KOREA INTERNET TRANSPARENCY Report

2015

Oct. 2015

Korea University Law School, Clinical Legal Education Center

Korea Internet Transparency Reporting Team

• CONTENTS

Ⅰ. Introduction

Internet is a medium through which various information, once limited to a select few, can be communicated without time or space limitations, thereby accelerating development of civilization and knowledge. The main reason why such high praises can be laid on internet is because anyone can easily access it. On the other hand, internet can be also used as a tool for illegal activities. Government should not only prevent such danger but also take care to nurture the positive aspects of the internet, by refraining from excessively monitor/censoring the use of internet.

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, may restrict freedom of speech and right of knowledge by abusing its power and unduly collecting a person's information and his/her communications or restricting flow of information.

Korean government can, without judicial prior review, delete or block internet posts, and approx. 0.1 million URLs are being deleted or blocked per year. Also, it is relatively easy for the government to collect an internet user's information, which amounts to approx. 0.6 million users' information per year on average.

With this backdrop, it is very important for the people to know the realities of the government's internet surveillance or censorship. Without knowing the real situations, harder it is 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.

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

Below, we analyze the status of Korean internet censorship and surveillance from 2011 to 2014, and its problems and prominent individual cases, based on the data disclosed by the government (Ministry of Science, ICT and Future Planning and KCSC)[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. Transparency Report published by Naver and Daum 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 case of wire or mobile telephone, the agency may view the contents of the call and text messages. In 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[2]

Category[3]		2011		2012		2013		2014	
		Documents	Accounts	Documents	Accounts	Documents	Accounts	Documents	Accounts
Interception	All communications	707	7,167	447	6,087	592	6,032	570	5,846
	All internet	446	1,815	265	1,654	401	1,887	372	1,748
	2 major providers	n/a	n/a	124	480	221	556	181	547
Communication metadata	All communications	235,716	37,304,882	239,308	25,402,617	265,859	16,114,668	259,184	10,288,492
	All internet	44,850	104,847	42,661	99,091	51,367	403,227	32,933	64,721
	2 major providers	n/a	n/a	9,760	44,553	7,990	23,163	6,940	13,857
Subscriber Identifying information	All communications	651,185	5,848,991	820,800	7,879,588	944,927	9,574,659	1,001,013	12,967,456
	All internet	138,248	915,313	133,912	667,677	115,194	392,511	114,260	489,916
	2 major providers	n/a	n/a	26,778	136,514	1	17	0	0
Search and Seizure	2 major providers*	n/a	n/a	3,266	294,626	14,408	636,074	15,585	428,256

TABLE 1: STATUS OF COMMUNICATIONS SURVEILLANCE 2011-2014

- On average, approx. 580 cases of Interception for all communications per year are conducted for approx. 6,300 accounts. Among them, Interception for internet is number approx. 370 per year, for approx. 1,800 accounts, which account for approx. 64%[4] of the total number of Interception.

---

[2] A more detailed table is available at: http://transparency.or.kr (Korean)

The table is produced with the data from 1) data published by Ministry of Science, ICT and Future Planning, which used the reports by communication service providers ; and 2) transparency report published by Naver and Daum Kakao, in which the number of requests and submitted data is disclosed.

[3] 'All internet' refers to the 'internet, etc' as categorized by the Ministry of Science, ICT, and Future Planning's report, and is a sum of the data reported by communication service providers (OSP such as portals and ISP, etc., excluding wire and wireless communication service providers). 'Two major providers' refer to Naver and Daum Kakao (however, the Kakao accounts in the search and seizure are excluded, as they have not been counted)

[4] In terms of number of documents (in terms of accounts, approx. 30%)

- Acquisition of communication metadata (phone numbers, time, locations, etc.) for all communications number approx. 0.25 million cases on average per year, for approx. 20 million accounts. Among them, acquisition of communication metadata for internet number approx. 43,000 per year, for 0.17 million accounts, which is approx. 1% of the total (in terms of number of accounts), probably because requests are mainly made to operators of mobile telecommunications business, and focused on 'cell tower dump'. The acquisition of these data is on the fall; accounts per document in 2011 were approx. 160, while they are only approx. 40 for the year of 2014. However, the fact that approx. 10 million accounts, amounting to 20% of the total population, are being subject to this Measure annually calls for strict scrutiny.

- Provision of subscriber identifying information is being made in the number of approx. 0.85 million cases per year, for approx. 9 million accounts. Provision of subscriber identifying information for internet service subscribers are being made in the number of approx. 125,000 cases per year, for approx. 600,000 accounts. This takes up about 6% of the total number of provision of subscriber identifying information (in terms of number of accounts). The provision of subscriber identifying information is on the rise, with agencies taking advantage of the fact that this measure does not require court order. 2014 saw the all-time high, with 1,001,013 requests and subscriber identifying information for 12,967,456 accounts provided.

- The data for search and seizure (which can be used for acquiring communications contents, metadata, and subscriber identifying information) on communication service providers are not available from the government. Only data disclosed to the public is the data provided in early 2015 by the two major online service providers in Korea – Naver and Daum Kakakao. According to them, the yearly totals search and seizure for these two providers number approx. 9,000, for approx. 0.45 million accounts on average.[5]. Since search and seizure is made to discern the 'contents' of the completed communications, one may estimate the search and seizure number for all service providers by taking into account the percentage of the two major service providers for the Interception above[6] with the result that information of approx. 1.5 million accounts of internet users or 5 million accounts of users of all forms of communications are being provided via search and seizure in the entire country. If this estimate is reasonable, search and seizure conducted on such a vast scale will be certainly the most serious problem, as it

[5] Search and seizure for Kakao excluded, as the number of accounts is missing

[6] In terms of accounts, approx. 30% of all internet, and 9% of all communications

allows the government to see the contents of the communications.

- If we look at the data provided by the two major service providers, for surveillance for major internet services (email, messenger, community, etc.), it is worrisome that while acquisition of communications metadata and subscriber identifying information is decreasing, powerful methods of surveillance such as Interception – which can see the 'contents' of the communications – and search and seizure – which can comprehensively collect all data including the contents of the communications – is on the rise.

