KOREA INTERNET TRANSPARENCY REPORT

한국 인터넷 투명성 보고서

2018

August 2018

Korea University Law School, Clinical Legal Education Center

Korea Internet Transparency Reporting Team

http://transparency.kr

• CONTENTS

Ⅰ. Introduction

The internet is a medium that allows information, once limited to a select few, to be communicated without time or space constraints, thereby accelerating the development of civilization and knowledge. The main reason why the internet merits high praise is because anyone can easily access it. However, the internet can be also used as a tool for illegal activities. The Government should not only prevent such dangers, but also take care to nurture the positive aspects of the internet, by refraining from excessively monitoring/censoring internet use.

The government may collect the communications information of internet users or regulate the communications between people, to promote sound culture or prevent crimes. Nevertheless, there always exists a risk that the government, during this process, could restrict freedom of speech and the right of knowledge by abusing its power and unduly collecting a person's information and his/her communications or restricting the flow of information.

The Korean government can, without prior judicial review, delete or block internet posts, approx. 100,000 URLs are being deleted or blocked per year. Also, with the "Temporary Measure (Temporary Blinds)" system which allows internet service providers to block internet posts upon requests by persons who simply 'claims' defamation, more than 450 thousand posts are being blocked annually. It is relatively easy for the government to collect users' information, which amounts to over 1 million internet users' information per year on average.

Given this backdrop, it is very important for the people to know the realities of government internet surveillance and censorship. Without knowing the real situation, it is harder to know the root of the problem and its seriousness. If people are not interested in the scope of censorship and surveillance, it will be more difficult to expect the government or service providers to be conscious of, or have a sense of responsibility for censorship and surveillance, and the current situation of widespread censorship and surveillance can only deteriorate.

The Korea Internet Transparency Report was created to not only ensure the people's right to know but also to urge the government not to exploit its power of censorship and surveillance, which should be kept in check by people's counter-monitoring.

In this 2017 Report, we analyze the status of Korean internet censorship and surveillance focusing on problems and prominent individual cases in 2016, based on the data disclosed by the

government (Ministry of Science and ICT, Korea Communications Standards Commission)[1], and assess the level of transparency and the road ahead for improvement.

[1] We have also used the data disclosed upon our request for information disclosure. The transparency reports published by Naver and Kakao, the two major online service providers in Korea, were also used.

Ⅱ. Surveillance – Methods

- For the government, including investigatory agencies, there are 4 major measures employed for surveillance of internet user's identifying information, communication metadata, and contents of the communications.

- **'Communication restricting measures'** (Wiretapping or Interception. Hereinafter referred to as **"Interception"**) refer to acquiring the 'contents' of the communications sent or received by the person subject to the investigations through cooperation from operator of telecommunications business, after written permission from the court (from Article 5 to Article 9-2, Protection of Communications Secrets Act). In the case of wire or mobile telephone, the agency may view the contents of the call and text messages. In the case of the Internet, the agency may view the contents of the emails, messages and chats, internet connections, and anonymous posts.

- **'Acquisition of Communications confirmation'**(Hereinafter referred to as **"Acquisition of communication metadata"**) refers to investigatory agencies acquiring from operator of telecommunications business the numbers related to communications (time and date of communications, phone numbers, number of usage, location, etc.) upon prior approval of the court (Article 13 – Article 13-4, Protection of Communications Secrets Act). If the request concerns use of internet, requesting agency can acquire the internet logs, IP addresses, etc.

- **'Provision of communications data'** (Hereinafter referred to as **"Provision of subscriber identifying information"**) refers to investigatory agencies requesting operator of telecommunications business to personal identification data of the person in relation to investigations (name, identification number, address, date of subscription and un-subscription, telephone number, ID, etc.) and the operators voluntarily providing such data (without court orders). (Article 83, Telecommunications Business Act)

- Also, by the Criminal Procedure Act, the government may conduct surveillance on communications via search and seizure after obtaining a warrant (Article 215, Criminal Procedure Act). **Search and seizure on service providers or telecommunications equipment** enable the prosecutors to collect all communications contents, metadata, and subscriber identifying information.

Ⅲ. Surveillance – Status and Analysis

1. Overview and Analysis

Category[2]		2013		2014		2015		2016		2017	
		Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.
Interception[3]	All communications	592	6,032	573	6,678	334	6,302	311	6,683	219	6,775
	All internet	401	1,887	372	1,748	179	998	181	899	135	827
	2 major providers	221	556	181	547	75	350	108	193	53	114
Communication metadata	All communications	265,859	16,114,668	259,184	10,288,492	300,942	5,484,945	303,321	1,585,654	301,257	1,052,897
	All internet	51,367	403,227	32,933	64,721	36,100	65,333	30,753	67,362	37,207	93,274
	2 major providers	7,990	23,163	6,940	13,857	7,199	13,024	8,003	23,951	8,224	23,579
Subscriber Identifying information	All communications	944,927	9,574,659	1,001,013	12,967,456	1,124,874	10,577,079	1,109,614	8,272,504	989,751	6,304,985
	All internet	115,194	392,511	114,260	489,916	100,643	423,533	84,302	312,056	65,151	263,579
	2 major providers	1	17	0	0	0	0	0	0	0	0
Search and Seizure	2 major providers*	14,408	-	15,684	-	13,183	1,032,033	13,157	722,876	9,538	10,791,104

TABLE 1. STATUS OF COMMUNICATIONS SURVEILLANCE 2013-2017

- On average, 406 cases of Interception (acquiring the contents of communications) for all communications per year are conducted for 6,494 accounts for 5 years from 2013 to 2017. Among them, Interception for internet number 254 per year, for 1,272 accounts, which account for approx. 62.5% of the total number of Interception (in terms of a number of documents).
- Acquisition of communication metadata (phone numbers, time, locations, etc.) for all communications number 286,113 cases on average per year, for 6,905,331 accounts. Among them, acquisition of communication metadata for internet number 37,672 per year, for 138,783

[2] 'All internet' refers to the 'internet, etc' as categorized by the Ministry of Science and ICT's report, and is a sum of the data reported by communication service providers (OSP such as portals and ISP, etc., excluding wire and mobile communication service providers). 'Two major providers' refer to Naver (including a subsidiary 'Campmobile') and Kakao. (However, the number of accounts in the search and seizure are omitted until 2014, as the numbers for Kakao have not been counted.)

[3] The Ministry of Science and ICT has found some errors in the calculation of the number of interception between the second half of 2014 and the first half of 2016 and revised those figures. Some figures are different from the statistics of the last report to reflect this change.

accounts, which is approx. 2% of the total (in terms of the number of accounts), probably because requests are mainly made to the mobile telecommunication service provider, and focused on 'cell tower dump.' While the number of acquisition of communications metadata is on the rise, the number of accounts fallen from 2013 (16,114,668 accounts) and 2014 (10,228,492 accounts) to 2015 (5,484,945 accounts), 2016 (1,585,654 accounts), and 2017 (1,052,897 accounts).

- Provision of subscriber identifying information number 1,034,036 cases per year, for 9,539,337 accounts. Provision of subscriber identifying information for internet service subscribers numbers 95,910 cases per year, for 376,319 accounts. This accounts for about 3.94% of the total number of provision of subscriber identifying information (in terms of a number of accounts). Provision of subscriber identifying information, as it does not require a court order but only a simple process of a request by investigatory agencies, are being conducted on a large scale, and more than 9.5 million accounts' information, which constitutes 18.4% of the total population, are subject to this process.

- The data for search and seizure on communication service providers (which can be used for acquiring communications contents, metadata, and subscriber identifying information) are not available from the government. The analysis relies on the data disclosed in transparency reports of two major online service providers. According to the reports, search and seizure on two companies numbered 9,538 in 2017, with 10,791,104 accounts subject to search and seizure. The number of cases decreased by 27% from 2016, but the number of accounts jumped 14.9 times. Particularly, the surge was caused by a single case that obtained 6,963,605 personal information for a certain presidential candidate's alleged violation of the law of personal information protection.

- Search and seizure on communication conducted on such a vast scale will be certainly the most serious problem, as it allows the government to see the contents of the communications. There is a growing need for reverse monitoring by the citizens against the government's search and seizure of power that can conduct almost unlimited communications surveillance.

2. Status and Analysis of Interception on Internet

	Prosecutors		Police		NIS		Military Investigatory Agencies, Etc.*		Total	
	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.
2013	-	-	59	81	334	1,798	8	8	401	1,887
2014	1	1	154	250	213	1,493	4	4	372	1,748
2015	-	-	29	65	150	933	-	-	179	998
2016	-	-	26	43	155	856	-	-	181	899
2017	-	-	31	66	104	761	-	-	135	827

TABLE 2. INTERCEPTION ON INTERNET, BY REQUESTING AGENCIES, 2013-2017

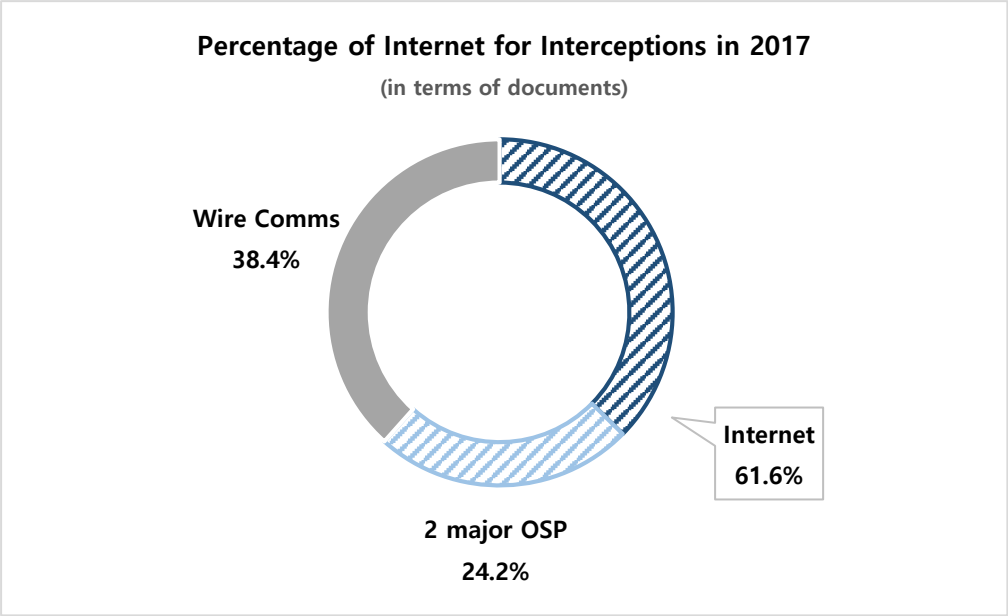
* MILITARY INVESTIGATORY AGENCIES, ETC. : MINISTRY OF DEFENSE, DEFENSE SECURITY COMMAND, KOREA COAST GUARD

