
- Lessons: What should intermediaries do in face of non-mandatory data requests? How about with users wishing to find out about those data requests?

a. Law

Article 83-3 of the *Telecommunication Enterprise Act* states that the intermediaries "may provide" the identity data of the parties to a communication when investigative authorities request it in writing.

In a country of about 50 million people, more than 6 million people's subscriber information was accessed without a warrant by investigative authorities in 2011[115]. That number increased to close to 10 million people in 2013.[116] These numbers were negatively referred to as "treating [the people] as potential criminals" by the country's Constitutional Court in the historical August 2012 decision that struck down the real name identification law.[117]

---

[115]Official website of the then relevant Korean Communication Commission http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=3&boardSeq=34922

[116]Official website of the now relevant Ministry of Science, ICT, and Future Planning, online: <http://www.xn--vb0b54r8od4wb7yz1lfqqs.com/www/brd/m_211/view.do?seq=1736&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=2>.

[117] *See* Constitutional Court's Decision 2010 Hunma 47, 252 (consolidated) announced August 28, 2012 and the subsequent decision of the Korean High Court in October 2012 (Seoul High Court, 2011Na19012, Chief Judge Kim Sang-Jun) which held a major portal liable for disclosing a blogger's identity to the police when no warrant was produced.

b. Intermediaries' behavior and civil society

One of the reasons for the large volume of warrantless requests for user data is that the intermediaries have complied with nearly all these requests, even though they were not required to. The investigatory authorities have no incentive to restrict the scope or volume of their requests, because there is no push-back from the intermediaries. To address the problem, the PSPD Law Center[118] filed a constitutional challenge against *Telecommunications Business Act* Article 83(3) for violating the "warrant" doctrine in the Korean Constitution. Article 83(3) allows police to access subscriber information without a warrant. The Constitutional Court dismissed the constitutional challenge in August 2012, stating that the provision merely *allows* the operators to make the disclosure and does not require them to do so, and therefore there is no "state action" involved in what the Court believed to be "voluntary acts of the telecommunications operator."[119]

Upon hearing that warrantless disclosure is not a result of State action, but rather the companies, the PSPD Law Center promptly filed a damages suit against a major portal for making a "voluntary" disclosure. The high profile case involved the defamation investigation[120] into a Youtube video clip[121] that featured the then cultural minister and international figure skating star Yuna Kim. After appealing the initial the decision, the complainant won damage awards of about US$500 in the High Court for Seoul District[122].

Although the decision was promptly appealed to the Supreme Court and is still ongoing, the repercussions were significant, because within two weeks all major portals and Internet companies stopped complying with Article 83(3) data requests[123]. Out of roughly 6 million data disclosures a year, about 500,000 to 600,000 were made by the portals. Therefore, if each individual brought it to court, the damages the Internet industry would have to pay would be astronomic. However, the telecoms, responsible for 90% of subscriber data disclosures in Korea, have responded quite differently than the Internet companies and continue to comply with Article 83(3) requests.

What is more, the telecoms refused to disclose to their customers when asked whether Article 83(3) data disclosures have been made, which meant that the victims could not even file a suit. In April 2013, PSPD filed another suit[124] forcing the telecoms to reveal the subscriber data that they have disclosed to the police under Article 83(3). PSPD was successful in the

---

[118] K.S. Park as Executive Director of PSPD Law Centre, who directed the lawsuits described here, later founded Open Net, www.opennetkorea.org, in 2013, which is now working jointly with PSPD Law Centre on the telco campaign.

[119] Constitutional Court, 2010Hunma439, August 23, 2012.

[120] Mee-yoo Kwon, "Cultural Minister Yu upset at Yu-na Video" *The Korea Times* (17 March 2010), online: <http://www.koreatimes.co.kr/www/news/nation/2010/03/117_62548.html>.

[121] YouTube, "TITLE" (18 March 2010), online: <http://www.youtube.com/watch?v=X5OOD72-MzA>.