2. Status and Analysis of Interception on Internet

	Prosecutors		Police		NIS		Military Investigatory Agencies*		Total	
	Documents	Accounts	Documents	Accounts	Documents	Accounts	Documents	Accounts	Documents	Accounts
2011	-	-	146	203	270	1,579	30	33	446	1,815
2012	-	-	63	101	188	1,535	14	18	265	1,654
2013	-	-	59	81	334	1,798	8	8	401	1,887
2014	1	1	154	250	213	1,493	4	4	372	1,748

TABLE 2. INTERCEPTION ON INTERNET, BY REQUESTING AGENCIES, 2011-2014

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

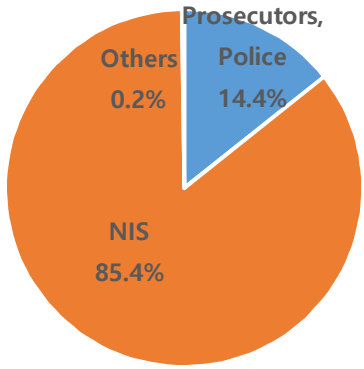
		2011		2012		2013		2014	
		Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts
All communications		707	7,167	447	6,087	592	6,032	570	5,846
All Internet		446	1,815	265	1,654	401	1,887	372	1,748
2 Major Providers	**Total**	n/a	n/a	124	480	221	556	181	547
	Naver	n/a	n/a	30	79	72	195	56	193
	Daum	n/a	n/a	53	324	68	272	47	237
	Kakao	n/a	n/a	41	47	81	89	78	117

TABLE 3. STATUS OF INTERCEPTION, 2011-2014

- Interception for internet (acquiring the contents of communications) has been conducted in 2014 after 372 requests, for 1,748 accounts (4.7 accounts per document).

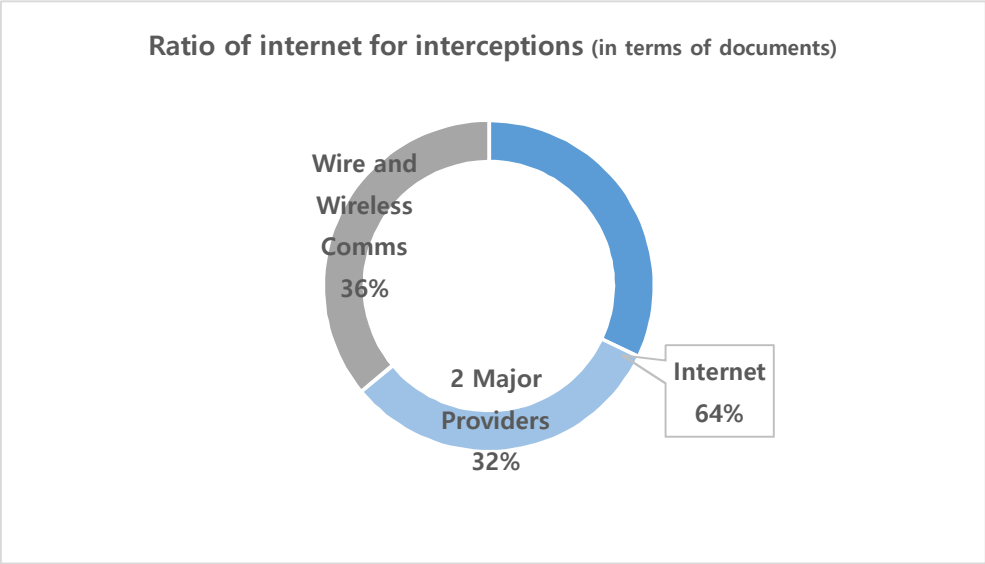
- 90% of all interceptions are made by the NIS, and seems to be employed for national security related investigations. In 2014, 85% of the interceptions were made upon NIS' requests. However, compared to 2011-2013, interceptions by the police was at an all-time high, while that of the NIS was at an all-time low (in terms of the number of accounts)

Interceptions, by requesting agencies in 2014 (in terms of accounts)



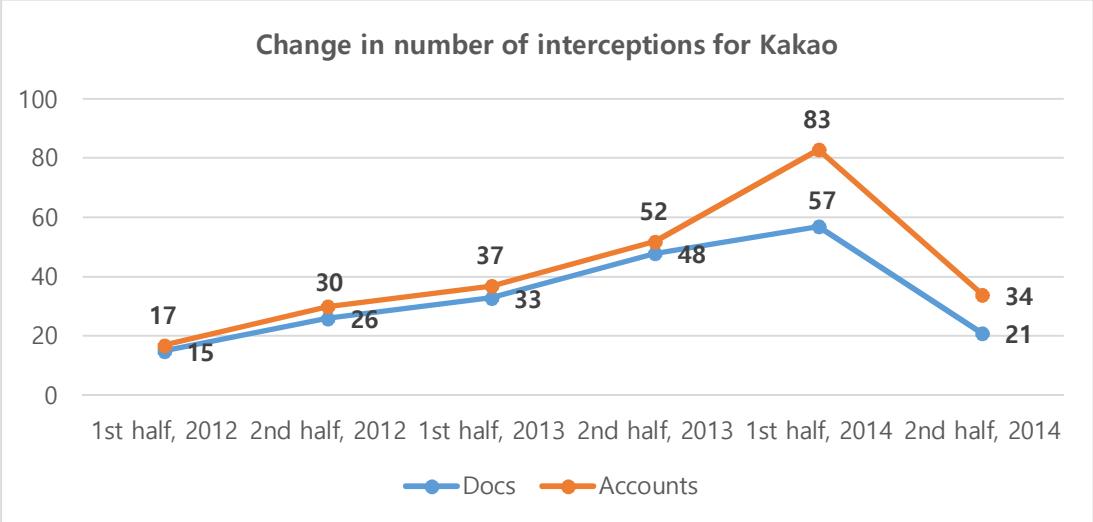
- According to the transparency report published by the two major providers, interceptions for the two firms account for about 50% of the interceptions for internet, and about 32% of all interceptions[7].

[7] In terms of documents (in terms of accounts, approx. 30% of internet, 9% of total communications)



	Naver		Daum		Kakako		Total	
	Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts
1st half 2012	13	51	29	190	15	17	57	258
2nd half 2012	17	58	24	134	26	30	67	222
1st half 2013	31	111	22	120	33	37	86	268
2nd half 2013	41	84	46	152	48	52	135	288
1st half 2014	39	131	28	125	57	83	124	339
2nd half 2014	17	62	19	112	21	34	57	208

TABLE 4. INTERCEPTIONS FOR 2 MAJOR PROVIDERS, 2012-2014



- In terms of number of accounts, the interceptions for all communications is decreasing; however, the interceptions for internet and the two major providers are on the rise. Especially of note is the fact that interceptions for Kakao, which holds more than 90% of the total Korean messenger service, has steeply increased from the first half of 2012 to first half of 2014. This trend can also be found in interceptions for Naver and Daum, which shows that interception is being conducted with increasing focus on major internet services, such as emails, messenger and communities. This is also a reflection of the current move from ground phones towards online messengers as a means of communications.

