KOREA INTERNET TRANSPARENCY REPORT

한국 인터넷 투명성 보고서

2017

October 2017

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, in order 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 2016 Report, we analyze the status of Korean internet censorship and surveillance focusing on problems and prominent individual cases in 2015, 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 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, in accordance with the Criminal Procedure Act, 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** enables 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	
		Documents	Accounts	Documents	Accounts	Documents	Accounts	Documents	Accounts
Interception[3]	All communications	592	6,032	573	6,678	334	6,302	311	6,683
	All internet	401	1,887	372	1,748	179	998	181	899
	2 major providers	221	556	181	547	75	350	108	193
Communication metadata	All communications	265,859	16,114,668	259,184	10,288,492	300,942	5,484,945	303,321	1,585,654
	All internet	51,367	403,227	32,933	64,721	36,100	65,333	30,753	67,362
	2 major providers	7,990	23,163	6,940	13,857	7,199	13,024	8,003	23,951
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
	All internet	115,194	392,511	114,260	489,916	100,643	423,533	84,302	312,056
	2 major providers	1	17	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

TABLE 1. STATUS OF COMMUNICATIONS SURVEILLANCE 2013-2016

- On average, 453 cases of Interception (acquiring the contents of communications) for all communications per year are conducted for 6,424 accounts. Among them, Interception for internet number 283 per year, for 1,383 accounts, which account for approx. 62% of the total number of Interception (in terms of number of documents).

[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.

- Acquisition of communication metadata (phone numbers, time, locations, etc.) for all communications number 282,327 cases on average per year, for 8,375,940 accounts. Among them, acquisition of communication metadata for internet number 37,788 per year, for 150,161 accounts, which is approx. 1.8% of the total (in terms of 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 has sharply fallen from 2013 (16,114,668 accounts) and 2014 (10,228,492 accounts) to 2015 (5,484,945 accounts) and 2016 (1,585,654 accounts).

- Provision of subscriber identifying information number 1,045,107 cases per year, for 10,347,925 accounts. Provision of subscriber identifying information for internet service subscribers number 103,600 cases per year, for 404,504 accounts. This accounts for about 3.9% of the total number of provision of subscriber identifying information (in terms of number of accounts). Provision of subscriber identifying information, as it does not require court order but only a simple process of request by investigatory agencies, are being conducted on a large scale, and more than 10 million accounts' information, which constitute almost 20% 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 13,157 in 2016, with 722,876 accounts subject to search and seizure. 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.

2. Status and Analysis of Interception on Internet

	Prosecutors		Police		NIS		Military Investigatory Agencies, Etc.*		Total	
	Documents	Accounts	Documents	Accounts	Documents	Accounts	Documents	Accounts	Documents	Accounts
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

TABLE 2. INTERCEPTION ON INTERNET, BY REQUESTING AGENCIES, 2013-2016

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

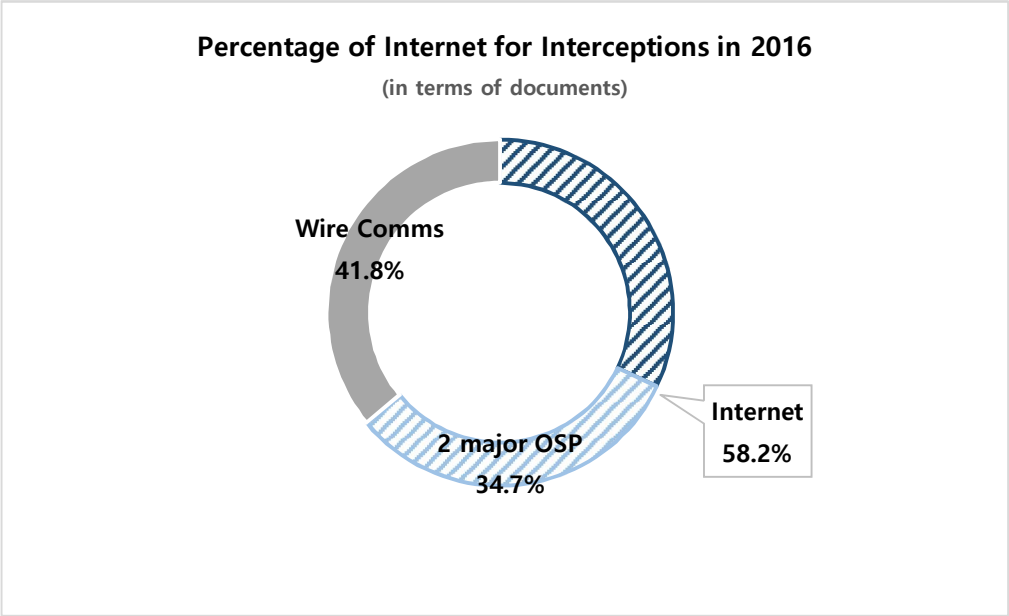
		2013		2014		2015		2016	
		Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts
All communications		592	6,032	573	6,678	334	6,302	311	6,683
All Internet		401	1,887	372	1,748	179	998	181	899
2 Major Providers	**Total**	221	556	181	547	75	350	108	193
	Naver	72	195	56	193	28	127	35	76
	Daum[4]	68	272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

TABLE 3. STATUS OF INTERCEPTION, 2013-2016

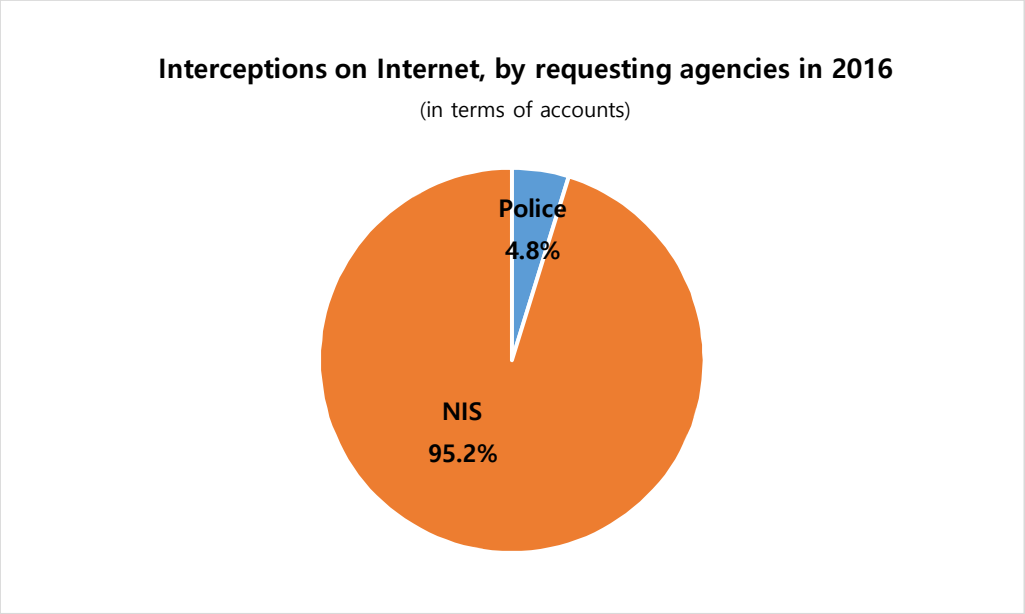
- Interception for internet (acquiring the contents of communications) has been conducted in 2016 after 181 requests, for 899 accounts (5 accounts per document).