		2013		2014		2015		2016		2017	
		Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.
All communications		592	6,032	573	6,678	334	6,302	311	6,683	219	6,775
All Internet		401	1,887	372	1,748	179	998	181	899	135	827
2 Major Providers	**Total**	221	556	181	547	75	350	108	193	53	114
	Naver	72	195	56	193	28	127	35	76	16	53
	Daum[4]	68	272	47	237	39	215	37	81	37	61
	Kakao	81	89	78	117	8	8	36	36	0	0

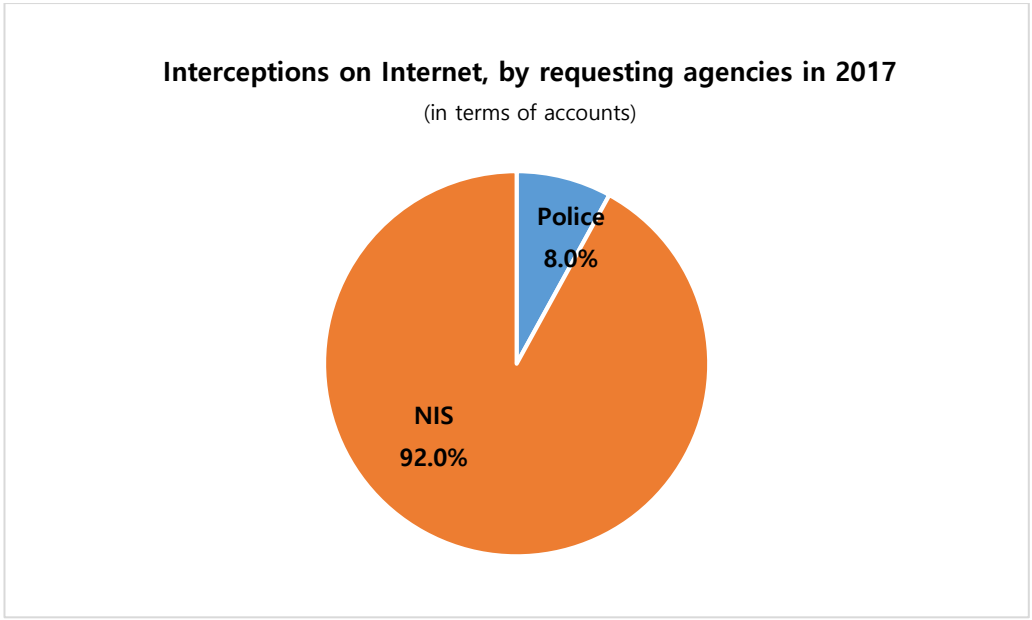
TABLE 3. STATUS OF INTERCEPTION, 2013-2017

- Interception for internet (acquiring the contents of communications) has been conducted in 2017 after 135 requests, for 827 accounts (6.12 accounts per document).
- Interception focuses on the internet. This is because the major means of communications has now become the internet, and acquisition of communications through emails and messenger has become essential.

[4] It is a portal service run by Kakao, who differentiates Daum and Kakao in its transparency report. Daum runs email, blog, and community services, while Kakao focuses on mobile messenger service.



- 98.8% of all interceptions (92% of interceptions on the internet, in terms of the number of accounts) are made by the NIS and seem to be employed for national security-related investigations.



3. Status and Analysis of Acquisition of Communication Metadata in Internet

	Prosecutors		Police		NIS		Others*		Total	
	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.
2013	4,604	310,101	44,866	87,320	273	729	1,624	5,077	51,367	403,227
2014	3,855	11,374	27,952	51,218	163	293	963	1,836	32,933	64,721
2015	6,587	16,430	28,776	45,804	197	315	540	2,784	36,100	65,333
2016	6,254	14,070	24,011	52,469	100	122	388	701	30,753	67,362
2017	7,975	25,631	28,725	66,170	185	294	322	1,179	37,207	93,274

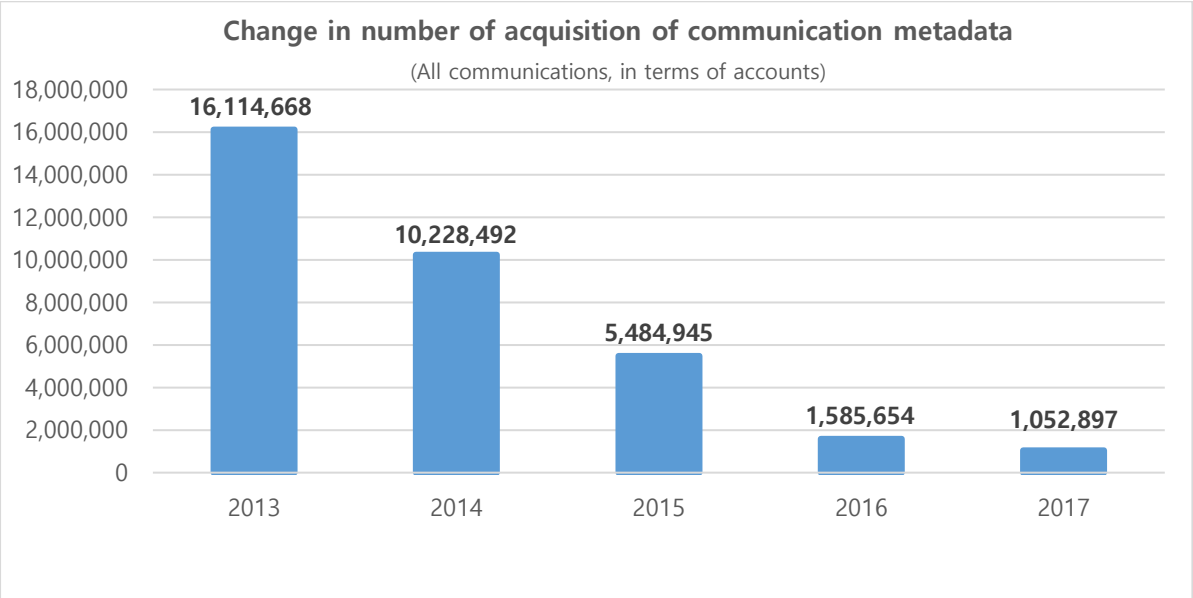
TABLE 4. ACQUISITION OF COMMUNICATION METADATA ON INTERNET, BY REQUESTING AGENCIES 2013-2017

* OTHERS: MILITARY INVESTIGATORY AGENCIES, KOREA COAST GUARD, ADMINISTRATIVE BODIES WITH POLICE AUTHORITIES (KOREA CUSTOMS SERVICE, MINISTRY OF JUSTICE, MINISTRY OF EMPLOYMENT AND LABOR, KOREA FOOD AND DRUG ADMINISTRATION, ETC.)

	2013		2014		2015		2016		2017	
	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.
All Communications	265,859	16,114,668	259,184	10,288,492	300,942	5,484,945	303,321	1,585,654	301,257	1,052,897
All Internet	51,367	403,227	32,933	64,721	36,100	65,333	30,753	67,362	37,207	93,274
2 Major Providers	7,990	23,163	6,940	13,857	7,199	13,024	8,003	23,951	8,224	23,579

TABLE 5. STATUS OF PROVISION OF COMMUNICATIONS METADATA, 2013-2017

- Acquisition of communication metadata (calling/receiving number, time, location, etc.) on the internet for the year 2017 was made for 93,274 accounts, in response to 37,207 requests. It takes up approx. 12.4% in terms of a number of documents, and 8.86% in terms of accounts.
- In terms of the number of accounts, it is a noticeably positive change that acquisition of communication metadata for all types of communications is sharply declining. However, acquisition of communication metadata for the internet was for 93,274 accounts which are 28% increased rate from last year, and the number of accounts provided by two major online service providers (OSPs), Naver and Kakao, has remained high with 23,579 accounts in 2017.



- The details of the provision of metadata for all communications by types of metadata are as follows.

	Documents	Accounts
Call log	272,659	991,191
Log record of computer communications or internet	6,608	20,087
Location of the sending cell tower	12,447	22,807
IP addresses	9,543	18,812
Total	**301,257**	**1,052,897**

TABLE 6. ACQUISITION OF COMMUNICATION METADATA IN 2017, BY CATEGORY (ALL COMMUNICATIONS)

4. Status and Analysis of Provision of Subscriber Identifying Information in Internet

	Prosecutor		Police		NIS		Others*		Total	
	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.
2013	19,054	93,662	91,485	280,469	1,548	5,318	3,107	13,062	115,194	392,511
2014	23,443	143,193	86,469	330,394	1,491	6,498	2,857	9,831	114,260	489,916
2015	17,796	94,942	79,498	313,140	1,353	9,763	1,996	5,698	100,643	423,533
2016	12,516	71,619	69,101	230,417	971	3,038	1,714	6,982	84,302	312,056
2017	9,778	62,064	53,328	194,821	747	2,469	1,298	4,225	65,151	263,579

TABLE 7. STATUS OF PROVISION OF SUBSCRIBER IDENTIFYING INFORMATION, BY REQUESTING AGENCIES, 2013-2017

* OTHERS : MILITARY INVESTIGATORY AGENCIES, KOREA COAST GUARD, ADMINISTRATIVE BODIES WITH POLICE AUTHORITIES (KOREA CUSTOMS SERVICE, MINISTRY OF JUSTICE, MINISTRY OF EMPLOYMENT AND LABOR, KOREA FOOD AND DRUG ADMINISTRATION, ETC.)