- The reason for the decrease of interceptions for Kakao in latter half of 2014 can be attributed to the mounting controversy around the prosecutors' announcement threatening massive surveillance on KakaoTalk which began on October 2014 and resulted in Kakao declaring its intention to refuse to comply with Interception warrants[8]. Naver and Daum also saw decreasing interceptions for the second half of 2014.

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
2011	3,133	7,074	38,733	89,601	230	291	2,754	7,881	44,850	104,847
2012	4,485	11,500	35,606	83,366	198	315	2,372	3,910	42,661	99,091
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

TABLE 5. ACQUISITION OF COMMUNICATION METADATA IN INTERNET, BY REQUESTING AGENCIES 2011-2014

* 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.)

[8] South Korea tries to ease cyber surveillance fears (Oct 16, 2014) http://www.reuters.com/article/2014/10/16/us-southkorea-cybersecurity-idUSKCN0I514A20141016
Korean "Digital Refugees": Controversy over Privacy and Surveillance (Oct 21, 2014) http://impunitywatch.com/korean-digital-refugees-controversy-over-privacy-and-surveillance/

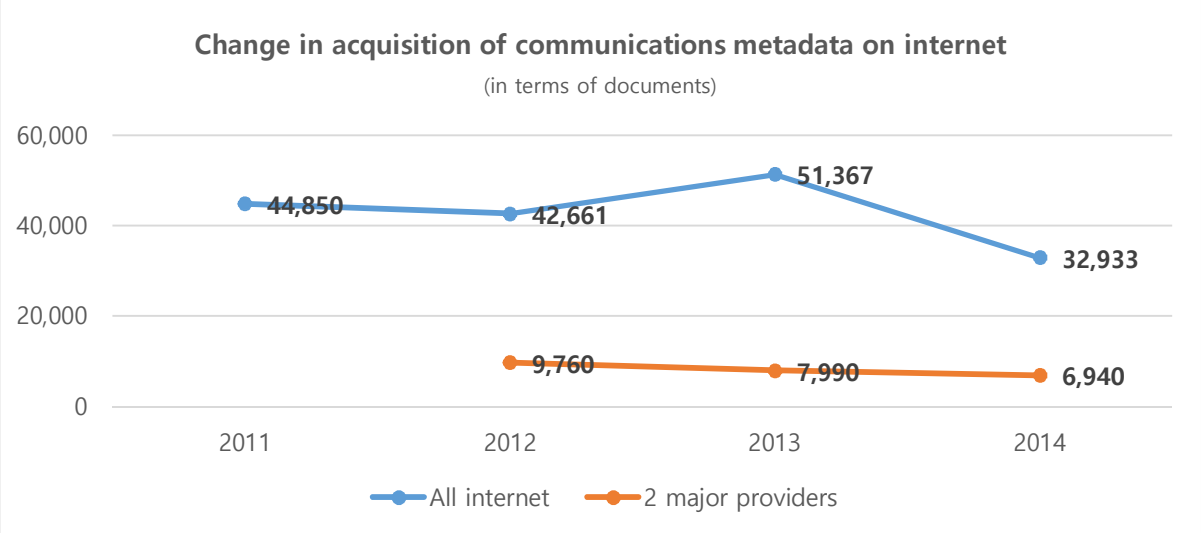
	2011		2012		2013		2014	
	Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts
All Communications	235,716	37,304,882	239,308	25,402,617	265,859	16,114,668	259,184	10,288,492
All Internet	44,850	104,847	42,661	99,091	51,367	403,227	32,933	64,721
2 Major Providers	n/a	n/a	9,760	44,553	7,990	23,163	6,940	13,857

TABLE 6. STATUS OF PROVISION OF COMMUNICATIONS METADATA, 2011-2014

- Acquisition of communication metadata in Internet for the year 2014 (calling/receiving number, time, location, etc.) was made for 64,721 accounts, in response to 32,933 requests, the lowest among 2011-2014.

- The accounts for 2013 increased by 4 times compared to 2012, which can be mainly attributed to the prosecutor receiving a massive amount of data (67 accounts per document) in 2013. As the accounts for Naver and Daumkakao does not show meaningful increase during that period, it seems likely that the prosecutors received the data mostly from internet network providers.

- Acquisition of communication metadata in Internet is slowly decreasing.



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
2011	16,499	81,177	113,158	654,296	3,484	20,488	5,107	159,352	138,248	915,313
2012	16,452	93,451	107,421	500,273	3,910	29,279	6,129	44,674	133,912	667,677
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