[122] Seoul High Court, 2011Na19012, October 18, 2012 (Chief Judge Kim Sang-Jun).

[123] Sunsik Kim and Soonhyeok Lee, "Susagigwane Gogaegjeongbo Tedeo Isang Jegong Anhae [Cusomer Information No Longer Given to Law Enforcement Agencies]" *Hankyoreh Newspaper* (1 November 2012), online: <http://www.hani.co.kr/arti/economy/economy_general/558613.html>.

[124] Jonghoon Kim, "Eitongsa, Susagigwane Gaein Jeongbo Jegong Yeobu Gonggaehala" Sonbaeso ["Mobile telecommunication companies should disclose whether personal information was offered to law enforcement agencies" Litigation charges against Mobile telecommunication companies]" *Global News* (16 April 2013), online: <http://www.gobalnews.com/news/articleView.html?idxno=2240>.

Seoul High Court in January 2015, and damages of about US$2-300 were awarded for each instance of refusal to disclose.[125] This case is also in the Supreme Court presently.

c. Lessons

We need to establish a clear stance on access to identification data of the users of communication services, because without a clear stance the intermediaries respond differently.

When people communicate with one another through voice, text, or images over the Internet or the telecommunication network, they mostly do so anonymously. Anonymous in the sense that even if those engaging in communication know each other's identities, the investigative authorities do not know their identities. If a constable eavesdrops on a subversive conversation between two unknown people over a brick wall, their identities remain within the realm of a reasonable expectation of privacy, which the constable could only penetrate with judicial supervision, such as a warrant.

However, the identity data of Internet intermediary service subscribers, namely "subscriber data", has been given insufficient legal protection around the world and has been, unfortunately, made accessible without a warrant to the investigative authorities in the U.S.[126], UK[127], Germany[128], France[129], and South Korea[130], among others.

The International Principles on the Application of Human Rights to Communication Surveillance holds that "metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection," because:

> Today, each of these types of information might, taken alone or analyzed collectively, reveal a person's identity, behavior, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time, or of all people in a given location, including around a public demonstration or other political event.[131]

The sensitivity of the subscriber identifying data was most succinctly captured by the Supreme Court of Canada in June 2014, which struck down as unconstitutional polices' warrantless acquisition of subscriber data, reasoning that:

> [P]articularly important in the context of Internet usage is the understanding of privacy as anonymity. The identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address and telephone number found in the subscriber information. Subscriber information, by tending to link particular kinds of information to identifiable individuals may implicate privacy interests relating to an individual's identity as the source,

---

[125] Seoul High Court January 19, 2015 Judgment 2014Na 2020811
[126] 18 U.S.C. § 2703(c)(1)(E), (2) (1948).
[127] *Regulation of Investigatory Powers Act 2000* (UK), c 23.
[128] Federal Electronic Communications Act, Article 113 (1); Telecommunications Act (TKG) (22 June 2004) (Germany)
[129] Art L34-1-6 Code des postes et communications electroniques.
[130] Telecommunications Business Act, Article 83(3) (Korea).
[131] Necessary and Proportionate, online: <https://necessaryandproportionate.org/>.

> possessor or user of that information. Some degree of anonymity is a feature of much Internet activity and depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure.[132]

Also, in a highly relevant article, Proffesor Jeffrey Skopek proposed the concept of "reasonable expectation of anonymity" as a privacy norm to be observed,[133] reasoning that:

> [T]he structural features of our world that are capable of maintaining the secrecy of "personal information" are not limited to those that hid the information . . . they can be also features that hide what makes that information *personal* . . . if the action took place online, relevant factors might include whether the actor used a pseudonym, whether pseudonym was connected to other traits, such as an IP address, and whether that IP address was connected to the actor's name.