	2013		2014		2015		2016		2017	
	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.	Doc.	Acc.
All Comms	944,927	9,574,659	1,001,013	12,967,456	1,124,874	10,577,079	1,109,614	8,272,504	989,751	6,304,985
All Internet	115,194	392,511	114,260	489,916	100,643	423,533	84,302	312,056	65,151	635,795
2 Major Providers	1	17	0	0	0	0	0	0	0	0

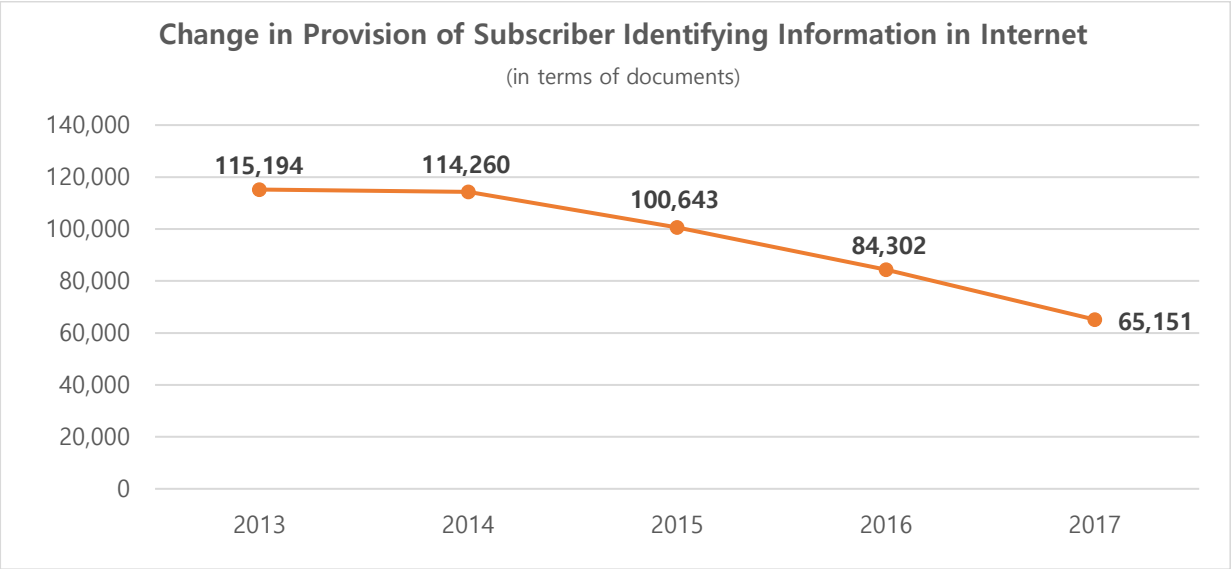
TABLE 8. STATUS OF PROVISION OF SUBSCRIBER IDENTIFYING INFORMATION 2013-2017

- Provision of subscriber identifying information for internet in 2017 was conducted for 635,795 accounts, through 65,151 requests.
- In 2016, the provision of subscriber identifying information both for all communications and the internet is slightly decreased. While the provision of subscriber identifying information on the Internet is decreasing, in terms of the number of documents. The trend of the provision of subscriber identifying information on the Internet is decreasing, but the accounts provided in 2017 has doubled from the previous year revealing more users are identified.
- After a lower court's decision in 2012[5] that ordered a major portal to pay damages for providing

[5] Seoul High Court, 2011Na19012, Decided Oct 18 2012

subscriber identifying information to the investigatory agencies, when the suspicion of a crime was uncertain, major portals ceased to provide subscriber identifying information from 2013. While the Supreme Court in March 2016 overruled the lower court's decision[6], two major providers still do not comply with the request for provision of subscriber identifying information. Considering the fact that the simplified process allowed the government to acquire personal information of communication users without any court warrant, it is a welcome improvement.

- As major portals stopped providing subscriber identifying information, subscriber identifying information of internet users now seems to be mostly being provided by the internet network service providers (ISPs).



[6] Supreme Court, 2012Da105482, Decided Mar 10 2016

5. Status and Analysis of Search and Seizure on Internet

- The government does not currently disclose data on search and seizure for communication service providers which contents and communication metadata, as well as subscriber identifying information, can all be acquired. Therefore, we have given the below analysis based on the numbers published by two major online service providers (OSPs), Naver and Kakao.

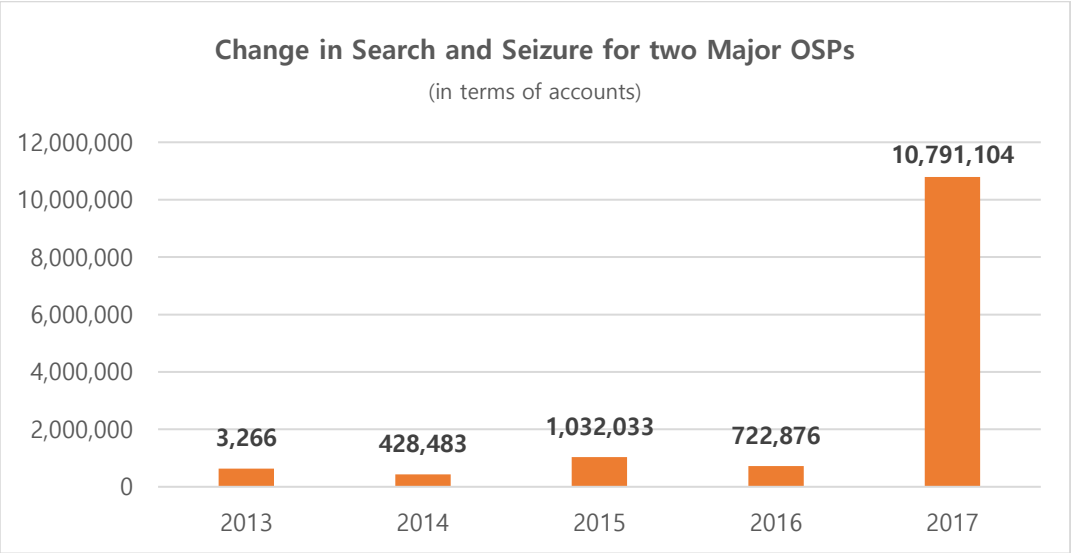
		Naver	Band[7]	Daum	Kakao	Total[8]
2013	Doc.	8,047	-	4,138	2,223	14,408
	Acc.	219,357	-	416,717	-	636,074+α
2014	Doc.	8,188	99	4,398	2,999	15,684
	Acc.	76,379	227	351,787	-	428,483+α
2015	Doc.	7,648	122	3,112	2,301	13,183
	Acc.	223,940	10,649	507,124	290,320	1,032,033
2016	Doc.	6,470	239	2,467	3,981	13,157
	Acc.	92,784	15,291	29,633	585,168	722,876
2017	Doc.	6,541	251	2,168	6,623	9,538
	Acc.	10,079,254	13,792	16,104	681,954	10,791,104

TABLE 9. SEARCH AND SEIZURE FOR 2 MAJOR OSPS, 2013–2017

- Search and seizure for two major OSPs in 2017 numbered 9,538, for 10,791,104 accounts. In 2017, the total number of accounts subject to interceptions, acquisition of communications metadata, and provision of subscriber identifying information for these OSPs was only 23,693. Compared to this, over 10 million accounts subject to search and seizure show that search and seizure is the most prevalent method for internet surveillance.

[7] A group-based social media service run by Camp Mobile, a subsidiary of Naver.

[8] '+α' refers to the number of accounts of Kakao, which has been not counted until 2014.

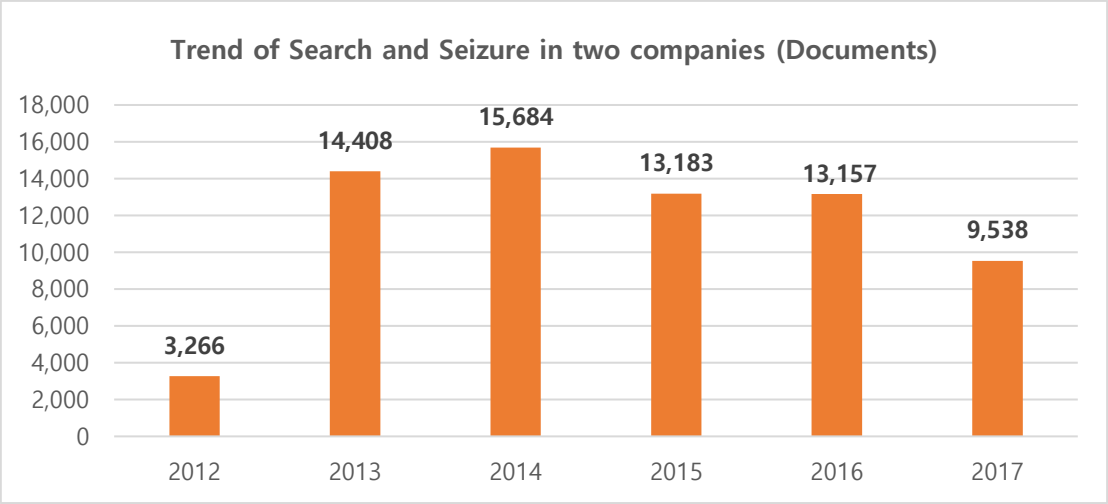


- The number of search and seizure searches for the two companies slowed to about two years since 2015 but jumped 14.9 times year-on-year to 10,791,104 accounts in 2017. The 2017 seizure and search statistics show the rapid increase in governmental activities to monitor the use of the Internet almost without limitation.

- Also, the statistics of two companies that 1,131 accounts per document have been done as search and seizure shows clear evidence of inclusive and overall surveillance. The surge was caused by a single case that obtained 6,963,605 personal information for a certain presidential candidate's alleged violation of the law of personal information protection. It is particularly problematic as search and seizure measures can identify even contents of the communication.

- The surge in search and seizure measures in 2017 could be seen as an optical illusion caused by one case[9] where about 7 million personal information was confiscated for the use of mass e-mailing (Naver Transparency Report 2017). However, in the first half of 2018, the number of information provision made by Naver and Kakao as responses of search and seizure already exceeded 6 million (9 thousand documents). It needs to be analyzed through a longer-term trend whether this increase in size is a temporary phenomenon or a sign of the mass production of search and seizure measures due to emerging issues such as use of macros.

[9] A secretariat staff in the organization chaired by Kim Min-chan, who ran for the 19th Presidential Election, was charged with violating the Privacy Act that he purchased a large amount of e-mail addresses from an illegal collector without the consent of users (Related article: "Kim Min-chan, former presidential candidate, used mass e-mail purchases. Yonhap News Agency. May 25, 2017. http://www.yonhapnews.co.kr/bulletin/2017/05/25/0200000000AKR20170525197300004.HTML).



- The number of cases of search and seizure for two major online service providers tripled in 2013, but since then it is in the trend of decreasing. Some analyze this trend as a result of incompliance of two companies for the subscriber identification. However, the explosive expansion of search and seizure in 2017 shows that it is not merely for the necessary information of users (that can be obtained by subscriber identification if service providers cooperate), but judicial institutions are eagerly utilizing the measures for inclusive surveillance.

IV. Censorship – KCSC's Deliberation and Request for Correction

1. Introduction

A. Overview

There are various ways the government blocks the flow of information on the internet (all kinds of data or knowledge in the form of text, voice or video within the telecommunications network). However, the most prevalent method used in Korea is the Communications Review conducted by the Korea Communications Standards Commission (KCSC)[10]. (Article 21. Act on the Establishment And Operation Of Korea Communications Commission, Article 8. Presidential Decree of the Act[11])

KCSC, upon deliberation, may hand down a "Request for Correction", which refers to a request to the communications service providers (OSPs such as portals including Naver or Daum, ISPs such as KT, Server Hosting Companies etc.) or administrators of community boards to delete or block access to information that KCSC has determined to be requiring deliberation for reasons of illegality or harmfulness to youths (information to be deleted or blocked is by URL, and can encompass the whole website, whole account, SNS contents and postings). The KCSC's Request for Correction, despite its name, is an administrative measure that is *de facto* binding, with about 98% of the compliance rate.