TABLE 7. STATUS OF PROVISION OF SUBSCRIBER IDENTIFYING INFORMATION, BY REQUESTING AGENCIES, 2011-2014

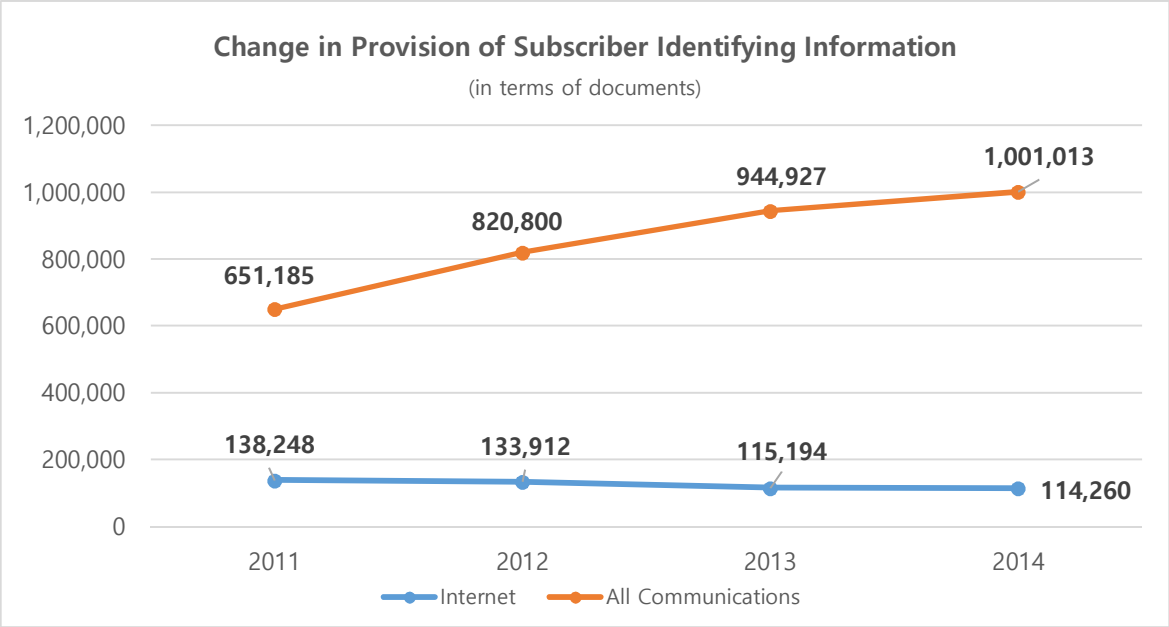
* OTHERS : MILITARY INVESTIGATORY AGENCIES, KOREA COAST GUARD, ADMINISTRATIVE BODIES WITH POLICE AUTHORITIES (KOREA CUSTOMS SERVICE, MINISTRY OF JUSTICE, MINISTRY OF EMPLOYMENT AND LABOR, KOREA FOOD AND DRUG ADMINISTRATION, ETC.)

	2011		2012		2013		2014	
	Docs	Accounts	Docs	Accounts	Docs	Accounts	Docs	Accounts
All Comms	651,185	5,848,991	820,800	7,879,588	944,927	9,574,659	1,001,013	12,967,456
All Internet	138,248	915,313	133,912	667,677	115,194	392,511	114,260	489,916
2 Major Providers	n/a	n/a	26,778	136,514	1	17	0	0

TABLE 8. STATUS OF PROVISION OF SUBSCRIBER IDENTIFYING INFORMATION 2011-2014

- Provision of subscriber identifying information for internet in 2014 was conducted for 489,916 accounts, through 114,260 requests.

- While the provision of subscriber identifying information overall continues to increase, provision of subscriber identifying information on internet is continuously decreasing, in terms of number of documents. After the court's decision in 2012 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. 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 is mostly being provided by internet network service provider.

5. Status and Analysis of Search and Seizure on Internet

- Data on search and seizure for communication service providers (through which contents and metadata of communications as well as subscriber identifying information can all be acquired) are not currently disclosed by the government. Therefore, we have given the below analysis based on the numbers published by Naver and Daum Kakao in early 2015.

		Naver	Daum	Kakao	Total
1st half, 2012	Documents	125	498	231	854
	Accounts	1,753	101,779	n/a	103,532
	Accounts for each Docs	14	204	n/a	109
2nd half, 2012	Documents	1,153	786	473	2,412
	Accounts	167,916	23,178	n/a	191,094
	Accounts for each Docs	146	29	n/a	88
Sub-Total					294,626

1st half, 2013	Documents	3,756	1,771	816	6,343
	Accounts	41,304	108,273	n/a	149,577
	Accounts for each Docs	11	61	n/a	36
2nd half, 2013	Documents	4,291	2,367	1,407	8,065
	Accounts	178,053	308,444	n/a	486,497
	Accounts for each Docs	41	130	n/a	86
Sub-Total					636,074
1st half, 2014	Documents	4,405	2,262	1,651	8,318
	Accounts	58,768	220,223	n/a	278,991
	Accounts for each Docs	13	97	n/a	55
2nd half, 2014	Documents	3,783	2,136	1,348	7,267
	Accounts	17,611	131,654	n/a	149,265
	Accounts for each Docs	5	62	n/a	33
Sub-Total					428,256

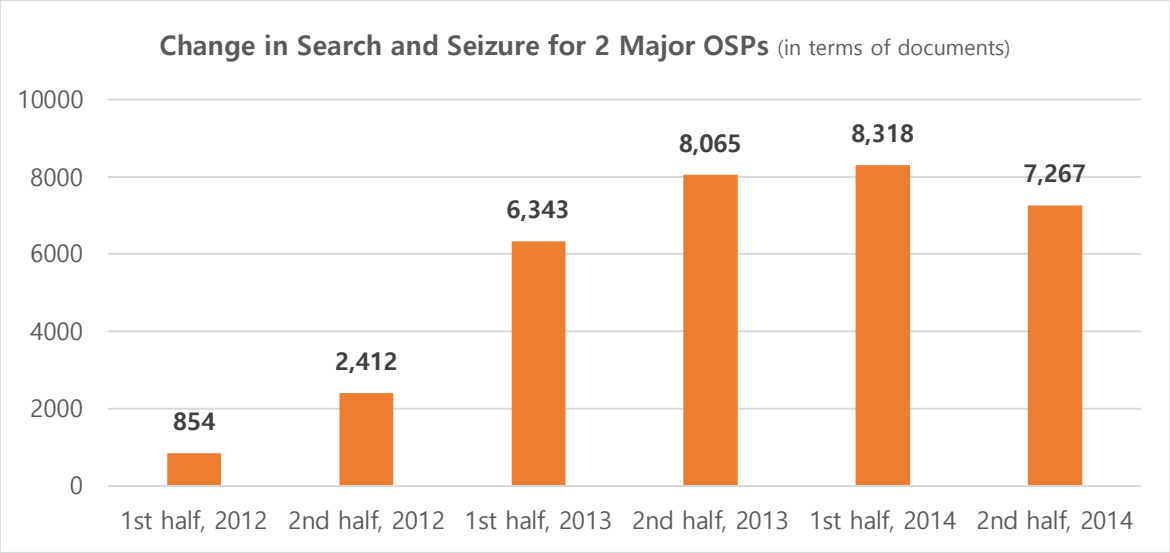
TABLE 9. SEARCH AND SEIZURE FOR 2 MAJOR OSPS, 2012 – 2014

- According to the above, search and seizure for two major OSPs in 2014 numbered 15,585, for 428,256 accounts (Kakao excluded for data being not available). On average, search and seizure for two OSPs alone amount to about 10,000 cases and 450,000 accounts yearly. If we include the data for Kakao, the number of accounts subject to search and seizure would be even more immense. In 2014, the total number of accounts subject to interceptions, provision of communications metadata, and provision of subscriber identifying information for these OSPs is only about 14,000. Compared to this, the 400,000 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 on average 68[9], showing that the scope of each search and seizure is very wide and comprehensive.