- Interception focus on internet. This is because the major means of communications has now become the internet, and acquisition of communications through emails and messenger have become important.

[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.



- 99% of all interceptions (95.2% of interceptions on internet, in terms of the number of accounts) are made by the NIS, and seem to be employed for national security related investigations.



- In October 2016, there was an important Supreme Court decision on online messenger interception. The Supreme Court stated that 'Interception' means to acquire or record contents of telecommunication in real time while the communication is being performed. Therefore, it does not include accessing records or contents of completed telecommunication stored on the communication service provider's server. Thus, the Supreme Court ruled that the interception in this case was illegal, as Kakao (which operates online messenger service KakaoTalk) periodically extracted the contents of the conversation already completed and stored on its server and provided them to the investigation agency. Accordingly, the contents of the KakaoTalk conversation in question was evidence illegally obtained, and therefore inadmissible. (Supreme Court, 2016Do8137, Decided Oct 13 2016)

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

	Prosecutors		Police		NIS		Others*		Total	
	Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts
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

TABLE 4. ACQUISITION OF COMMUNICATION METADATA IN INTERNET, BY REQUESTING AGENCIES 2013-2016

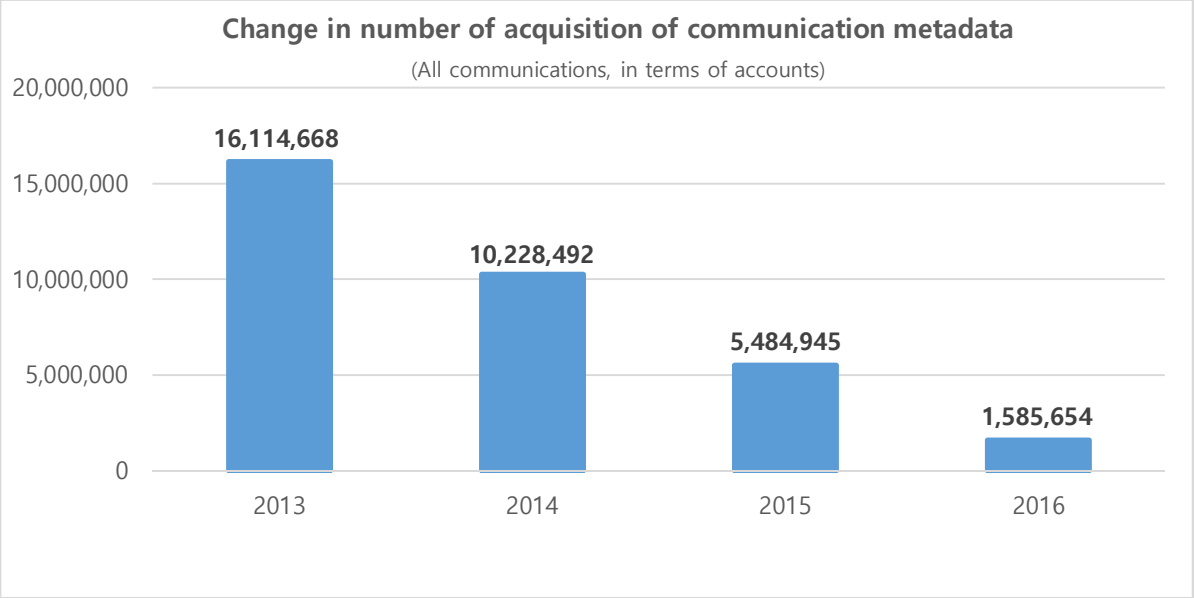
* OTHERS : MILITARY INVESTIGATORY AGENCIES, KOREA COAST GUARD, ADMINISTRATIVE BODIES WITH POLICE AUTHORITIES (KOREA CUSTOMS SERVICE, MINISTRY OF JUSTICE, MINISTRY OF EMPLOYMENT AND LABOR, KOREA FOOD AND DRUG ADMINISTRATION, ETC.)

	2013		2014		2015		2016	
	Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts
All Communications	265,859	16,114,668	259,184	10,288,492	300,942	5,484,945	303,321	1,585,654
All Internet	51,367	403,227	32,933	64,721	36,100	65,333	30,753	67,362
2 Major Providers	7,990	23,163	6,940	13,857	7,199	13,024	8,003	23,951

TABLE 5. STATUS OF PROVISION OF COMMUNICATIONS METADATA, 2013-2016

- Acquisition of communication metadata (calling/receiving number, time, location, etc.) on the internet for the year 2016 was made for 67,362 accounts, in response to 30,753 requests. It takes up approx. 10% in terms of number of documents, and 4.2% 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 is on the rise, and the number of accounts provided by 2 major online service providers (OSPs), Naver and Kakao, has markedly increased from 13,024 accounts in 2015 to 23,951 accounts in 2016.



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

	Documents	Accounts
Call log	268,693	1,523,111
Log record of computer communications or internet	7,513	23,779
Location of the sending cell tower	17,326	19,272
IP addresses	9,789	19,492
Total	**303,321**	**1,585,654**

TABLE 6. ACQUISITION OF COMMUNICATION METADATA IN 2016, BY CATEGORY (ALL COMMUNICATIONS)

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

	Prosecutor		Police		NIS		Others*		Total	
	Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts
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

TABLE 7. STATUS OF PROVISION OF SUBSCRIBER IDENTIFYING INFORMATION, BY REQUESTING AGENCIES, 2013-2016

* 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	
	Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts
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
All Internet	115,194	392,511	114,260	489,916	100,643	423,533	84,302	312,056
2 Major Providers	1	17	0	0	0	0	0	0

TABLE 8. STATUS OF PROVISION OF SUBSCRIBER IDENTIFYING INFORMATION 2013-2016

- Provision of subscriber identifying information for internet in 2016 was conducted for 312,056 accounts, through 84,302 requests.

- In 2016, the provision of subscriber identifying information both for all communications and the internet is slightly decreased. In addition, the provision of subscriber identifying information on the Internet is continuously decreasing, in terms of the number of documents.