B. Categories of Request for Correction

The categories are as follows.

① Deletion of information: Having the communications service provider (mostly OSPs) to remove the information by URL.

② Blocking Access: for information on the overseas server, having the network operator that provides internet access service (ISPs) to block access to such information in Korea

---

[10] While censorship as a legal term refers to prior censorship, censorship as used in this report shall refer to a wider definition of censorship, in which administration reviews the contents of information and decides whether to block the distribution of such information.

[11] ACT ON THE ESTABLISHMENT AND OPERATION OF KOREA COMMUNICATIONS COMMISSION
ARTICLE 21 (DUTIES OF KOREA COMMUNICATIONS STANDARDS COMMISSION)
4. Deliberation on information prescribed by Presidential Decree as necessary for nurturing sound communications ethics, from among information disclosed to the public and distributed via telecommunication circuits, or requests for correction

③ Termination or Suspension of Use: Termination of the contract between the provider of communications service and the user (contract for the use of sites, blogs, IDs, etc.), or suspending the user's use of the service

④ Ordering display of a 'Harmful Information to Juveniles' Notice, or changing the display thereof

Among the above 4 requests, ①-③ are measures that wholly prevent the flow of the targeted information, and Request for Correction generally refers to these measures. The ④ accounts for less than 1% of the total requests.
(Hereinafter the Request for Correction shall be referred to as "Takedown Request")

C. Information Subject to Deliberation

KCSC may give takedown requests for "illegal information under Article 44-7 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.", and "Information that needs deliberation, such as information harmful to youths, etc." (Article 21. Act on the Establishment And Operation Of Korea Communications Commission, Article 8. Presidential Decree of the Act). Illegal information under Article 44-7 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. refers to obscenity, defamation, assault/stalking, technical damage, harmful information for youths for commercial purposes that is not in compliance with display obligations, speculation, disclosure of state secrets, violation of National Security Act, and other information for criminal purposes.

"Information that needs deliberation, such as information harmful to youths, etc." is not specific in definition and thus there is some room for discussion in the actual scope of the information subject to takedown request, but the KCSC, following 'Deliberation Rules for Communications' (KCSC Regulations 38), gives out takedown requests to wholly delete or block the information if it finds such information to be 'harmful information', even if it is not 'illegal information' per se.

D. Procedures and Effect

Information subject to takedown requests is first recognized by the KCSC through citizen's reports. Related agencies request for deliberation, and KCSC monitors. The recognized information, after

reviewing by the secretariat, is deliberated by the communications subcommittee for the final decision on takedown request.

The internet service provider or community board administrator (hereinafter 'service provider') are given notice of the takedown requests, and the service providers are obligated by law to inform the KCSC of the result of the takedown requests without delay. With this certain binding effect and the fear of consequences for non-compliant companies, service providers tend to follow the takedown requests and delete or block as requested.

For the takedown requests, service providers or the actual user (who posted the information in question) may submit an objection to the KCSC within 15 days of being given notice of the takedown request (Article 8.5, Enforcement Decree of the Act on the Establishment and Operation of Korea Communications Commission).

2. Status and Analysis[12]

A. Number and Ratio of Deliberations, Takedown Requests by Categories

		2014	2015	2016	2017
Total number of deliberations		140,421	158,073	211,187	91,853
Takedown Requests	Total	132,884	148,751	84,872	84,872
	Deletion	24,581	27,650	15,499	15,499
	Termination or suspension of use	10,031	9,821	2,617	2,617
	Blocking	97,095	111,008	66,659	66,659
	Display of 'Harmful Information to Juveniles'	1,177	272	97	97
Determination of 'Harmful Contents to Juveniles'		274	148	148	64
Non-Relevant		7,096	9,174	9,248	6,917

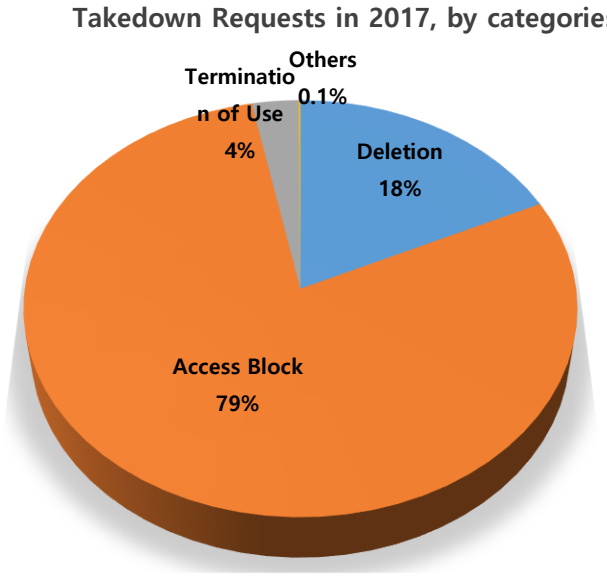
TABLE 10. DELIBERATION AND TAKEDOWN REQUESTS BY KCSC 2014-2017[13]

- In 2017, total of 91,853 information was deliberated by the end of the term of the 3rd KCSC by June 12, and since the second half of 2017 there has been no deliberation at all. Among them 84,872 (92.4%) were subject to takedown requests, with only 6,917 cases (7.6%) determined as 'non-relevant' (information not found to be problematic and allowed to be posted), dismissal, or withdrawal. The deliberation volume by period ratio is similar to the previous year since more tha 90,000 information was deliberated during only the first half of the year.
- Among the takedown requests in 2017 (total of 84,872), 'Blocking access' numbered 66,659 (78.5%), 'Deletion' 15,499 (18.3%), 'Termination or suspension of use' 2,617 (3.1%), 'Others (regarding display of 'harmful information for juveniles')' was 97 (0.1%)[14].

[12] The statistics below is based on data disclosed by KCSC. The categories used follow those used by KCSC, but some of them are not accurate because of duplicate or changed categories, and some of them have been rearranged for the sake of unity.

[13] Note that the 2017 statistics are collected by the end of the term of the 3rd KCSC by June 12. The 2017 figures are subject to minor changes until the official publication of the KCSC almanac (scheduled for late 2018).

[14] For definition of each category of takedown requests, refer to Section V 2 'Categories of Takedown Requests.



- The most numerous takedown requests are 'blocking access' (79% of total), meaning that mostly information on an overseas server was the subject of deliberation (For the information in domestic servers, deletion or termination of use is a usual decision). 'Others' are takedown requests related to the display of 'harmful information to juveniles,' which have been rarely applied - less than 1%, and have fallen even more since 2015. This is probably because the KCSC does not strictly determine whether 'lewd information' or 'harmful information' is 'harmful information for juveniles' but rather, tends to block adults' access to them also by utilizing takedown requests that wholly block or delete such information.
- The number of deliberations and takedown requests has been on a steep rise. Due to the termination of the 3rd KCSC by June 12 and reorganization of 4th KCSC on January 30, 2018, it was not appropriate for trend analysis with 2017 figures. Nevertheless, it is hard not to criticize for being excessive about over 2,000 deliberations per meeting and approximately 17,000 takedown requests per month.

B. Categories of Takedown Requests [15]

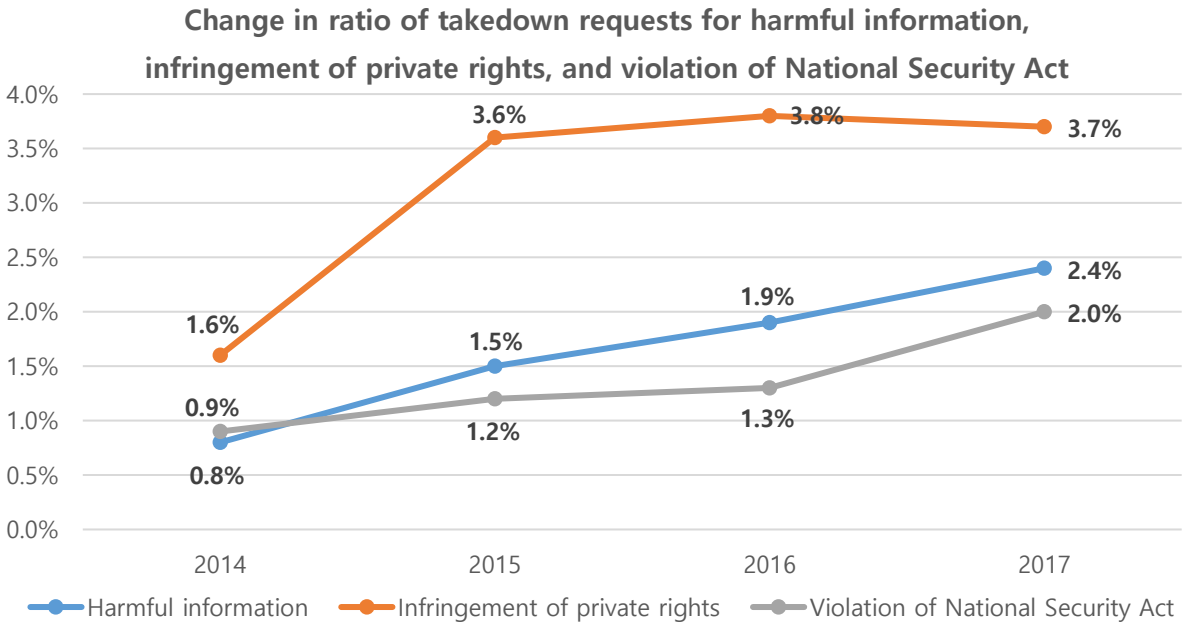
[15] Illegal Information refers to information that have illegal contents or aids and abets such illegal acts, as provided under Article 44-7 (1) Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. and Criminal Code. Harmful information is what, without illegality, is deemed to be against good morals and other social orders. Infringement of Private Rights refer to information in violation of a persons' rights (portrait, defamation, IP, etc.). They are usually put under deliberation upon the person's report, and information violating portrait rights is usually leaked sex videos.