[9] Excluding documents for Kakao, as the its accounts have not been counted

- Search and seizure is usually conducted to acquire the contents of communications after they have taken place. Therefore, if we consider the ratio of accounts of two major OSPs for interceptions (about 30% of the whole internet), we can roughly estimate that about 1,500,000 accounts are being affected through search and seizure.



- Search and seizure for the two OSPs are continuously increasing from first half of 2012 to first half of 2014. Especially, we can see that it has increased three times after the beginning of Park administration in 2013. 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, but 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 130,000 accounts, while the increase in search and seizure in 2013 was for about 10,000 requests covering 300,000 accounts. In other words, while search and seizure certainly could have increased in numbers as a replacement of provision of subscriber identifying information, the increase in the number of warrants is too low to cover the lack of provision of subscriber identifying information, and the increase in the number of accounts affected shows that search and seizure with no relation to subscriber identifying information has increased steeply.

- The reason why search and seizure for the two OSPs decreased in late 2014 can likely be attributed to the controversy surrounding the government's threat of massive surveillance of KakaoTalk in October.

IV. Surveillance – Problematic Cases and Issue

1. Surveillance related to Railway Union Strike[10]

During the December 2013 strike by the Railway Union, investigatory agencies have monitored communications of union officials and members who have participated in the strike, citing as the reason investigations into charges of Interference of Business. According to the union and other organizations who have disclosed notice on execution received from investigatory agencies,

- Prosecutors and police have executed search and seizure warrant for the Kakao Talk and Naver Band accounts for leadership of Korean Confederation of Trade Unions, and have seized their Kakao Talk and Naver Band communications made between Dec 19 2013 to Dec 25 2013.
- They have also searched and seized one union member's Kakao Talk and Naver Band account information, and have thereafter acquired subscriber identifying information of other people who have participated in the conversation with that union member between the time of when he have joined the Band to December 2013, as well as details of incoming/outgoing calls and Kakao Talk communication contents during that period.
- They have requested acquisition of communications metadata for one union member's telephone number and Naver Band, and have acquired the following data for the period between Dec 8 2013 to Dec 19 2013: 1) the member's telephone call details (including calls and callbacks, location of the base stations); 2) the Bands he participated in; and 3) subscriber information of other people who participated in the communications with the

[10] "Search and Seizure and Eavesdropping – 'Cyber Inspection' for Kakao, Band, etc. abound" (News Cham, Oct 15 2014) http://www.newscham.net/news/view.php?board=news&nid=86210 (Korean)

"Police accused of real-time monitoring of workers' Kakao Talk and 'cyber shadowing' the families" (News Cham, May 13 2014) http://www.newscham.net/news/view.php?board=news&nid=77976 (Korean)

"Naver Band is not safe from the government! Police has requested the information for the chat buddies and their conversations in the Band where the suspect is a member (News release, Assemblyman Chung Rae Jung's Office, Oct 13 2014) (Korean)

union member; and 4) incoming/outgoing call details.

- They have requested provision of communications confirmation data for the Kakao Talk account of the Railway Union regional director, and have received location data when he was connected to Kakao Talk, during the period of Dec 28 2013 to Jan 16 2014.
- It is also believed that they also acquired telephone / internet access location data for a union member's family member, including internet access location data for a teenager child of a union member, when he/she accessed bank or newspaper webpages.

2. Search and Seizure of Naver Band of Teachers who Criticized the President for the Sewol Ferry Tragedy[11]

In October 2014, investigatory agencies conducted search and seizure for a Naver Band community of teachers who criticized President Park for her response to the Sewol Ferry Tragedy.

Seoul Jongno Police Station announced that it was issued a warrant in early August for the Naver Band, in order to investigate who participated in 'The Second Teacher's Declaration for the Resignation of President Park'. 80 teachers who were members of that Band, on May 28 2014, wrote on the Blue House (Presidential Office) free board that 'We, 80 teachers, cannot stand by and watch while the Ship named Korea is sinking', and that 'President should take responsibility of the whole incident and resign'. Ministry of Education reported the above teachers to the police for a violation of State Public Officials Act, and Jongno Police Station, under the instructions from the prosecutors, began its investigation of the teachers, and conducted search and seizure for the Naver Band of which the teachers were members. The search and seizure resulted in the police acquiring personal information of the teachers, as well as some of the posts made in the Band.

[11] "'Government's Aggression' – Naver Band of the Teachers Criticizing President Park for Sewol Ferry was Cleaned Out (Ohmynews, Oct 14 2014)
http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0002043541 (Korean)

3. Search and Seizure of Kakao Talk of People Involved in Rally / Protests regarding Sewol Ferry Tragedy[12]

It was found that the prosecutors and the police searched and seized KakaoTalk while investigating people involved in Sewol Ferry protests for violations of Assembly and Demonstration Act.

Jin Woo Jung, Deputy Head of Labor Party, was investigated for his actions in holding the "June 10 Blue House People's Assembly', which called for the investigations into the true cause of the Sewol Ferry Tragedy and punishment of the culprits, near the official residence of Prime Minister at Samcheong-dong, and then consequently attempting to march to the Blue House. His Kakao Talk messages, IDs and phone numbers of people who talked with him using Kakao Talk, date and time of the conversations, details of all incoming/outgoing calls, and all pictures in file format during the period of 40 days from May 1 to June 10 were all searched and seized. Among of the Kakao Talk messages searched and seized were his password for his credit card, his work in the Labor Party, his work in the social movement, conversations with his family and friends. Approximately 3,000 people's conversations in dozens of Kakao Talk chat rooms and their phone numbers, details of incoming/outgoing calls, image files were all made part of the search and seizure.