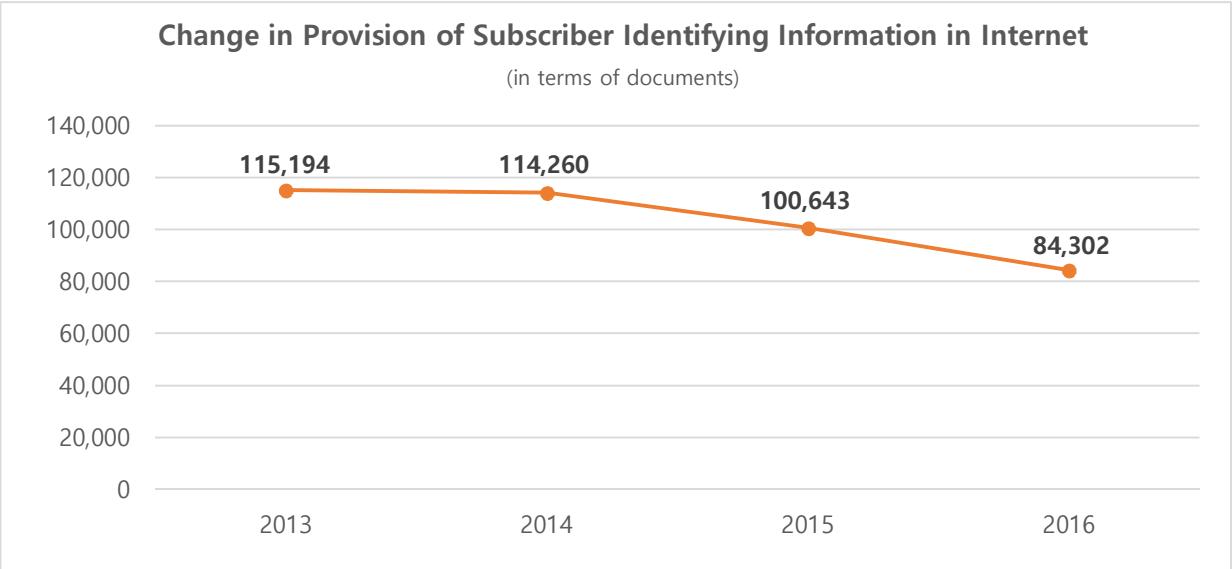
- After a lower court's decision in 2012[5] that ordered a major portal to pay damages for providing subscriber identifying information to the investigatory agencies, when the suspicion of crime was uncertain, major portals ceased to provide subscriber identifying information from 2013. While the Supreme Court in Mar 2016 overruled the lower court's decision[6], 2 major providers

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

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

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).



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	Docs	8,047	-	4,138	2,223	14,408
	Accounts	219,357	-	416,717	-	636,074+α
2014	Docs	8,188	99	4,398	2,999	15,684
	Accounts	76,379	227	351,787	-	428,483+α
2015	Docs	7,648	122	3,112	2,301	13,183
	Accounts	223,940	10,649	507,124	290,320	1,032,033
2016	Docs	6,470	239	2,467	3,981	13,157
	Accounts	92,784	15,291	29,633	585,168	722,876

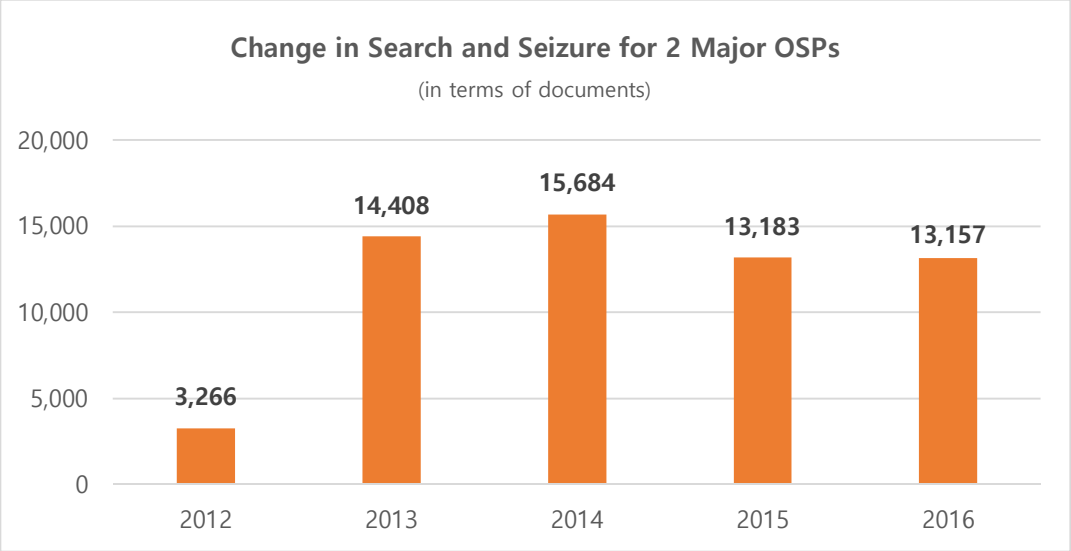
TABLE 9. SEARCH AND SEIZURE FOR 2 MAJOR OSPS, 2013–2016

- According to the above chart, search and seizure for two major OSPs in 2016 numbered 13,157, for 722,876 accounts. In 2016, the total number of accounts subject to interceptions, acquisition of communications metadata, and provision of subscriber identifying information for these OSPs was only 24,144. Compared to this, over 0.7 million accounts subject to search and seizure show that search and seizure is the most prevalent method for internet surveillance.

- Also, accounts for each document is 55, showing that the scope of each search and seizure is very wide and comprehensive. In regards to search and seizure for Kakao, which dominates the online messenger service market with more than 90% of the market share, number of accounts per document is approx. 147. 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.

[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.



- Search and seizure for two major online service providers increased drastically in 2013, more than three times compared to the year before. After 2013, the numbers keep steady until 2015. Naver explains this as a 'balloon effect', with investigatory agencies relying on search and seizure to obtain subscriber identifying information after major portals stopped complying with requests of subscriber identifying information without court orders. However, while it is true that after provision of subscriber identifying information was stopped, the search and seizure increased, it cannot be wholly attributed to a balloon effect. In 2012, provision of subscriber identifying information by the two OSPs was conducted for about 25,000 requests covering about 130,000 accounts, while the increase in search and seizure after provision of subscriber identifying information was stopped was for about 10,000 requests covering at least 300,000 accounts. In other word, while search and seizure certainly could have increase in numbers as a replacement of provision of subscriber identifying information, the increase in the former is not enough to wholly replace the latter. Also to be noted is the fact that comprehensive search and seizure on internet communications (unrelated to provision of subscriber identifying information) has increased substantially.

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)[9]. (Article 21. Act on the Establishment And Operation Of Korea Communications Commission, Article 8. Presidential Decree of the Act[10])

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 overseas server, having the network operator that provides internet access service (ISPs) to block access to such information in Korea

---

9 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.

10 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 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 monitoring. The recognized information, after review 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[11]

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

		2014	2015	2016
Total number of deliberations		140,421	158,073	211,187
Takedown Requests	Total	132,884	148,751	201,791
	Deletion	24,581	27,650	35,709
	Termination or suspension of use	10,031	9,821	8,422
	Blocking	97,095	111,008	157,451
	Display of 'Harmful Information to Juveniles'	1,177	272	209
Determination of 'Harmful Contents to Juveniles'		274	148	148
N/A		7,096	9,174	9,248

TABLE 10. DELIBERATION AND TAKEDOWN REQUESTS BY KCSC 2014-2016

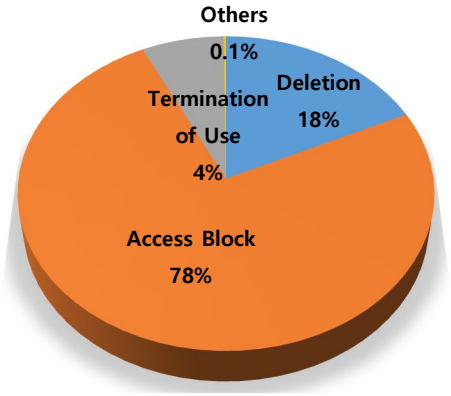
- In 2016, total of 211,187 information was deliberated, and among them 201,791 (95.6%) were subject to takedown requests, with only 9,248 cases (4.4%) determined as 'non-relevant' (information not found to be problematic and allowed to be posted).