		2014		2015		2016		2017	
		Numbers	Ratio	Numbers	Ratio	Numbers	Ratio	Numbers	Ratio
Illegal	Obscenity / Prostitution	49,737	37.4%	50,695	34.1%	81,898	40.6%	30,200	35.6%
	Gambling	45,800	34.5%	50,399	33.9%	53,448	26.5%	21,545	25.4%
	Medicine, Food	20,160	15.2%	26,071	17.5%	35,920	17.8%	18,556	22.0%
	Drugs[16]	1,725	1.3%	-	-	-	-	-	-
	Illegal Finance	1,694	1.3%	1,620	1.1%	2,234	1.1%	1,349	1.6%
	Personal Information	2,085	1.6%	1,860	1.3%	2,011	1.0%	524	0.6%
	Third Party Transaction	1,959	1.5%	958	0.6%	5,586	2.8%	1,820	2.1%
	Counterfeit	1,961	1.5%	1,973	1.3%	1,493	0.7%	1,225	1.4%
	National Security	1,137	0.9%	1,836	1.2%	2,570	1.3%	1,662	2.0%
	Copyright	-	-	862	0.6%	956	0.5%	976	1.1%
	Etc.	3,541	2.7%	4,916	3.3%	4,274	2%	1,798	2.1%
	Sub-Total	129,799	97.7%	141,190	94.9%	190,390	94.3%	79,655	93.9%
Harmful	Hate Speech	705	0.5%	891	0.6%	2,455	1.2%	1,166	1.4%
	Swears	194	0.1%	549	0.4%	734	0.4%	774	0.9%
	Violence, Cruelty	101	0.1%	535	0.4%	313	0.2%	109	0.1%
	Etc.	0	0.0%	207	0.1%	116	0.1%	0	0.0%
	Sub-Total	1,000	0.8%	2,182	1.5%	3,618	1.9%	2,049	2.4%
Infringement of Private Rights	Portrait	1,706	1.3%	3,768	2.5%	7,557	3.7%	3,129	3.7%
	Defamation etc.	379	0.3%	1,611	1.1%	226	0.1%	39	0.0%
	Sub-Total	2,085	1.6%	5,379	3.6%	7,783	3.8%	3,168	3.7%
Total		132,884	100.0%	148,751	100.0%	201,791	100%	84,872	100%

TABLE 11. STATUS OF INFORMATION SUBJECT TO TAKEDOWN REQUESTS BY CATEGORIES, 2014-2017

[16] From 2015, the figures of "Drugs" have been included in "Medicine, Food".

- In 2017, among the total number of information subject to takedown requests, illegal information numbered 79,655, amounting to 93.9% of the total, while harmful information numbered 2,049 (2.4%), and information violating other's rights numbered 3,168 (3.7%). More specifically, obscene information numbered 30,200 (35.6%), information inciting gambling spirit numbered 21,545 (25.4%), and illegal medicine and food numbered 18,556 (22.0%). The three categories of information, ranking first, second and third in numbers respectively, hold over 88% of the total.
- Takedown requests for violations of the National Security Act have steeply increased, with 0.9% in 2014, 1.2% in 2015, 1.3% in 2016, and 2.0% in 2017. This shows that KCSC and the 'related agencies' – NIS, police, etc. – are exerting more effort to review contents in violation of National Security Act.
- Takedown requests for harmful information have sharply increased, with 0.8% in 2014, 1.5% in 2015, 1.9% in 2016, and 2.4% in 2017.
- Takedown requests for infringement of private rights have also increased, and most of them were an infringement of portrait rights (mainly leaked sex videos). However, takedown requests for defamatory information have decreased since 2015.



- The ratio of takedown requests for illegal information has been slightly falling since 2014. This is troubling when compared with the fact that the number of takedown requests for violation of National Security Act has steeply increased when disagreements exist on the illegality of such information. Also to be considered is the fact that a number of takedown requests for harmful information, which is in practice largely dependent on the discretion of the current committee, has also risen.

C. Takedown Request Status by Cause of Recognition and Related Agencies[17]

	2014		2015		2016		2017	
Complaints	50,892	36.2%	44,565	28.2%	76,207	36.1%	33,007	35.9%
Monitoring	33,944	24.2%	36,447	23.1%	39,270	18.6%	10,384	11.3%
Related Agencies	55,585	39.6%	77,061	48.8%	95,710	45.3%	48,462	52.8%
Sub-Total	140,421	100%	158,073	100%	211,187	100%	91,853	100%

TABLE 12. TAKEDOWN REQUEST STATUS, BY CAUSE OF RECOGNITION 2014-2017

	2014	2015	2016	2017
Ministry of Food and Drug Safety	17,163	24,079	27,988	14,417
Sports Toto (Sports Gambling)	21,114	24,577	-	8,336
K-toto (Sports Gambling)	-	9,047	18,532	-
The National Gaming Control Commission	5,455	6,426	16,702	7,993
Korea Sports Promotion Foundation	-	1,875	834	121
Korea Communications Commission*	1,137	1,838	2,570	1,696
Police Agency	459	2,668	1,739	108
Prosecutors	-	248	1,037	1,876
Financial Supervisory Service	1,835	1,807	1,584	503
Korea Racing Authority	925	1,198	2,809	1,320
Intellectual Property Protection Association	542	232	243	100
Ministry of Culture, Sports, and Tourism	-	507	420	778
Local Governments	5,179	1,682	19,775	9,777
Etc.	1,776	877	1,477	1,437

[17] Based on number of deliberations, not takedown requests

Total	55,585	77,061	95,710	48,462

TABLE 13. TAKEDOWN REQUEST STATUS, BY RELATED AGENCIES, 2014-2017[18]

- In 2017, recognition of KCSC was through requests from related agencies (48,462 cases, 52.8%), complaints (33,007 cases, 35.9%), monitoring (10,384 cases, 11.3%).
- Requests from related agencies are mostly from K-Toto, and the National Gambling Control Commission, which shows that mostly illegal food and drugs, and speculative information are being regulated through reports from the relevant organizations.
- Since 2015, the number of requests from related government agencies has sharply increased exceeding 50 % in 2017. This shows that government agencies are exerting more effort to regulate and censor information on the internet, largely depending on KCSC's takedown requests.

F. Rate of Compliance with the Takedown Requests and Appeals to the Takedown Requests

	2014	2015	2016	2017
Portals	99.7%	99.8%	99.5%	98.8%
Network Providers	100%	100.00%	100%	100%
Others	97.9%	88.3%	87.7%	80.3%

TABLE 15. RATIO OF COMPLIANCE WITH TAKEDOWN REQUESTS, 2014-2017

- The rate of compliance for service providers and board admins in 2015 is 96%. Internet network service providers (KT, etc.) that block overseas sites have 100% compliance rate without exception, and the rate for portals are also close to 100%. This shows that while Takedown Requests are 'requests' in form, they have *de facto* binding power.

[18] Korea Communications Commission, upon receiving other agencies' report, submits request for deliberation to KCSC. The original agency, such as police, to submit report thereto varies.

3. Major Issues and Current Problematic Cases [19] [20]

A. Removal and Blocking of "Harmful Content"

a. Issue

The scope of KCSC's takedown requests is not limited to illegal contents, but also "harmful contents." Content is determined as "harmful" by KCSC, based on various reasons such as excessive cursing, violence, cruelty, or repugnance. This approach differs widely from other governments' approach, which regulates only clearly illegal contents, and/or blocks harmful contents only from minors. The takedown requests of harmful content by KCSC is problematic for the following reasons.

Harmful content, while arguably not educational or helpful, is still protected by freedom of speech, and adults should not be denied access to them. We should remember that curses or repugnant speech also are effective ways to convey underlying emotions. Also, they directly show a person's thoughts, thereby stimulating evaluation and discussion of such thoughts in the "free market of ideas."

Assuming for the sake of argument that harmful content should be regulated in order to protect minors, any regulation should be allowed only to the extent of minor's access to them. Completely denying adult's access to such content is equivalent to the State forcing the standards of an adult's right to know to be lowered to the level of the minors. In addition, the concept of "harmfulness" is inherently subjective and abstract, and governmental restriction of speech based on such concept is on shaky grounds. Our democracy is built on the free flow of ideas, and the Constitutional Court of Korea has found that information subject to KCSC's takedown requests should be limited to

[19] The deliberation by the KCSC in 2017 was conducted only until June 12, the expiration of the third committee, and was not conducted until February 2018 when the fourth committee was launched. As a result, the number of annual deliberations was reduced by half, and the number of problematic cases was somewhat small. However, as more than 90,000 information was deliberated only in the first half as shown in Table 10, the volume of deliberation was similar to the previous year. Minutes of each deliberation can be found on the homepage of the KCSC (Notice - Sub-committee Deliberations -Minutes of communications sub-committee)
http://www.kocsc.or.kr/04_know/communication_SCommittee_List.php (Korean).

[20] The second half of 2017 – first half of 2018. Refers to 2015, 2016, 2017 KRIT report for problematic cases for previous periods.

"illegal and other similar information."

b. Current Problematic Cases

① Distortion of history

- There was a case in which the postings on a website claiming that the North Korean military was involved in the 5.18 Democratization Movement were deleted because they distorted history (at the 18th KCSC - subcommittee in 2018). At that time, the existence of the May 18 Democratic Movement Act, which was enacted in March 2018 and is expected to take effect in September was mentioned as one of the reasons for the deletion. The decision to delete was reviewed by claims of the posters, but it stays. In the review, the opinions of the subcommittee members were split: majority of members argued that the information should be deleted as the rumor of North Korean military intervention is an expression of hatred against historical events with victims which has recently been actively discussed. On the contrary, one member argued that the information should not be deleted because of the issue of freedom of expression that could be infringed on Internet information regulation through the review of harmful information. On these contentious issues, there is a growing need to expand the fundamental basis for deliberation of KCSC.

② Hate speech (discrimination, disparagement)

- The policy for "discrimination and disparagement" is mainly used to review expressions of hatred toward minorities, including women, certain locals, disabled people, and immigrants. It promotes hostile, threatening and degrading biases against a particular group, usually by gender, nationality, or region, with no rational reason, by using deprecating or disgusting expressions. Articles expressing misogyny and disparagement by men against women have been reviewed around certain community sites, and recently increasing postings of their counterparts expressing anger and disgust against men. This tendency of new conflicts raises the need for deep-dive principles of deliberation as it shows both the critics on the censorship which risks the unnecessary control of information which does not have the possibility to lead hatred towards minorities and the dangerousness of the hatred expression itself.