Also, Hye In Yong, a university student who proposed and participated in silent march called 'Stay Still', regarding the Sewol Ferry Tragedy and then taken to the police, also had her Kakao Talk searched and seized. The search and seizure warrant list includes Yong's Kakao Talk ID and chat room nickname, account information of Kakao Talk IDs of people Yong talked with (ID, nickname, date of joining the Kakao Talk, phone number used to authenticate identity when joining, mac address of the phone number, access IP), and conversations, photos, videos Yong shared with other Kakao Talk users during the period of May 12 – May 21. Especially, mac address, which is a distinct number given to Lan cards, etc. for network communications, can be used to track access to base stations and access locations

[12] "Casual Talks of Thousands Also Eavesdropped by the Police – the Worries of 'Kakao Talk Inspection' Now a Reality" (Hankyoreh, Oct 1 2014)
http://www.hani.co.kr/arti/society/society_general/657769.html (Korean)

4. Analysis of the Cases

Surveillance of Social Network Services cannot help being considered excessive, considering the fact that it is conducted not only for the target of the investigations, but also for numerous people who simply participated in conversations with the suspect. The simple act of being in the same chat room is enough to be open to the risk of having one's private conversations disclosed to the investigatory agencies, and because one does not receive any notice thereof, he/she cannot even be aware of his/her communications information being acquired by the investigatory agencies. Also problematic is the common practice to specify as object of search and seizure all communications and details thereof during a certain period, regardless of proximity/relationship to the crime.[13] Also, above cases were mostly for investigations for violations of interference with business (due to strike), Assembly and Demonstration Act, State Public Officials Act (that prohibits political activities of teachers), which are all related to freedom of expression issues. It bears thinking about whether such violations call for investigations involving massive surveillance, and whether such investigations do not infringe upon principle of proportionality. The procedures must be reformed to only request information reasonably limited to the purposes of investigations.

[13] In 2008 and 2009, prosecutors, during the course of investigating about 100 people involved with the violations of Political Fund Act by Kyung Bok Joo, a candidate for the Superintendent of the Seoul Education Office Election held on July 30 2007, have obtained court warrant for, and conducted search and seizure on emails of Mr. Joo and Min Seok Kim (Secretary of Seoul Branch of the Korean Teachers Union) for the period of 7 years, between October 2001 to December 2008. Also, prosecutors have searched and seized emails between Jan 2008 to Aug 2008 of Eun Hee Kim, one of the writers for the MBC PD Notes, which was involved in a criminal proceedings for defamation.

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

1. Introduction

There are various ways the government blocks the flow of information in 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)[14]. (Article 21. Act on the Establishment And Operation Of Korea Communications Commission, Article 8. Presidential Decree of the Act[15])

KCSC, upon deliberation, may hand down "Request for Correction", which refers to its request to the communications service providers (OSP such as Portals, ISP such as KT, Server Hosting Companies etc.) or administrator 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.

2. Categories of Request for Correction

The categories are as follows.

① Deletion of the information: Having the communications service provider to remove the information by URL.

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

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 the Display of 'Harmful Information to Youths' Notice, or changing the display thereof

---

[14] 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.

[15] 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

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 takes less than 1% of the total requests.
(Hereinafter the Request for Correction shall be referred to as "Takedown Request")

3. Information Subject to Deliberation

KCSC may give takedown request 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 fins such information to be 'harmful information', even if it is not 'illegal information' per se.

4. Procedures and Effect

Information subject to takedown requests are first recognized by the KCSC through people'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.

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)

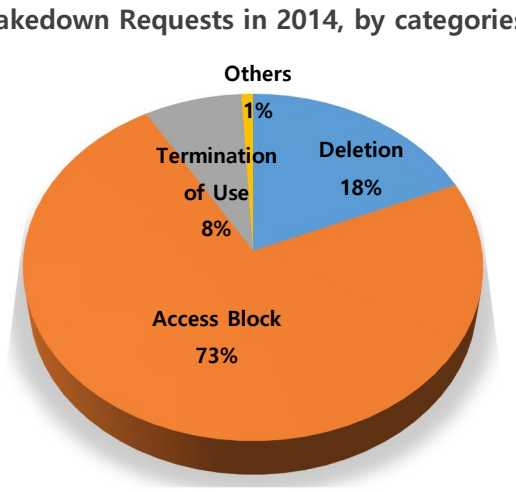
VI. Censorship - Status and Analysis[16]

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

		2011	2012	2013	2014
Total number of deliberations		57,944	75,661	110,714	140,421
Takedown Requests	Total	53,485	71,925	104,400	132,884
	Deletion	9,058	17,827	22,986	24,581
	Termination or suspension of use	12,398	14,342	16,914	10,031
	Blocking	31,357	39,296	62,658	97,095
	Labelling	672	460	1,842	1,177
Determination of Media Product Harmful to Juveniles		379	429	376	274
N/A		3,496	3,201	5,615	7,096

TABLE 10. DELIBERATION AND TAKEDOWN REQUESTS BY KCSC 2011-2014

- In 2014, total of 140,421 information was deliberated, and among them 132,884 (94.6%) were subject to takedown requests, with only 7,096 cases (5.1%) determined as 'non-relevant' (information not found to be problematic and allowed to be posted)
- Among the takedown requests in 2014(total of 132,884), 'blocking access' numbered 97,095(73%), 'deletion' 24,581 (18%), 'termination or suspension of use' 10,031(8%), and 'others (regarding display of 'harmful information for youths')' was 1,177(1%)[17].

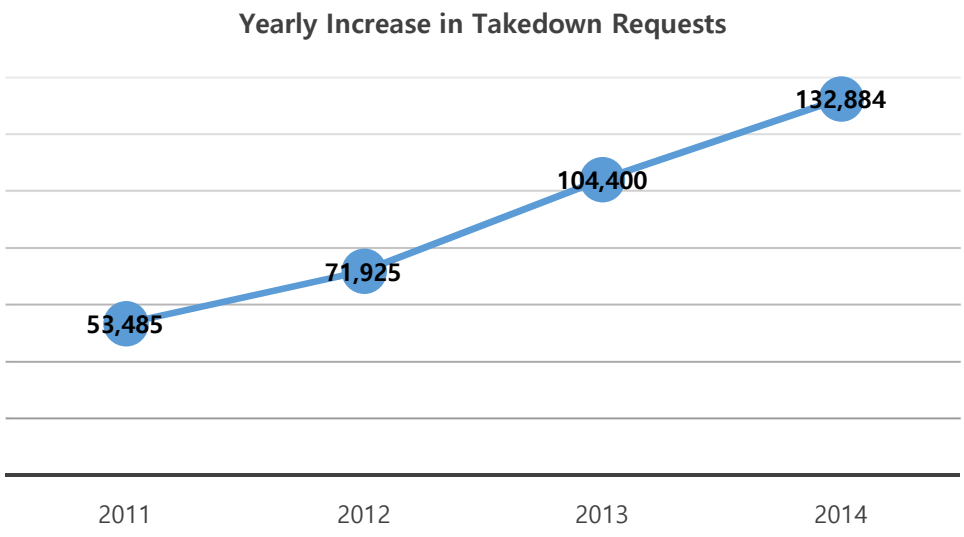


[16] The statistics below is based on data disclosed by KCSC. The categories used follow those used by KCSC, but some of them are not accurate because of duplicate or changed categories, and some of them have been rearranged for the sake of unity.