- Among the takedown requests in 2016 (total of 201,791), 'Blocking access' numbered 157,451 (78%), 'Deletion' 35,709 (17.7%), 'Termination or suspension of use' 8,422 (4.2%), 'Others (regarding display of 'harmful information for juveniles')' was 209 (0.1%)[12].

[11] 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.

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

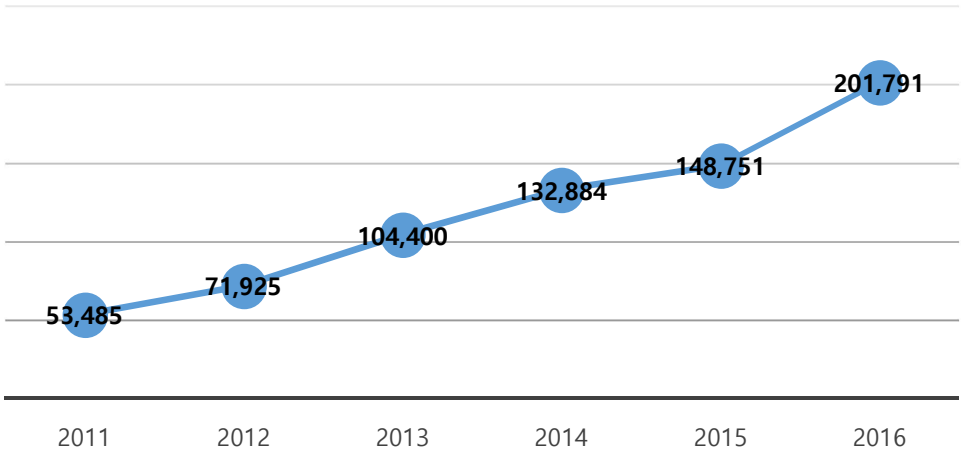
Takedown Requests in 2016, by categories



- The most numerous takedown requests are 'blocking access', meaning that mostly information on an overseas server was the subject of deliberation. '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 to 0.2% in 2015 and 0.1% in 2016. 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. In particular, in 2016, it surged by 1.3 times compared to last year, exceeding 200,000, which is nearly 4 times that of 2011. Over 2,000 deliberations per meeting and approximately 17,000 takedown requests per month were made and it is hard not to criticize for being excessive.

Yearly Increase in Takedown Requests



B. Categories of Takedown Requests [13] [14]

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

TABLE 11. STATUS OF INFORMATION SUBJECT TO TAKEDOWN REQUESTS BY CATEGORIES, 2014-2016

[13] The below is based on the KCSC's categories, and as some of them have changed, the numbers may contain errors. For example, harmful information such as Hate speeches had been counted under "Illegal Information", and illegal information such as obscenity and prostitution had been counted under "Harmful Information".

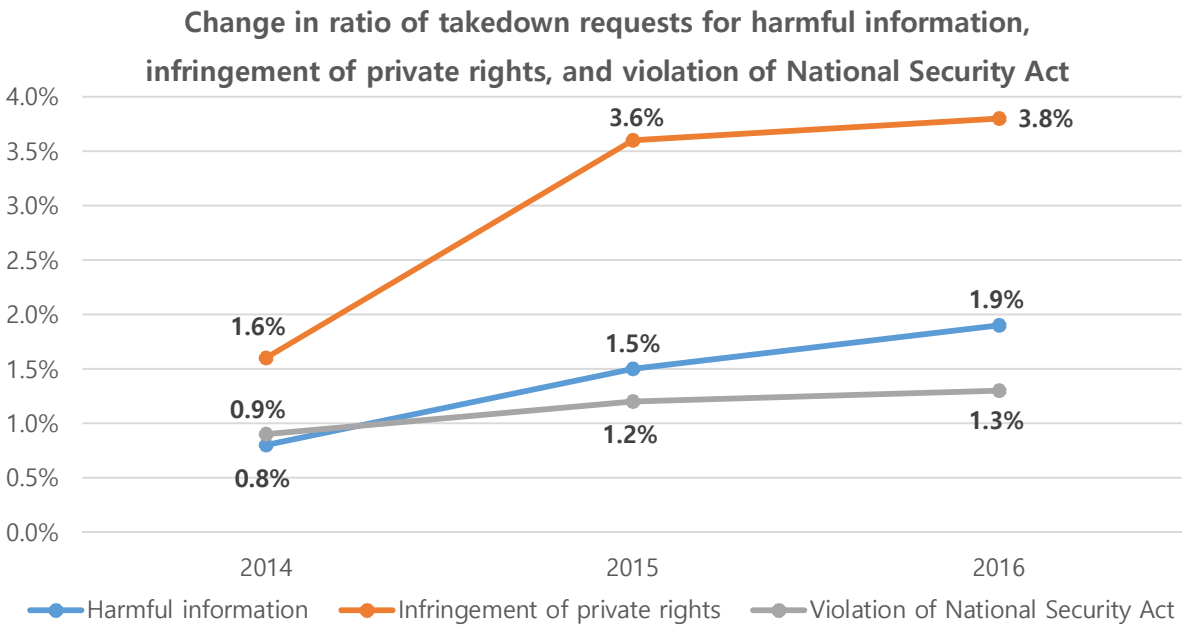
[14] Illegal Information refers to information that have illegal contents or aids and abets such illegal acts, as provided under Article 44-7 (1) Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. and Criminal Code. Harmful information are those that, 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.

- In 2016, among the total number of information subject to takedown requests, illegal information numbered 190,390, amounting to 94.3% of the total, while harmful information numbered 3,618 (1.9%), and information violating other's rights numbered 7,783 (3.8%). More specifically, obscene information numbered 81,898 (40.6%), information inciting gambling spirit numbered 53,448 (26.5%), and illegal medicine and food numbered 35,920 (17.8%). The three categories of information, ranking first, second and third in numbers respectively, hold over 85% of the total.

- Takedown requests for violations of the National Security Act have steeply increased, with 1,137 cases in 2014, 1,836 cases in 2015 and 2,570 cases in 2016. Recognition of such information in 2016 were all through requests by related agencies. 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 2,000 cases in 2014, 2,182 cases in 2015, and 3,618 cases in 2016.

- Takedown requests for infringement of private rights have also increased, and most of them were infringement of portrait rights (mainly leaked sex videos). However, takedown requests for defamatory information have steeply decreased in 2016.