B. The illegality of individual information and websites

- The KCSC's takedown requests must be conducted based on whether the contents of information itself are illegal. If a statement is censored solely due to a possibility of illegality, or if a whole website is blocked due to the fact that the website happens to have numbers of illegal information, then the right to know and to use such statement or website for a lawful purpose is violated.
- In the same vein, KCSC sometimes cites the impracticality of reviewing multiple individual contents within a single account or website and blocks the whole account/website. In such cases, even legal contents within the account/site will be blocked as well, and inevitably results in excessive administrative regulation thereon.
- Due to the continuous critics, there are few cases now where a correction request is decided on for the entire site. Nevertheless, The KCSC members still argue such needs for correction of the entire site. There are remarks of members suggesting shutdown of the whole website, or arguing the investigation on the posters and apply them in the review that goes definitely beyond the scope of the authority of KCSC. What is worse is that some members often express the need of consolidation of KCSC rather than securing cautious deliberation.[21]

C. Violation of National Security Act – 'Praising and Inciting'

a. Issue

- It is fundamentally problematic that the KCSC, an administrative body, but not a judicial authority, decides whether the contents are illegal and regulates the contents. The decision on the application of the law and whether it is illegal or not should be left to an independent

[21] In the deliberation of dcinside.com postings (at the 2nd deliberation sub-committee meeting of the 4th KCSC), the argument to shutdown the whole website was raised as well as the discussion about possible investigation of the user who posted the postings through the website manager

judicial institution because not all the KCSC committee members are legal experts, and the administrative body is likely to be affected by government power. However, the KCSC are deciding to delete or block information that is not clear of illegal or illegal. The problem is especially serious in cases where it is difficult to judge the illegality of the expression, such as defamation or violation of the National Security Law. What is particularly worrisome is that the number of violations of the National Security Law is on the rise.

- Article 7 (1) of the National Security Act(the "Act") provides: "Any person who praises, incites or propagates the activities of an antigovernment organization, a member thereof or of the person who has received an order from it, or who acts in concert with it, or propagates or instigates a rebellion against the State, with the knowledge of the fact that it may endanger the existence and security of the State or fundamental democratic order, shall be punished by imprisonment for not more than seven years."

- This article criminalizes the speech itself, without requiring a criminal act, and thus is subject to criticism on its unconstitutionality. The UN Human Rights Council has also recommended its deletion.[22] The Supreme Court has held that this article must be limited to the circumstances where the speech endangers the existence and security of the nation, or where there is a clear and present danger of harm to the democracy. However, KCSC repeatedly deletes posts that do not contain any aggressive expressions towards South Korea, but which are simply sympathetic to North Korean claims and/or ideologies or praises and glorifies the North Korean government.

D. Defamation

a. Issue

- Korean defamation law prosecutes truthful claims as well as false claims, a trap which accusatory or critical articles can often fall into. If a statement of fact is published solely for public interest

[22] UN Human Rights Committee, Kim v Republic of Korea (574/94)

without the purpose of defaming another person and is true or the person reasonably believed it to be true, then it is not punishable as defamatory. The above standard requires a delicate balancing test by a judiciary body, but KCSC takes it upon itself to undertake such judgment.

- Questions on public figures or consumer review on a product/service have high public value, and thus more weight should be given towards freedom of expression and right to know. Therefore, such posts should not be deleted hastily, but KCSC has several times deleted posts, claiming that if the identical posts were posted on several forums or if a post used excessive swear words, the posts were made for 'defamatory purpose.'

E. Obscenity

a. Issue

- According to the Supreme Court, 'obscenity' is something that (1) violates the sexual morals by arousing sexual desires of ordinary persons and harming the normal sense of sexual shame; (2) depicts or expresses sexual organs or acts indecently to the degree that it inflicts damage or distorts the personal dignity or value of human beings who deserve respect or protection, beyond merely showing simple vulgarity or indecency; and (3) does not have any literary, artistic, ideological, scientific, medical or education values, but merely invokes sexual interests as a whole or predominantly does so in light of social norms. (2006do3558, Decided March 13, 2008)
- The lengthy definition above shows the difficulty of determining whether certain content is "obscene," but KCSC routinely censors about 5,000 contents due to obscenity per month. Many of them are simple images of male/female genitals, without any allusion to sexuality or sexual acts. Also, novels displayed in personal blogs, which contain a sexual description, the magnitude of which do not exceed sexual descriptions often found in published literature, are sometimes removed as obscene content.

F. Deliberation on Personal Broadcasting Videos

a. Issue

- The Internet personal broadcasting website is basically an internet platform service that mediates the distribution of video contents produced by a number of unspecified Internet users in real time. In other words, Internet personal broadcasting contents are expressions of the general public, and most of them are transmitted in real time. However, KCSC does not understand the characteristics of this internet service but obsesses over the term 'Broadcasting,' and, it is strengthening its deliberation authority with the standards applied to the broadcasting.

b. Current Problematic Cases

- It was suggested for pornography last year, but was already banned from watching the broadcast in question over time, citing that it had a discussion platform with a discussion frame that was already missing. The review committee had a conflict over the position that regulations on information that could not already be accessed were ineffective and that the broadcasting schedule should be regulated to prevent distribution of similar cases. (9th Review in 2018)
- In July 2018, the subcommittee decided to use "voice transmission" (so-called "black house") to the organizers of the online broadcasting platform (BJ) who sent the voice over the Internet (Internet broadcasting platform). The organizers insisted that the voice in question was not actually a sexual act, but an audio sound designed to arouse viewers' curiosity, but that it was an effective way to prevent a recurrence of sexual acts. In addition, the relevant Internet broadcasting service operators were advised to strengthen autonomous regulations. (38th Parallel in 2018). The channel of the B.J. was already provided only to adult users who accessed through adult authentication, and the review of illegal information was made with no clear judgment on the illegal broadcasting system.

G. KCSC Professionalism and Transparency

a. Issue

- KCSC can be regarded as an actual censorship institution as it can make recommendations such as deletion, blocking, and suspension of account use through deliberation reviews, and the compliance rate is close to 100 %. Nevertheless, the concerns of the expertise of KCSC members continue to emerge. The KCSC does not have the jurisdiction and investigative rights to regulate specific actions, and can only monitor information distribution on the Internet and make recommendations called as 'requests for correction.' Nevertheless, the members call on the Secretariat to monitor the corresponding to the investigation by the judicial investigative agencies or insist on its necessity.
- In principles, KCSC deliberates and recommends for correction in the level of specific information (URL level). However, members often misunderstand the mechanism of Internet technology which is quite different from other media such as broadcast media and stress the necessity of deliberation/regulation of service providers and platforms, and sometimes decide to request excessive corrections to platforms and service providers.
- While it would reinforce its regulating power, KCSC often shows the lack of expertise and professionality. The members of KCSC, in the deliberation of Internet contents, often show a misunderstanding of the issues of deliberation and rely on the related agencies.
- As well as the expertise of Internet technologies and issues they deliberate, the members of KCSC often show the lack of sophistication as public agencies to make public decisions. Even in public meetings, inconsiderate remarks making groundless prejudices towards women sometimes giving sexual humiliation to others, or belittling Internet users related the posting the committee deliberate.

  Despite such issues as qualifications and sophistication of KCSC committee members, the current disclosure policy of deliberation is very limited. The principles of open disclosure allow, in principle, on-site observing at the committee meeting, but the agenda and meeting data used for meetings are rarely disclosed to the observers. The unedited version of meeting transcripts or audio/video recordings of meeting that are necessary for sound monitoring are not disclosed, either.

Ⅴ. Censorship - Deletion Order of Election Commissions: 19th Presidential Election

1. Introduction

- Under the Public Election Act, The Election commissions can request online service providers ("OSPs") to delete Internet postings that violate the Public Official Election Act. The law mandates that an OSP who has received a request must comply immediately. If the OSP does not comply with the order, it shall be subject to fine or criminal punishment (Article 82-4 of Public Official Election Act[23]).
- This system functions as a censorship institution, considering that a national body, not a judicial one, reviews the citizen's expressions and determines whether to ban distribution of those expressions. Especially, expressions about a national election or candidates, which are subject to censorship under this system, are all political expressions and directly linked to the people's right to know, and thus must be more strongly protected. Therefore, it is highly necessary to

[23] PUBLIC OFFICIAL ELECTION ACT Article 82-4 (Election Campaigns by Utilizing Information and Communications Networks)
(3) When the election commission of each level (excluding the Eup/Myeon/Dong election commission) or a candidate has found that any information violating the provisions of this Act was posted on the Internet homepage or its bulletin board or chatting page etc., or that the fact of transmitting it through the information and communications networks, it may demand the person who manages or operates the Internet homepage posting the relevant information to delete the relevant information, or may demand the manager or operator of the Internet homepage handling the transmitted information, or the provider of information and communications services under the provisions of Article 2 (1) 3 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (hereinafter referred to as "provider of information and communications services") to refuse, suspend or restrict the said handling. If a person who manages or operates an Internet homepage or a person who provides information and communications services does not comply with a candidate's request in such cases, the candidate may notify the election commission having jurisdiction over the relevant constituency of the fact in writing, while if the election commission having jurisdiction over the relevant constituency finds that the information that the candidate requests to delete or the information the handling of which the candidate requests to refuse, suspend, or restrict violates any provision of this Act, it may request the person who manages or operates the Internet homepage or the person who provides information and communications services to delete the information or to refuse, suspend, or restrict the handling of such information.
(4) The manager or operator of the Internet homepage or the provider of information and communications services who has received a demand from an election commission pursuant to paragraph (3) shall promptly comply with it.
(5) The manager or operator of the Internet homepage or the provider of information and communications services who has received a demand from an election commission pursuant to paragraph (3), may raise objections to the election commission that has made such a demand within three days from receiving the said demand, and the person who has posted or transmitted the relevant information may do so within three days from the date on which the relevant information was deleted or any handling thereof was refused, suspended or restricted.

monitor whether this authority has been excessively abused or not.

- The People's Solidarity for Participatory Democracy (PSPD) requested the National Election Commission to disclose information on the current status of cyber violations in the 19th presidential election. Regarding the 19th presidential election, a total of 40,222 Internet posts were called for deletion by the National Election Commission in 17 provinces. Against the requests, National Election Commission deleted 352 Internet posts were deleted. Only one case was appealed by OSPs, but it was rejected. Below is an analysis of the status of requests for deletion of illegal posts and the measures conducted by the National Election Commission regarding the 19th presidential election. The original data was obtained by PSPD through request for information disclosure.

-

2. Analysis

A. Requests for Deletion

- Regarding the 19th Presidential Election, the cyber violation identified by National Election Commission was 4.6 times of one in 18th Election.[24]

	Accusation	Investigation Request	Warning, etc.	Deletion Request	Total
18th Election	10	23	9	7,159	7,201
19th Election	42	7	73	40,222	40,344
Increase (% against 18th Election)	32 (320)	16 (69.6)	64 (711)	33,063 (461.8)	33,143 (460.3)

- The following table shows the status of cyber violation of the Election Act regarding the 19th

[24] Source: <Comprehensive Survey of the 19th Presidential Election> published by National Election Commission. p.196.

Election received from the central and regional Election Commissions. The National and Regional Election Commissions issued 42 complaints, 7 investigation requests, 1 transfer, and 71 warnings.