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

- The most numerous takedown requests is 'blocking access', meaning that mostly information on overseas server was the subject of deliberation. 'Others' are takedown requests related to the display of 'harmful information for youths', which have been rarely applied, less than 1%. This is probably because the KCSC does not strictly determine whether 'lewd information' or 'harmful information' is 'harmful information for youths' but rather, tends to block adults' access to them also by utilizing takedown requests that wholly block or delete such information.

- The number of deliberation and takedown requests are increasing sharply. Looking at each year, on 2011 57,944 cases were deliberated and 53,485 cases were given takedown requests. In 2012, 75,661 cases were deliberated and 71,925 cases were given takedown requests. In 2013, 110,714 cases were deliberated and 104,400 cases were given takedown requests. 2014saw 140,421 cases being deliberated and 132,884 cases being given takedown requests. Roughly speaking, takedown requests are increasing 1.3 times each year, and compared to 2011, 2014 saw more than double deliberations and takedown requests.



2. Categories of Takedown Requests[18] [19]

		2011		2012		2013		2014	
		Numbers	Ratio	Numbers	Ratio	Numbers	Ratio	Numbers	Ratio
Illegal	**Obscenity / Prostitution**	9,343	**17.5%**	14,409	**20.0%**	32,330	**31.0%**	49,737	**37.4%**
	Gambling	21,137	**39.5%**	28,785	**40.0%**	35,892	**34.4%**	45,800	**34.5%**
	Medicine, Food	16,404	**30.7%**	20,544	**28.6%**	20,329	**19.5%**	20,160	**15.2%**
	Drugs	28	0.1%	645	0.9%	1,875	1.8%	1,725	1.3%
	Illegal Finance	98	0.2%	610	0.8%	1,747	1.7%	1,694	1.3%
	Personal Information	42	0.1%	116	0.2%	1,090	1.0%	2,085	1.6%
	Third Party Transaction	734	1.4%	856	1.2%	1,585	1.5%	1,959	1.5%
	Counterfeit	699	1.3%	1,251	1.7%	1,551	1.5%	1,961	1.5%
	National Security	2,020	3.8%	681	0.9%	691	0.7%	1,137	0.9%
	Etc.	1,877	3.5%	1,112	1.5%	2,038	2.0%	3,541	2.7%
	Sub-Total	52,382	**98.0%**	69,009	**95.9%**	99,128	**95.0%**	129,799	**97.7%**
Harmful	**Hate Speech**	4	0.0%	147	0.2%	617	0.6%	705	0.5%
	Swears	/	/	/	/	/	/	194	0.1%
	Violence, Cruelty	47	0.1%	137	0.2%	90	0.1%	101	0.1%
	Etc.	384	0.7%	896	1.2%	1,407	1.3%	0	0.0%
	Sub-Total	435	**0.8%**	1,180	**1.6%**	2,114	2.0%	1,000	**0.8%**

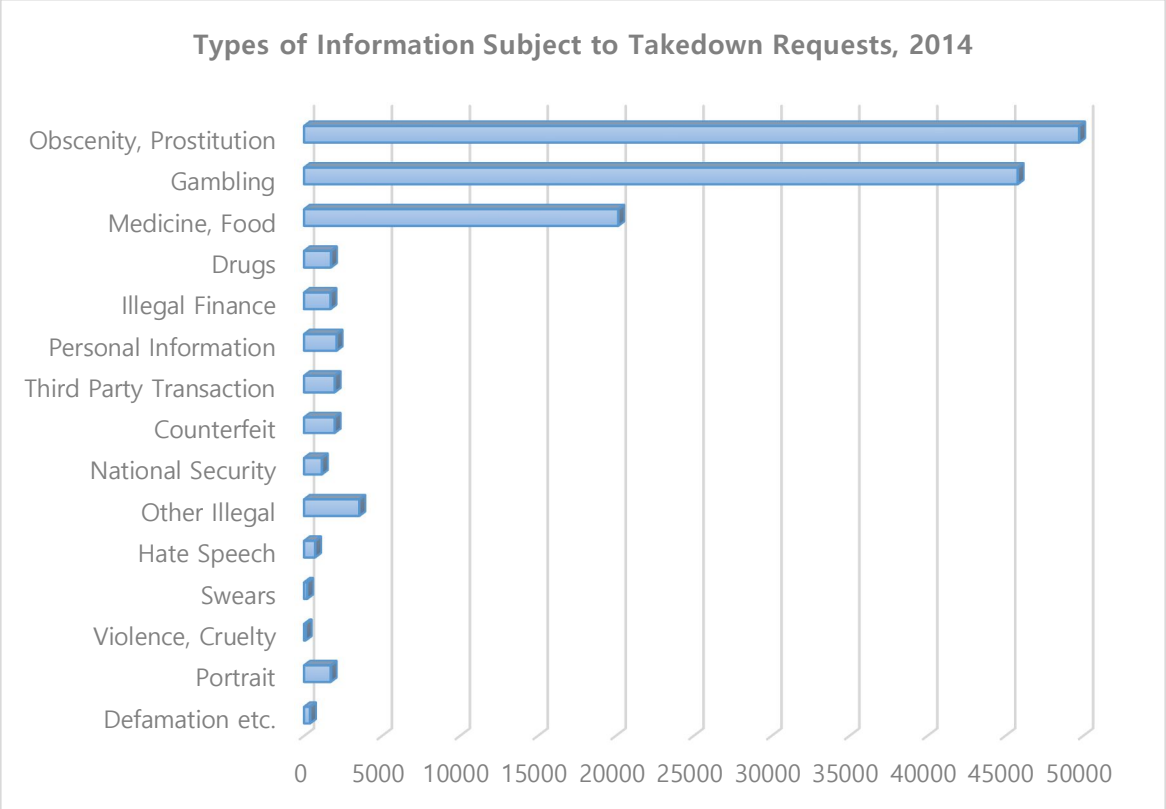
[18] The below is based on the KCSC's categories, and as some of them have changed, the numbers may contain errors. For example, deliberation for New Media was omitted from the statistics in 2012-2013, and harmful information such as Hate speeches have been counted under "Illegal Information", and illegal information such as obscenity and prostitution have been counted under "Harmful Information".