- The ratio of takedown requests for illegal information has fallen from 97.7% in 2014 to 94.9 in 2015 and 94.3% in 2016. This is troubling when compared with the fact that number of takedown requests for violation of National Security Act has increased, when disagreements exist on the illegality of such information. Also to be considered is the fact that number of takedown requests for harmful information, which is in practice largely dependent on the discretion the current committee, has also risen.

C. Takedown Request Status by Cause of Recognition and Related Agencies[15]

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

TABLE 12. TAKEDOWN REQUEST STATUS, BY CAUSE OF RECOGNITION 2014-2016

	2014	2015	2016
Ministry of Food and Drug Safety	17,163	24,079	27,988
Sports Toto (Sports Gambling)	21,114	24,577	-
K-toto (Sports Gambling)	-	9,047	18,532
The National Gaming Control Commission	5,455	6,426	16,702
Korea Sports Promotion Foundation	-	1,875	834
Korea Communications Commission*	1,137	1,838	2,570
Police Agency	459	2,668	1,739
Prosecutors	-	248	1,037
Financial Supervisory Service	1,835	1,807	1,584
Korea Racing Authority	925	1,198	2,809
Intellectual Property Protection Association	542	232	243
Ministry of Culture, Sports and Tourism	-	507	420
Local Governments	5,179	1,682	19,775
Etc.	1,776	877	1,477
Total	55,585	77,061	95,710

TABLE 13. TAKEDOWN REQUEST STATUS, BY RELATED AGENCIES, 2014-2016

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

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

- In 2016, recognition of KCSC was through requests from related agencies (95,710 cases, 45.3%), complaints (76,207 cases, 36.1%), monitoring (39,270 cases, 18.6%).

- Requests from related agencies are mostly from Ministry of Food and Drug Safety, 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, to take up almost 50% of the total number of cause of recognition. This shows that government agencies are exerting more effort to regulate and censor information on the internet, largely depending on KCSC's takedown requests.

D. Location of Information Subject (Mediums subject) to Takedown Requests

	2014		2015		2016	
Blogs, etc.	10,800	**8%**	**18,138**	**12.2%**	**54,323**	**26.9%**
Community, etc.	11,556	**9%**	**4,302**	**2.9%**	**2,629**	**1.3%**
Sites	87,675	**66%**	**106,197**	**71.4%**	**70,538**	**35.0%**
Others (P2P, Webhard)	5,262	**4%**	**5,182**	**3.5%**	**2,900**	**1.4%**
SNS	17,591	**13%**	**14,932**	**10.0%**	**71,401**	**35.4%**
Total	132,884	**100%**	**148,751**	**100%**	**201,791**	**100%**

TABLE 14. INFORMATION SUBJECT TO TAKEDOWN REQUESTS, BY LOCATIONS, 2014-2016

- In 2016, social media and websites are the main locations where the information subject to takedown requests are found. Usually, the entire website is shut down if it is related to obscene or gambling information which are the main subjects of takedown requests.

- Takedown requests for the information on social media has soared in 2016, usually for the reason of obscenity. Even so, it is worrisome that social media, which is considered as a relatively private communication space, is being massively monitored by KCSC.

E. Giving notice and opportunity to submit opinion to authors of postings

- KCSC's takedown request is an administrative disposition that restricts rights and imposes obligations on individuals. However, the notice had only been given to the information technology service provider such as OSPs or ISPs that distributes the information which is subject to KCSC's disposition (in case of information on overseas servers, Korean internet network service providers). The author of the postings or administrators of overseas websites were not given any prior opportunity to submit opinion, nor were they given notice even after the disposition had taken place. In light of the above, a legislation was amended as of Jan 20, 2015.[16]

- However, KCSC has established its internal regulations to give opportunity to submit opinion only when 'careful review is required due to judicial disagreements, social controversy, disagreements among stakeholders are expected, etc., or when the exceptional circumstances call for the submission of opinion by the party'. In accordance with the above internal rule, KCSC only grants opportunity to submit opinion in exceptional cases.

- As a result, only 1,754 cases out of total 148,751 cases of takedown requests were given opportunity to submit opinion (1.2%), and post-notices on the authors were only 19. It was further reduced in 2016, resulting that only 265 cases (0.13%) out of total 201,791 cases of takedown requests were given opportunity to submit opinion.

---

[16] Act on the Establishment and Operation of Korea Communications Commission (Sanctions, etc.)
(2) Where the Korea Communications Standards Commission intends to determine sanctions under paragraph (1) and a request for correction under subparagraph 4 of Article 21, it shall provide an opportunity for the relevant person or his/her agent to state his/her opinion in advance: Provided, That where it intends to determine a request for correction under subparagraph 4 of Article 21, it may choose not to provide an opportunity for the relevant person or his/her agent to state his/her opinion in any of the following cases:
1. Where it is necessary to make an urgent request for correction for public safety and security or welfare;
2. Where it is clearly impracticable or unnecessary to hear the opinion of the relevant person and his/her contact details are unknown;
3. Where it is clearly impracticable or unnecessary to hear the opinion of the relevant person, and a statement of opinion based on a request for correction is deemed unnecessary because the fact that is a prerequisite for the request for correction is objectively proved in accordance with the final and conclusive judgement, etc. made by a court;
4. Where the relevant person clearly expresses his/her intention of relinquishing an opportunity to state his/her opinion.
(6) Where the Korea Communications Standards Commission makes a request for correction, it shall inform the relevant person of whether he/she may institute administrative appeal and administrative litigation against such disposition, whether he/she may object to such disposition, the procedure and period for making a request therefor, and other necessary matters.

- Laws and basic principles on administrative procedures require that concerned party be granted the right to participate and to defend themselves. This principle should be extended to all information subject to KCSC's takedown requests. However, KCSC seems to be confusing principle and exceptions in granting this fundamental, and this is in violation of principle of due process.

F. Rate of Compliance with the Takedown Requests and Appeals to the Takedown Requests[17]

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

TABLE 15. RATIO OF COMPLIANCE WITH TAKEDOWN REQUESTS, 2014-2016

- 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.

	2014			2015			2016		
	Submissions	Accepted	Refused	S	A	R	S	A	R
Objections	24	0	24	21	0	21	17	1	16
Withdrawal	26	23	3	20	19	1	18	17	1

TABLE 16. OBJECTIONS AND WITHDRAWALS, 2014-2016

* S : SUBMISSIONS / A : ACCEPTED / R : REFUSED

- Among 483,426 takedown requests during the period of 3 years, only 126 cases (0.03%) have been subject to objections or request for withdrawal. In 2016, only 35 cases (0.02%) of request for withdrawal or objections have been made among 201,791 cases of takedown requests. This seems to be because the owner of the information (poster or the admin of an overseas website)

[17] Appeals to the KCSC's takedown requests include objections and request for withdrawal. Objections are made based on alleged error of KCSC's decision, and requests a re-deliberation by the KCSC, while request for withdrawal is usually made after change in circumstances on information in question, and requests suspension of the takedown request's effect. Other appeals include administrative appeal and administrative litigation

usually does not receive notice that their information has been deleted or blocked, and as the objection is reviewed by the KCSC itself, many people likely believe that there is low chance of KCSC reversing its position.