	Actions					Total
	Accusation	Investigation Request	Transfer	Warning	Deletion Request	
Fake News	16	5	1	45	20,111	25,178
Prohibited Reporting of Polls	2	-	-	2	12,083	12,087
Backbiting of Candidates	1	1	-	-	839	841
Demeaning and Insulting Specific Area	1	-	-	-	428	429
Etc.	22	1	-	24	1,761	1,808
Total	42	7	1	71	40,222	40,343

- Deletion requests were 40,222, mainly through Regional Election Commissions (93.4%). Primary reasons were fake news (62.4%), prohibited reporting of polls (30.0%), backbiting of candidates (17.64%), and demeaning and insulting specific area (1.06%).
- There was only 1 case of objection made by online service provider or manager of the website. However, the objection was rejected due to a violation of Article 108 (Prohibition of publication of public opinion polls) of the Public Official Election Act.

Commission	Fake News	Prohibited Reporting of Polls	Backbiting of Candidates	Demeaning and Insulting Specific Area	Etc.	Total
Central	1,939	570	19	2	107	2,637
Regional	37,585	23,172	820	11,513	426	1,654
Total	40,222	25,111	839	12,083	428	1,761

- These actions were made mainly targeted on social networking sites and websites. 75.2% of the total actions were about social networking services, followed by 24.7% on the websites.

	Accusation	Investigation Request	Warning, etc.	Deletion Request	Total
Website	6	5	10	9,945	9,966
SNS	30	2	54	30,269	30,355
Text Message	4	0	8	0	12
E-mail	0	0	1	0	1
YouTube	10	2	0	0	8
Total	42	7	73	40,222	40,344

- Most requests made by Regional Election Commissions were also fake news, prohibition of publication of polls, and demeaning of candidates in order. However, Commissions in Ulsan, Sejong, Gangwon, Chungbuk requests deletion of postings more on the prohibition of publication of polls than fake news.

Commission	Fake News	Prohibited Reporting of Polls	Backbiting of Candidates	Demeaning and Insulting Specific Area	Etc.	Total
Central	1,939	570	19	2	107	2,637
Seoul	3,759	1,129	70	-	233	5,191
Busan	821	598	25	28	90	1,562
Daegu	1,649	855	63	45	32	2,644
Incheon	529	299	15	132	126	1,101
Gwangju	777	168	61	-	1	2,007
Daejeon	1,908	364	111	-	38	2,421
Ulsan	365	629	3	10	15	1,022

Sejong	306	580	-	-	250	1,136
Gyeonggi	5,206	1,012	23	-	368	6,609
Gangwon	399	1,125	12	6	26	1,568
Chungbuk	1,029	1,305	82	4	177	2,597
Chungnam	1,893	142	-	5	40	2,080
Chonbuk	889	811	56	39	16	1,811
Chonnam	1,190	883	23	5	46	2,147
Gyeongbuk	849	330	177	2	14	1,372
Gyeongna,	818	153	13	35	163	1,182
Jeju	785	130	86	115	19	1,135
Total	25,111	12,083	839	428	1,761	40,222

- Under the Public Election Act, a candidate camp can request deletion of posts aimed at a specific candidate. The following table shows the status and results of the application for deletion of information made by four major candidates for the 19th Presidential Election. Moon Jae-in camp requested the deletion of most information about the information related to the allegations against Moon followed by Ahn Cheol-soo, Sim Sang-jung, Hong Joon-pyo in order. For 300 cases out of 352 applications for deletion of four candidates (85.2 %) were not accepted and the information remains.

Candidate	Request			Result			
	Date	No. of Case	Allegation	Deletion	Non-deletion	Blocking Access	Total
Moon Jae-in	2017.02.16.	4	Son's Employment	-	4	-	4
	2017.02.28.	2	Father's North Korean Army	2	-	-	2
	2017.03.05.	174	Father's North Korean Army	39	-	-	39
			LCT allegation	-	129	6	135

	2017.03.10.	29		-	29	-	29
	Sub-total	209		41	162	6	209
Hong Joon-pyo	2017.03.19.	4	Party Primary Poll	4	-	-	4
	2017.04.21.	1	Pig Rutting Agent	-	1	-	1
	Sub-total	5		4	1	-	5
Ahn Cheol-soo	2017.02.14.	123	Military Duty, Involvement in MB government	-	123	-	123
	Sub-total	123		-	123	-	123
Sim Sang-jung	2017.04.30.	1	Political Activities	-	1	-	1
	2017.05.01.	1	Closure of In-party Sexual Assualt	-	1	-	1
	2017.05.02.	1	Fake News	-	1	-	1
	2017.05.05.	1	Blanket Wage	1	-	-	1
	2017.05.06.	5	Closure of In-party Sexual Assualt	-	5	-	5
	2017.05.07.	5	Son's Luxury School	-	5	-	5
	2017.05.08.	1	Closure of In-party Sexual Assualt	-	1	-	1
	Sub-total	15		1	14	-	15
Total		352		46	300	6	352

3. Problematic Cases

a. Deletion of online polls made by citizens

- Article 108(5) mandates specific requirements of polls effectively limit unnecessary political campaigns. However, the cases deleted due to the Article include poll-typed information promote policies. (i.e., information utilizing poll quationing 'who is the most propoer candidate to represent candle lighting people and liquidate deep-rooted evil?') These cases can open space for information provision and policy debates. However, the cases were deleted in the name of posting unauthorized poll results.

b. Deletion of critic and satiric information in the name of 'demeaning.'

- Critics were often deleted in the name of 'demeaning.' Even web postings reconstructed with a candidate's official remarks or postings made with a candidate's previous campaign were also deleted to avoid 'demeaning.' For example, a YouTube video, edited with a candidate's appearance on the air, pointing out that there are differences by linking him with past remarks, was deleted as it was admitted as demeaning candidate.

c. Considerate to the deletion requests made by candidates

- 300 out of 352 (85.2%) requests for deletion made by four candidates (Moon, Hong, Ahn, and Sim) were rejected, and only 46 requests (13%) were accepted for deletion. Only 51 requests out of 209 (24.4%) made by Moon camp, the most requester, were accepted, and none of Ahn camp's request (123 requests) was accepted.

4. Conclusion

- There found cases of deletion that the Election Act were excessively applied regarding 19th Presidential Election in 2017. Even critical or satiric web postings were deleted in the name of 'demeaning' of candidates. Also, only since the information looks like polls, many cases were deleted since Public Election Act mandates specific requirements of election polls. These excessive applications of Election Act can prevent citizens from free expression in the election politics. Fortunately, Election Commissions were considerate to conduct actions to address the deletion requests made by candidates to avoid abuse that candidates can exploit the current Election Act.
- The basic principle for Election Commissions must secure wide freedom of political expression. If the current culture of Election Commissions that inclusively regulates critical or satiric information toward candidates continues, freedom of expression and citizen's rights to know can be shrunk. Thus the effectiveness of representative democracy can be weakened. Fundamentally, Article 82(4) of the Public Election Act that mandates Central and Regional Election Commitions inclusive authority to regulate information on the election should be revised.

VI. Evaluation of Transparency

1. Surveillance

A. Information Disclosure Status

- In accordance with the current Telecommunications Business Act [25] and Protection of Communications Secrets Act[26], Communications Service Providers have a duty to report to the Ministry of Science and ICT biannually on details of communication information submitted to the government for its Interceptions (Communication Restricting Measures), Acquisition of communication metadata (Communication Confirmation Data), and Provision of Subscriber Identifying Information (Communications Data). The Ministry discloses statistical data based on

[25] TELECOMMUNICATIONS BUSINESS ACT Article 83 (Protection of Confidentiality of Communications)
(5) Where a telecommunications business operator provides communications data according to the procedures under paragraphs (3) and (4), he/she shall retain the ledgers prescribed by Presidential Decree, which contain necessary matters, such as the records that communications data are provided, and the related materials, such as the written requests for provision of data.
(6) A telecommunications business operator shall report on the current status, etc. of provision of communications data, to the Minister of Science and ICT twice a year, in accordance with the methods prescribed by Presidential Decree, and The Minister of Science and ICT may ascertain whether the details of a report submitted by a telecommunications business operator are correct and the management status of related materials under paragraph (5).

[26] PROTECTION OF COMMUNICATIONS SECRETS ACT
Article 9 (Execution of Communication-Restricting Measures)
(3) Any person who executes the communication-restricting measures, is commissioned to execute such measures or asked for cooperation therewith shall keep records in which the objectives of the relevant communication-restricting measures, the execution of such measures, the date on which cooperation is made and the object of such cooperation are entered for a period fixed by Presidential Decree.
Article 13 (Procedures for Provision of Communication Confirmation Data for Criminal Investigation)
(7) An operator of the telecommunications business shall, when he/she provides any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies with the communication confirmation data, make a report on the provision of the communication confirmation data twice a year to the Minister of Science and ICT, and keep records in which necessary matters, including the provision of the communication confirmation data, are entered and other materials related to requests for the provision of the communication confirmation data, etc. for seven years from the date on which each of such communication confirmation data is provided.
(8) The Minister of Science and ICT may check on the authenticity of reports made by operators of the telecommunications business under paragraph (7) and the management of related materials, including records, which need to be kept by them.

the reports.

- The statistics show, by each of the three measures, the number of requests by the agencies (prosecutors, police, NIS, others), number of telephones/accounts subject to the above measures, and number of requests by the communications method (wire telephone/mobile phone/internet, etc.). For Communication Restricting Measures (Interceptions), the numbers for normal/urgent measures are each disclosed.

B. Problem and the Road Ahead for Improvement

a. The Ministry discloses only the numbers, but should also endeavor to specify the details

- The purpose of the transparency report is to enable counter-surveillance and evaluation of the public for government's actions. However, the Ministry currently only discloses the total number of the measures, and it is difficult to give an accurate evaluation on whether the government's surveillance is kept under check or not.
- In order for the public to give such evaluations, the Ministry must provide information on, for each surveillance conducted, (1) the reason for surveillance (criminal suspect, etc.); (2) what details were watched (contents of the communications, access logs, identifying information, accounts of the other parties, locations, etc.); (3) what was the scope of surveillance (total period of surveillance, the number of times it was extended, number of accounts subject to each surveillance, etc.); and (4) whether it was normal or urgent, whether it resulted in indictment or guilty decision, etc. Also, overall statistics on these data must also be disclosed.

b. Non-disclosure of the status of surveillance via "Search and Seizure on Telecommunication"

- The most serious problem is that the status of surveillance through search and seizure, which can collect the whole spectrum of data including the contents, metadata, and subscriber identifying information, is not disclosed at all.
- As the Ministry receives a report on the three surveillance processes, there is no reason why it can't receive a report on the status of search and seizure on communication service providers, which is wider in scope and amount than the above three measures.

- According to the recent Transparency Report published by Naver and Kakao, search and seizure for Communication Service Providers seem to be the most prevalent method for internet surveillance, with a massive amount of data collected.