The Snowden revelations also highlight the importance of subscriber information. It is theorized that the ready availability of subscriber information makes it very profitable for the authorities to engage in non-individualized, massive surveillance on the content and the metadata.[134] Post-Snowden, Brazil was the first country that explicitly imposed the requirement of judicial approval for police access to subscriber-identifying information.[135] Even before Snowden, Chile required court approval for such access, which was reported in Access' Implementation Guide on the Necessary and Proportionate Principles.[136] In April 2014, the Korean National Human Rights Commission decided that the lack of a requirement for judicial authorization for police to access the collected data violates international human rights.[137]

Another lesson to be learned is from the different responses of two intermediary groups: portals and telecoms. Telecoms are in a closer relationship with the government, because the mobile telecoms depend on the wavelength monopolies granted or auctioned off by the government and the wired telecoms depend on the infrastructure provided by the government, such as underground tunnels and the power poles through which their lines are laid. Furthermore, because of the state-sponsored monopolies, the mobile telecom market is oligopolistic, therefore the telecom operators are not concerned with consumer wishes, because consumers do not alternative providers to choose from. Once Korean telecoms are entrenched into stable market shares, they do not make great efforts to "out-innovate" the competitors for a higher percentage. The commentators often refer to 50:30:20 among the top three operators (SKT, KT, and LGU+) as the "golden divide" that the three operators take comfort in.

6. Global Lessons

---

[132] *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212.
[133] Jeffrey M. Skopek, "Reasonable Expectations of Anonymity" (2015), 101 Virginia L Rev 691.
[134] K.S. Park, "Communications Surveillance in Korea" *OpenNet Korea*, online: <http://opennetkorea.org/en/wp/main-privacy/internet-surveillance-korea-2014>.
[135] Marco Civil da Internet 12.965, de 23.04.14, art. 10, s. 1
[136] Amie Stepanovich and Drew Mitnick, "Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance" *Access* (May 2015), online: <https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf>.
[137] online: <http://news.mt.co.kr/mtview.php?no=2014041611218282360>.

Intermediaries play a pivotal role in delivering human rights in Korea. Many of the restrictions on free speech and privacy come in the form of "soft law". Administrative censorship relies almost entirely on formally non-binding "corrective requests". Notice-and-takedowns, although found to be unprecedentedly mandatory, have left room for innovation, which the intermediaries have exercised in order to protect freedom of speech through KISO. However, some of the top intermediaries have demonstrated contradicting behavior when it comes to reforming the current notice-and-takedown system.

Intermediaries have a narrow ability to exercise any rights-favoring discretion regarding mandatory surveillance supported by judicial orders. However, the leading intermediaries, Naver, Daum, and Google, have focused more on publishing transparency reports and adopting privacy-favoring technologies, such as shortening data retention periods and replacing server-level encryption with device-level encryption. These actions should be recommended to all intermediaries. The major impetus for human rights should come from the judiciary issuing the warrants, as it is the judiciary who will be affected by the ubiquity of such surveillance and its volume. This should be entered into public discourse by improved notification systems.

As to warrantless surveillance allowed on subscriber identifying data, the telecoms and the Internet companies have shown varying degrees of rights-favoring attitudes. One observation is that the more dominating market shares an intermediary has, the less likely it is to take a rights-protective position.

Finally, we need to educate intermediaries of the clear world standards protecting human rights, such as www.necessaryandproportionate.org and www.manilaprinciples.org. For instance, large intermediaries state that they prefer mandatory notice-and-takedowns whereby they are obligated to take down perfectly lawful material as long as someone gives a notice. Their reasoning is that they do not want to be in a situation where they have to make decisions on the content. It is either an attitude based on misunderstanding or not committing to the user-generated content. When the scholars and advocates argue that intermediaries should not be asked to judge on content legality, what they mean is that intermediaries should not be held liable for judging incorrectly. It does not mean that intermediaries should have their discretion to protect users' privacy or free speech taken away, even against government orders or requests. They are the last bastion of the users' privacy and free speech and the intermediaries should remind themselves of the important role they play.