- In the case of objections, KCSC rarely overturns its own decision. On the other hand, requests for withdrawal were mostly accepted which seems to be because this request is made for using the blocked URL for other purposes after deleting all alleged illegal information.

G. Breakdown of Each Type of Information Subject to Takedown Requests

a. Obscenity

	Numbers	Ratio
Blocking Access	73,342	89.6%
Deletion of Information	5,021	6.1%
Termination or Suspension of Use	3,327	4.1%
Display of 'Harmful Content to Juveniles'	208	0.2%
Total	81,898	100%

TABLE 17. TAKEDOWN REQUESTS OF OBSCENE INFORMATION IN 2016

- Takedown requests for information of obscenity · prostitution takes up the biggest share, with 81,898 requests. 90% of the requests is 'blocking access', which are mostly directed to closing down websites using overseas servers.

	Numbers	Ratio
Display of genitals	20,733	25.3%
Display of sexual activities	54,958	67.1%
Child pornos	263	0.3%
Prostitution	4,712	5.8%
Others	1,232	1.5%
Total	81,898	100%

TABLE 18. CONTENTS OF OBSCENE INFORMATION IN 2016

	Numbers	Ratio
Complaints	48,096	58.7%
Monitoring	13,797	16.8%
Requests by Related Agencies	20,005	24.4%
Total	81,898	100%

TABLE 19. CAUSE OF RECOGNITION OF OBSCENE INFORMATION IN 2016

- Obscene information are mostly image or videos of genitals and sexual activities, and recognized by complaints (58.7%).

b. Defamation

	Numbers	Ratio
Total deliberations	1,144	100%
Takedown requests	226	19.8%
Dismissal, etc.	133	11.6%
Finding of no defamation	785	68.6%

TABLE 20. RESULT OF DELIBERATION OF DEFAMATION INFORMATION IN 2016

- In 2016, 1,144 cases of defamation were deliberated, among which 226 cases (19.8%) were decided to be given takedown requests, and 785 cases (68.6%) were found to not constitute defamation.

- Out of 188 cases of whether consumer review constitutes defamation, 176 cases (93.6%) were found to be non-defamation or dismissed (non-circulation of information), and only 12 cases (6.4%) were decided to be given takedown requests. We can see that consumer reviews are more easily found to have public value and not constitute defamatory information.

c. Harmful information

	Numbers	Ratio
Complaints	471	13.5%
Monitoring	2,932	83.7%
Requests by Related Agencies	99	2.8%

TABLE 21. CAUSE OF RECOGNITION OF OBSCENE INFORMATION IN 2016

	Hate speech	Swears	Violence, cruelty	Against social order	Others	Total
Numbers	2,455	734	309	13	107	3,618
Ratio	68%	20%	8.5%	0.5%	3%	100%

TABLE 22. CONTENTS OF HARMFUL INFORMATION IN 2016

- Deliberations on harmful information is mostly started by KCSC monitoring (83.7%). Most of them fall under the category of hate speech, swears, violence and cruelty, and takedown requests for 'inciting social unrest' and 'against social order' was made for 13 cases in 2016.

d. Deliberations on Social Media and Personal Broadcasting Websites

- In the case of takedown requests for the information on social media, the main reason of takedown requests is obscenity or prostitution (83.1%).

	Numbers	Ratio
Gambling	10,487	14.7%
Obscenity / Prostitution	59,367	83.1%
Illegal Food and Drugs	354	0.5%
Violation of National Security Act	600	0.8%
Infringement of Private Rights	161	0.2%
Etc.	432	0.6%
Total	71,401	100%

TABLE 23. TAKEDOWN REQUESTS TO SOCIAL MEDIA BY CATEGORIES, IN 2016

- In the case of takedown requests for internet personal broadcasting websites, the biggest reason was excessive swearing (41.8%), followed by obscenity (34.5%) and hate speech (10.9%). Personal broadcasting is essentially a personal form of expression, but KCSC seems to find this kind of medium functions similarly to a public TV, and holding deliberations under this premise.

	Numbers	Ratio
Gambling	4	7.3%
Obscenity / Prostitution	19	34.5%
Swears	23	41.8%
Violence, Cruelty	3	5.5%
Hate Speech	6	10.9%
Total	55	100%

TABLE 24. TAKEDOWN REQUESTS TO PERSONAL BROADCASTING WEBSITES BY CATEGORIES, IN 2016

- Takedown requests on such personal broadcasting websites are mostly suspension of service of the BJs (Broadcast Jockey is a term used for Korean personal broadcasting websites referring to users who broadcast their videos in real-time through their own channel on the websites) which is a temporary suspension of use contract between internet service provider (Africa TV) and user (BJ). BJ then cannot use his/her account in Africa TV for a period of time. This 'suspension of service' functions as a personal sanction on the user, which amounts to an intervention of an administrative body in contractual relationships between private parties. Thus, people question whether KCSC is overstepping its scope of power limited to determining the distribution of information.[18]

[18] KCSC Regulating Afreeca TV - Government in the Business of Censoring private videos? (Opennet Korea, Mar 9 2016) http://opennet.or.kr/11278 (Korean)

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, are 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 a 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 "illegal and other similar information".

[19] 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 2016 – first half of 2017. Refer to 2015, 2016 KRIT report for problematic cases before 2016.

b. Current Problematic Cases

① Swearing

- Some posts that repeatedly used swear words toward 'Samsung' without mentioning of facts were deleted for being 'information that contains vulgar language such as excessive swears (16th, 20th Sub-committee, 2017). Also, posts that contain curses towards no specific target were also deleted. There exist concern that it is excessive to censor posts, the harmfulness of which is unclear.

② Distortion of history

- There were cases where some posts claiming that Dokdo is Japanese territory were deleted for the reason of 'distorting history' (16th Sub-Committee, 2017). There exist concern that it's a violation of freedom of expression to delete a person's post simply because he argued a point of view on history which is different from the one advanced by the state.

③ Hate speech (discrimination, disparagement)

- Deliberations under this category are usually reserved for hate speeches against minorities such as women, residents of a certain region, disabled persons, and migrants. Recently, however, posts in a certain community website that encourage 'male hate' has been deliberated in numbers. There exist criticisms that it is excessive to censor posts that are trivial in nature or do not pose real risk of leading to hate against minorities.

④ Violation of social order

- The category recently causing the most concern is 'information that may significantly incite social unrest' (Article 8 subpara. 3 item k), usually referred to as 'Violation of social disorder' clause. There were a number of cases where internet postings that raised suspicions about the facts announced by the government were deleted under this clause. In 2015, posts claimed that the National Intelligence Service (NIS) was involved in the Sewol Ferry tragedy and the delay in rescue (33rd Sub-Committee, 2015), and posts claimed that various North Korean provocations/attacks were not actually carried out by North Korea, but were simple accidents or staged by the NIS were deleted (61st, 62nd, 63rd, 64th Sub-Committees, 2015). In 2016, the deletion of postings expressed dissent to THAAD (Terminal High Altitude Area Defense, American anti-ballistic missile defense system) deployment in South Korea, referring to the hazards of the THAAD, has been a big controversy (53rd, 54th, 56th, 58th Sub-Committees, 2016).