- As seen above, excessive use of search and seizure is suspected. Thus status thereon must be disclosed in detail.

c. Inadequate notice to the party subject to surveillance

- Notice to the party subject to surveillance is a basic matter of transparency. Protection of Communications Secrets Act provides that prior notice must be given for the execution of surveillance under the Act, within 30 days from the day prosecutor submits an indictment, or takes a disposition not to institute any prosecution or indictment.[27] However, all dispositions taken in regards to criminal proceedings must be given notice to the person subject to such disposition, at the time such disposition is conducted, in accordance with the procedural due process. If the time of notice is based on the day of the indictment, the subject of surveillance cannot become aware of his/her basic rights being violated during the period of investigations. Therefore, the procedures must be improved to ensure that notice is given to the subject of surveillance at the time the surveillance has been conducted.

- What is more, the actual rate of notice is a meager 38.5%.[28] Without notice being properly given to the subjects of the surveillance, they have no way of knowing they are being watched.

- Also, as the provision of communications data does not entail any notice obligations, investigatory agencies and service providers do not give notice to the person subject to surveillance.[29]

---

[27] Article 9-2, 9-3, and 13-3, Protection of Communications Secret Act

[28] "Less than half have been given notice for communications restricting measures, provision of communications confirmation data, and search and seizure " (Press Release by Assemblyman Chung Rae Jung's Office, Oct 19 2014)

[29] If a user wishes to know whether his/her information has been given to the government through provision of communications data, he/she must request the telecommunications providers. Mobile Communications Providers did not give out this information even upon request, but with a High Court's decision on Jan 19 2015, ordering the service provider to compensate the user for emotional damage in the amount between KRW 200,000 and 300,000 for each information not disclosed, the providers are now disclosing such information.

2. Censorship

A. Current Status of Information Disclosure

- KCSC discloses statistics on deliberations and takedown requests of each quarter, by categories and general reasons (gambling, illegal food and drugs, obscenity and prostitution, violations of private rights, and others), and also publishes a white paper triennially with more details. Deliberation committee held semiweekly, can be attended by anyone who applies in advance, and the minutes are uploaded regularly on the home page. Also, it may disclose more specific details upon FOIA Request. But KCSC does not disclose the unedited version of meeting recordings or meeting materials to the public, thus prevent more effective monitoring. Also, they hardly allow the observer to record meetings.
- In terms of election commissions, there is no preemptively or voluntarily disclosed data of deletion order. However, they disclosed data on each case for all deletion orders in response to FOIA request.

B. Problem and Road Ahead for Improvement

a. KCSC and NEC need to disclose data for each deliberation

- For people to evaluate whether the deliberation procedures are conducted properly or not, KCSC should disclose, by each information subject to its deliberation, (1) contents; (2) category; (3) service provider; (4) URL(even partially redacted); (5) how KCSC became aware of the information; and (6) applicable provisions. At the deliberation meetings, the members do not go through every information subject to deliberation, but reviews only important cases or the problematic portion of the information. Therefore, it is difficult for the public to evaluate whether the deliberations are being conducted properly, simply by attending a meeting or reviewing the minutes.
- Also, the NEC should strengthen its transparency by voluntarily releasing data that can evaluate the appropriateness of its system operation, rather than by disclosing the data only when there is a disclosure request.

b. KCSC and Election Commissions need to comply with its obligations to give notice and opportunity to submit an opinion to authors of postings

- Authors of postings having his/her basic rights restricted due to the takedown request by the KCSC were not given notice nor opportunity to submit his/her opinion thereon, because the recipient of the takedown request was the service provider. To rectify this situation, an amendment for the Act on the Establishment and Operation of Korea Communications Commission (amending Article 25 (2) and 6), providing to the person who posted the information in question notice and opportunity to submit his/her opinion, entered into force from Jan 2, 2015. However, KCSC interprets the Act's exceptive clauses widely and has an internal policy that only provides opportunity for prior submission of opinion for information that 'is expected to bring about legal dispute, social controversy, or conflict of interest, thereby requiring careful review', or information that 'exceptionally requires statement of opinion from the party involved'. According to KCSC's internal policy, the secretariat's opinion on such information is considered by the Communications Sub-Committee, which decides whether to provide such an opportunity. As such, clearly illegal information (such as obscenity, prostitution, gambling) or information that is required by law to be deliberated upon within 7 days (violations of National Security Act, etc.) are not given the opportunity to submit opinion, as such information 'requires prompt measures in consideration of public safety and well-being'. Only information falling under the category of violations of rights (defamation, etc.) and information that seem to be open to dispute are given an opportunity for submission of opinion.

- However, prior notice and opportunity to submit opinion is a procedural safeguard that should be granted to all administrative dispositions that limit the rights of or confer obligations on a person, including any takedown requests. The KCSC, by only providing such opportunity on exceptional cases, seems to be confusing the principle with the exceptions. According to the Amendment to the Act, 'exception' to the submission of opinion is provided in Article 25(2), and any other cases that do not fall under this exception should be given prior notice and opportunity for submission of opinion. To meet the procedural due process, anomalous cases that fall under the exception should be decided on a case by case basis of balancing test. Regardless of requirements for prior notice and submission of opinion, as the Amendment (Article 25(6)) does not have any exceptive clauses for post-notice. Therefore, post-notices must be given to the parties without exceptions. Needless to say, these principles should be applied to deletion orders of election commissions as well.

Ⅶ. Conclusion

For internet surveillance, the Ministry of Science and ICT discloses only the numbers of the surveillance and does not disclose the statistics on search and seizure, the most comprehensive measure of all. Therefore, our analysis of search and seizure was based solely on the service providers' transparency report, and as such was limited in properly evaluating the surveillance landscape.

Although the interception, provision of communication metadata, provision of subscriber identifying information have shown similar or decreasing trend compared to last year, the status of search and seizure released by the two major Internet companies has grown as much as 15 times revealing that judicial institutions expand inclusive and vast surveillance. In particular, the explosive expansion of search and seizure measure, almost unlimited surveillance measure, calls for the counter-surveillance of civil society towards the governmental surveillance.

In the case of Internet censorship, the transparency level of the KCSC and the Election Management Committee was rated higher than that of the surveillance. However, as shown by the trend of increasing the number of deliberation and correction requests, censorship is getting significantly higher. Also, the argument of expanding censorship agency is problematic. On the other hand, it is regrettable that the government is reluctant to disclose full raw data of deliberation meeting such as unedited recordings or meeting materials that allow citizens to monitor and respond to the deliberation process effectively.

We found The authority mandated to Election Commissions under the Public Election Act excessively deleted Internet postings even including political critics towards election or candidate while the Act is fundamentally constructed to secure voter's rights by preventing unnecessary political campaign. Particularly, the status of deletion for the cyber violation of Election Act regarding 19th Presidential Election in 2017 shows the likelihood to shrink voter's freedom of political expression and rights to know, thus to weaken the effectiveness of representative democracy. Therefore, it is urgent to adjust the excessive online censorship power vested in Central and Regional Election Commissions.

The government must realize that excessive Internet censorship and surveillance has a chilling effect on the free flow of information, restricts people's freedom of expression and their right to know, as well as hinders internet sector's growth. The government can exercise its power, but only to the extent of fulfilling justifiable purposes.

Also, transparency is essential for people's monitoring, participating in, and improving the administration in a democratic society. Surveillance and censorship lead to violations of people's basic right such as freedom of expression, right to know, right to informational self-determination, right to privacy, and so forth. Therefore, they must be conducted transparently as possible. It is hoped that the government, instead of causing unnecessary distrust and suspicion among people thereby generating social costs, can ensure a higher level of transparency to promote people's trust and fruitful discussions. *<The End>*

• Source of the Data

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 1H 2013

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 2H 2013

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 1H 2014

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 2H 2014

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 1H 2015

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 2H 2015

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 1H 2016

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 2H 2016

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 1H 2017

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 2H 2017

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures, Provision of Communications Confirmation Data, and Provision of Communications Data, 2011-2013 (Response to Information Disclosure Request)

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures, Provision of Communications Confirmation Data, and Provision of Communications Data on Internet, 1H 2014 (Response to Information Disclosure Request)

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures, Provision of Communications Confirmation Data, and Provision of Communications Data on Internet, 2H 2014 (Response to Information Disclosure Request)

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures, Provision of Communications Confirmation Data, and Provision of Communications Data on Internet, 1H 2015 (Response to Information Disclosure Request)

- Ministry of Science, ICT and Future Planning, Status of Communications Restricting Measures, Provision of Communications Confirmation Data, and Provision of Communications Data on Internet, 2H 2015 (Response to Information Disclosure Request)

- Ministry of Science, ICT and Future Planning, Status of Provision of Communications Confirmation Data by Category, 2015 (Response to Information Disclosure Request)

- Ministry of Science and ICT, Status of Communications Restricting Measures, Provision of Communications Confirmation Data, and Provision of Communications Data on Internet, 2016 (Response to Information Disclosure Request)

- Ministry of Science and ICT, Status of Communications Restricting Measures, Provision of Communications Confirmation Data, and Provision of Communications Data on Internet, 2016 (Response to Information Disclosure Request)

- Ministry of Science and ICT, Status of Communications Restricting Measures, Provision of Communications Confirmation Data, and Provision of Communications Data on Internet, 2017 (Response to Information Disclosure Request)

- Naver Transparency Report (https://nid.naver.com/user2/privacycenter/globalInfo.nhn)

- Kakao Transparency Report (http://privacy.kakaocorp.com/en/transparence/report/request)

- Band Transparency Report (http://www.campmobile.com/band/privacyCenter/transparency)

- KCSC, Status of Deliberations on Communications, 2011-1H 2014 (Response to Information Disclosure Request)

- KCSC, Status of Deliberations on Communications, 2014 (Response to Information Disclosure Request)

- 2nd KCSC White Paper (May 2011 – Apr 2014)

- KCSC, Status of Deliberations on Communications, 2015 (Response to Information Disclosure Request)

- KCSC, Status of Deliberations on Communications, 2016 (Response to Information Disclosure Request)

- KCSC, Status of Deliberations on Communications, 2017 (Response to Information Disclosure Request)

- Election Commission, Status of Request for Cyber Violation based on the Public Election Act (Response to information Disclosure Request made by PSPD)

- Election Commission, Number of Deletion of Internet postings based on the Article 82-4(3) of the Public Election Act (Response to information Disclosure Request made by PSPD)

- Election Commission, Number of Objection Requests against the Deletion of Internet postings based on the Article 82-4(5) of the Public Election Act (Response to information Disclosure Request made by PSPD)

- Election Commission, Status of Action against the Cyber Violation at the 19th Presidential Election (Response to information Disclosure Request made by PSPD)

* The above data and other data can be found on http://transparency.or.kr (Korean)