- An administrative agency censoring people's expressions based on an abstract and authoritarian concept is seen by many as an abuse of power to compel a totalitarian mindset, block criticisms of the state, and control public opinion. As such, there exists a rising concern that it is unconstitutional.

B. Illegality of individual information and websites

a. Issue

- 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 individual multiple 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.

b. Current problematic cases

① KCSC has decided to shut down 2 personal adult broadcasting websites for the reason that those were distributing obscene contents (42nd Sub-Committee 2016, 17th Sub-Committee 2017). There is a criticism that it was inappropriate to decide to shut down the entire websites due to the existing of some illegal contents without considering the characteristic of the Internet platform service that mediates the distribution of video contents produced by a number of unspecified users in real time.

② There was a case where KCSC has misconceived a legitimate game website where real money was not exchanged as an illegal gambling website and decided to shut down the website. After receiving a complaint from the operator, KCSC canceled the decision. KCSC should note that their decision based on erroneous judgement of illegality may lead to the breach of the right to operate business (94th Sub-Committee 2016, 2nd Sub-Committee 2017).

③ There were a number of cases where KCSC decided to block access to webpages that provided proxy programs and methods to bypass blockade and access websites blocked by KCSC as illegal information (7th Sub-Committee 2017, etc.). KCSC's request for correction does not by itself have any binding power on the illegality of the information, and thus information, which provides access to that information subject to request for correction, also is not illegal in any way. KCSC's decision to delete such information without any legal basis but for the reasons of having 'purpose of illegal act and incitement thereof', is therefore questionable.

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

a. Issue

- 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 democratic fundamental 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.[21] 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 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 North Korean government.

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

b. Current Problematic Cases

- On April 21, the Seoul Administrative Court ruled that the Korea Communications Standards Commission (KCSC)'s decision to block access to the "North Korea Tech" website is unlawful, and canceled the decision.
- KCSC, in its 22nd Sub-Committee in 2016, resolved to block access to the North Korea Tech (http://northkoreatech.org), which is a blog run by a British reporter that reports news of North Korean IT, for the reason of it being a 'site that praises and glorifies North Korea in violation of the National Security Act'.
- North Korea Tech is a media that known worldwide for its unique expertise on North Korean IT news. It is based on not only North Korean media but reports from other governments and media. Much of its posts are fact checks on North Korean reports and criticisms of the North Korean stance. Therefore, North Korean Tech is often cited by various media, including Wall Street Journal, Reuter, BBC, as well as South Korean press. It reports North Korean IT issues for academic and reporting purposes, and does not contain any content that 'praises and glorifies' North Korea. KCSC claimed that some of the information in the blog quotes or posts links to reports and data from North Korean media, including the Korean Central News Agency (KCNA; the state news agency of North Korea), thereby violating Article 7 (1) of the National Security Act, or Article 7 (5) of the same Act ("Any person who manufactures, imports, reproduces, holds, carries, distributes, sells or acquires any documents, drawings or other expression materials, with the intention of committing the act as referred to in paragraph (1), (3) or (4), shall be punished by the penalty as referred to in the respective paragraph"). Therefore, the KCSC argued, the blog is an illegal website in violation of the National Security Act.
- However, as can be seen from a simple reading of the text of the relevant clauses in the Act, simple quotes and links to North Korean reports and data for academic and reporting purposes cannot be viewed as a violation of the Act. Even assuming that the quoted or linked information is illegal information and that such information can be blocked individually, there is no escaping criticism that blocking access to the whole website is excessive.
- The Court held that the blocking of a website must be conducted only in an inevitable and exceptional circumstance where the website as a whole can be evaluated as illegal, and therefore it was unlawful to entirely block access to northkorea.org which contains a lot of information that cannot be considered as in violation of the National Security Law. The Court also said that KCSC infringed the principle of "minimum regulation" for blocking the website without sufficient investigation and review.

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 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 has a 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'.

b. Current Problematic Cases

① Some posts blaming a former councilor being involved in a case where he was arrested on a charge of sexual harassment against his daughter, citing news articles, were deleted because he was later found not guilty (39th, 42nd Sub-Committees, 2016).

② A post by an electronics repair service company that compared their repair work with their competitor's work, using some disparaging expression was deleted because such expression has a greater purpose of slandering the competitor than the public interest (25th, 28th Sub-Committee 2017)

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 a 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 of sexuality or sexual acts. Also, novels displayed in personal blogs, which contain sexual description, the magnitude of which do not exceed sexual descriptions often found in published literatures, are sometimes removed as an obscene content.

b. Current Problematic Cases

- KCSC decided to terminate the use of an adult BJ's account which provided explicit strip dance videos without exposing genitals, for the reason of 'providing obscene information' (17th, 21st Sub-Committee 2017). Considering that the BJ's channel was shown only to adult users who accessed through adult authentication, it is doubtful whether such contents should be regarded as illegal pornography with harmful effects that must be blocked even to the adults.

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

- KCSC gave several correction requests (recommendation for voluntary correction) to 'Africa TV,', the largest internet personal broadcasting website in Korea for following cases ; a person swearing was broadcasted live while the BJs were broadcasting an event held by Africa TV (40th, 43rd Sub-Committee 2016), a part of BJ's genital area was accidentally exposed (88th Sub-Committee 2016), an image of genitals was unintentionally exposed while broadcasting the Internet search screen (32nd Sub-Committee 2017), a BJ who broadcasts about travelling Thailand received a correction request for saying that that there are many corrupted police officers in Thailand, so travelers should be cautious about frequent crackdown on foreign travelers (58th Sub-Committee 2016).

Ⅴ. Censorship - Deletion Order of Election Commissions

1. Introduction

- Election commissions has the authority to order online service providers ("OSPs") to delete internet postings that violate the Public Official Election Act. The law mandates that an OSP who has received an order must comply immediately. If the OSP does not comply with the order, it shall be subject to a fine or criminal punishment (Article 82-4 of Public Official Election Act[22]).
- This system functions as censorship, 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 monitor whether

[22] 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.

this authority has been excessively abused or not.

- Korea Internet Transparency Report Project Team filed a FOIA request which demanded to release the deletion order documents of 20th Korean General Election in 2016 against the National Election Commission ("NEC"). As a result, it is revealed that 17,101 internet postings were deleted by election commissions' orders, and there was no objection. Among these data released by NEC, below is the analysis on 4,050 takedown cases made by 3 of main election commissions (the National Election Commission, the Seoul Election Commission and the Incheon Election Commission).[23]

2. Analysis

A. Reasons for Deletion

- The most frequent reasons for deletion orders were: "violation of the restriction on publication of results of public opinion poll" (46.2%), "dissemination of false information" (27.04%), and "slander against candidates" (17.63%).

Reasons	Numbers	Ratio
Violation of the restriction on publication of results of public opinion poll	1,871	46.20%
Dissemination of false Information	1,095	27.04%
Slander against candidates	714	17.63%
Violation of election campaign period	221	5.46%
Interference with freedom of election	9	0.22%
Etc.	140	3.46%
Total	4,050	

TABLE 25. REASONS FOR DELETION ORDERS OF 3 ELECTION COMMISSIONS (NATIONAL, SEOUL, AND INCHEON) IN 2016

[23] This analysis is from the Issue Report by People's Solidarity for Participatory Democracy ("PSPD"), 'Report on Election Commission's Internet Posting Deletion Requests' (Oct 4, 2016).
http://www.peoplepower21.org/PSPD_press/1451830 (Korean)
The data analysis was made by Media Today, PSPD, and Incheon Ilbo, and synthesized by PSPD.

- The table below shows the result divided by each election commission.

Reasons	Numbers		
	National	Seoul	Incheon
Violation of the restriction on publication of results of public opinion poll	368	1,205	298
Dissemination of false Information	498	540	57
Slander against candidates	181	7	526
Violation of election campaign period	101	96	24
Interference with freedom of election	5	0	4
Etc.	10	8	122
Total	1,163	1,856	1,031

TABLE 26. REASONS FOR DELETION ORDERS BY EACH ELECTION COMMISSION (NATIONAL, SEOUL, AND INCHEON) IN 2016

- The most frequent reason for deletion order by NEC was "dissemination of false Information". Postings on candidate Na Kyung Won were most frequently deleted by the orders, followed by postings on candidates Moon Jae In and Ahn Chul Soo.

- Seoul Election Commission most frequently ordered to takedown for the reason of "violation of the restriction on publication of results of public opinion poll".

- Incheon Election Commission has many cases of slander against candidates with over 50% of the total. Among these cases, many postings were criticizing candidate Yoon Sang Hyun.

B. Hosting Websites

Websites that had the largest number of deleted postings were Daum (An online portal website, which includes community, blog est. services) with 992 cases, Twitter with 699 cases, Naver (A Portal website) with 451 cases, Ilgan Best (A community website) with 392 cases, MLB Park(A community website) with 263 cases, and Facebook with 235 cases.

3. Problematic Cases

A. Deletion of postings merely quoting poll results

- Article 108 (6) of the Public Official Election Act states, "Where any person publishes or reports the result of a public opinion poll on election, he/she shall publish or report matters specified by guideline for conducting public opinion polls...". This article aims to restrict mainly publishing or reporting from the press which is influential and has a duty to report fairly, for preventing the public opinion from being distorted.
- However, election commissions have been applying this article to postings of individual voters, demanding the same level of obligation of the press. 1,840 cases out of 1,871 cases of deletion due to violation of this article were postings merely quoted poll results that had been reported in the press. Some of the cases involved postings that are clippings of the poll result reported in the press as it is or screenshots of TV news, and even postings that had merely mentioned the trend of public opinion without quoting any specific number were deleted.

B. Deletion of online surveys citizens participated

- Article 108 (5) of the Public Official Election Act requires certain conditions when implementing polls in order to prevent people from actually election campaigning for a candidate or a party in the name of 'objective public opinion polls'. However, when look at the cases deleted by this article, it appears that most of the deleted postings were not aiming to find out approval rating of a candidate, but rather were attempting to induce citizens to participate and further their political opinion through questions such as 'What is the role of candidate Moon Jae In?' or 'Who does The Minjoo Party of Korea need more, candidate Park Young Sun or Jung Chung Rae?'.

C. Deletion of satirical or critical opinion on candidates as "slander"

- Many postings that criticize candidates were deleted for the reason of "slander against candidates" just because those contained some offensive or derogatory expressions. In the case of candidate Moon Dae Sung, a posting that criticized him for his past plagiarism in his doctoral dissertation which resulted in degree cancellation was deleted. In the cases of candidate Yoon Sang Hyun, over 500 postings which stated a critical opinion on Yoon's military service related issue and divorce were deleted. Also, a satirical expression of an image that photoshopped candidate Yu Seung Min's face into an image of eunuch was deleted as it was deemed to be 'Slander'.

D. Deletion of postings raising suspicion and deletion of a whole posting for part of it being false

- A number of postings that had raised a suspicion on candidate Na Kyung Won's daughter's college admission were deleted for the reason of "dissemination of false information". Also, a number of postings that shared a video clip criticizing candidate Ahn Chul Soo were deleted, even when they merely shared the URL link of the video clip. Other than that, there was a posting deleted because it miswrote the number that a candidate had been elected.

E. Deletion of postings questioning counting-ballots process as "interference with freedom of election"

- The "interference with freedom of election" article aims to punish "a person who interferes with the freedom of election by a deceptive scheme or in a deceitful or unlawful way". The NEC deleted postings that raised suspicions on processes of voting and counting ballot or criticized Election Commissions under the charge of "Interference with Freedom of Election", and it would not be able to escape criticism on their such excessive regulations.

4. Conclusion

- During the 20th General Election period, lots of cases were discovered where election commissions ordered to take down postings including doubts on candidates and critical opinions on them, applying the Public Official Election Act excessively. Also, the fact that postings about a certain candidate were most intensively deleted in a certain district suggests that election commissions unquestioningly accepted deletion requests of candidates without sufficient legal consideration.

- Freedom of political expression must be strongly guaranteed. If expressions which are mere judgement, opinions on candidates or various criticism or raising suspicions on them for the purpose of verifying candidate qualification have to be controlled by censorship, the voters' freedom of expression and the right to know will be seriously chilled and choked. Fundamentally, Article 82-4 of the Public Official Election Act which allows excessive and broad censorship by election commissions needs to be reformed.

VI. Evaluation of Transparency

1. Surveillance

A. Information Disclosure Status

- In accordance with the current Telecommunications Business Act [24] and Protection Of Communications Secrets Act[25], 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

[24] 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).

[25] 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.

Identifying Information (Communications Data). The Ministry discloses statistical data based on 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 accurate evaluation on whether the government's surveillance is kept under check.
- 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 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 report on the three surveillance processes, there is no reason why it can't receive 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 seems to be the most prevalent method for internet surveillance, with 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 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.[26] 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 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%.[27] Without notice being properly given to the subjects of the surveillance, they have no way of knowing they are being watched.
- Also, as 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.[28]

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

[27] "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)

[28] 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.
- 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, 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 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 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 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 does 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.

While the number of surveillance has declined overall in 2016, it is still highly problematic that massive numbers of communications information – approx. 1/5 of the whole population annually – is being provided to investigatory agencies due to their comprehensive and massive surveillance practice.

For internet censorship, the level of transparency is quite high compared to that of internet surveillance, and our analysis was more comprehensive due to KCSC and NEC's disclosures. The largest problem would be the increase in the number of deliberations (takedowns) each year.

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 leads 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 in as transparent manner 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, 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)

- 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)

- 'Report on Election Commission's Internet Posting Deletion Requests' (Oct 4, 2016), Issue Report by People's Solidarity for Participatory Democracy ("PSPD"), http://www.peoplepower21.org/PSPD_press/1451830 (Korean)

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