[19] 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 (publicity, defamation, IP, etc.). They are usually put under deliberation upon the person's report, and information violating publicity is usually leaked sex videos.

Infringement of Private Rights	**Portrait**	324	0.6%	1,046	1.5%	1,964	1.9%	1,706	1.3%
	Defamation etc.	344	0.6%	690	1.0%	1,194	1.1%	379	0.3%
	Sub-Total	668	**1.2%**	1,736	**2.4%**	**3,158**	3.0%	**2,085**	1.6%
Total		53,485	100%	71,925	100.0%	104,400	100.0%	132,884	100.0%

TABLE 11. STATUS OF INFORMATION SUBJECT TO TAKEDOWN REQUESTS BY CATEGORIES, 2011-2014

- In 2014, among the total number of information subject to takedown requests, illegal information numbered 129,799, amounting to 97.7% of the total, while harmful information numbered 1,000 (0.8%) and information violating other's rights numbered 2,085 (1.6%). More specifically, obscene information numbered 49,737 (37.4%), information inciting gambling spirit numbered 45,800 (34.5%), and illegal medicine and food numbered 20,160 (15.2%). The three categories of information, ranking first, second and third in numbers respectively, hold over 87% of the total.



- It can be seen that takedown requests for obscene information is rising steeply, with 9,343 cases in 2011, 14,409 cases in 2012, 32,330 cases in 2013, and 49,737 cases in 2014, showing that KCSC is focusing on regulating obscenity.

- Takedown requests for violations of National Security Act (which are mostly violations of Article 7, criminalizing the speech praising North Korea) was highest in 2011, with 2,020 cases, but decreased to around 600 in 2012 and 2013, but rebounded to 1,137 cases in 2014.

- Takedown requests for harmful information continuously increased during the period of 2011 (435 cases), 2012 (1,180 cases) and 2013 (2,114 cases), but 2014 saw approx. 50% decrease, with only 1,000 cases.

- Takedown requests for defamation increased continuously, with 344 cases in 2011, 690 cases in 2012, and 1,194 cases in 2013, but steeply decreased to 379 in 2014. This is because KCSC is taking a more strict approach to deliberation for defamation (especially consumer's reviews which are subject to plethora of reports by business), or because temporary measures are relatively easier to apply.

3. Takedown Request Status by Cause of Recognition and Related Agencies[20]

	2011		2012		2013		2014	
Complaints	15,188	28.20%	21,597	29%	36,862	34%	50,892	36.20%
Monitoring	5,455	10.10%	12,942	17.40%	20,866	19.20%	33,944	24.20%
Requests by Related Agencies	33,166	61.60%	40.018	53.70%	50.817	46.80%	55,585	39.60%
Sub-Total	53,809	100%	74,557	100.0%	108,545	100.0%	140,421	100%

TABLE 12. TAKEDOWN REQUEST STATUS, BY CAUSE OF RECOGNITION 2011-2014

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

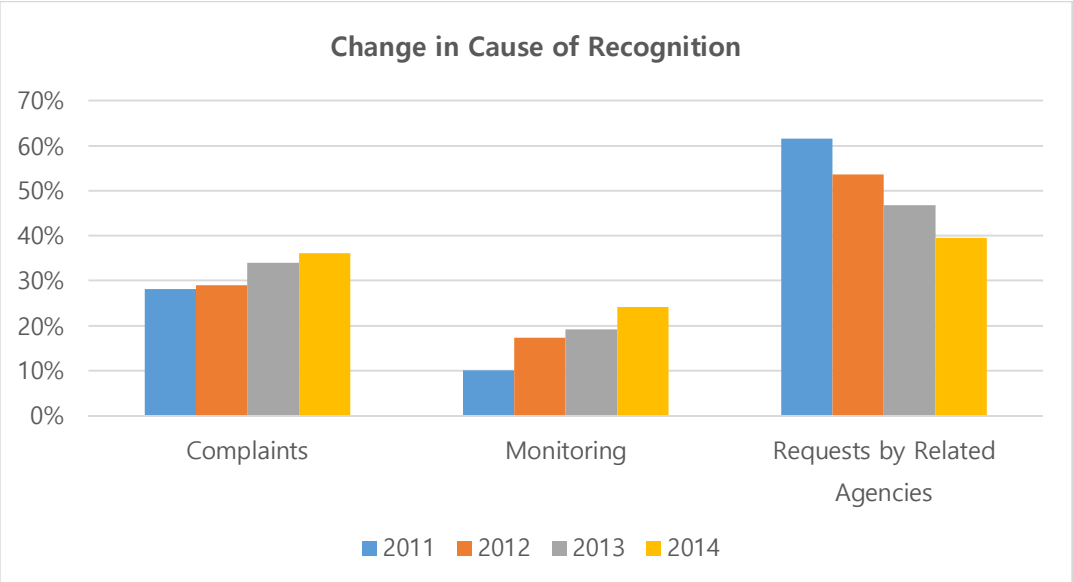
	2011	2012	2013	2014
Ministry of Food and Drug Safety	9,079	16,346	18,423	17,163
Sports Toto (Sports Gambling)	5,576	7,597	16,097	21,114
Game Rating Board	2,846	7,041	7,086	/
The National Gaming Control Commission	3,691	5,463	4,225	5,455
Korea Communications Commission *	8,346	700	701	1,137
Police Agency	2,662	758	340	459
Financial Supervisory Service	246	760	1,854	1,835
Korea Racing Authority	536	608	835	925
Intellectual Property Protection Association	385	605	821	542
Local Governments	268	138	784	5,179
Etc.	277	352	569	1,776
Total	33,912	40,368	51,735	55,585

TABLE 13. TAKEDOWN REQUEST STATUS, BY RELATED AGENCIES, 2011-2014

*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.

- In 2014, recognition of KCSC was mostly through requests from related agencies (55,585 cases, 39.6%), complaints (50,892 cases, 36.2%), and monitoring (33,944 cases, 24.2%).

- Recognition through requests from related agencies are on the decline, while the ratio of complaints and monitoring is increasing. KCSC is in the process of strengthening its monitoring process.



- Requests from related agencies are mostly from Ministry of Food and Drug Safety, Sports 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.

- The reason why the ratio of local government increased sharply in 2014 is because the Seoul City has launched its Internet Civilian Monitoring Group, which conducts internet monitoring.

4. Location of Information Subject to Takedown Requests

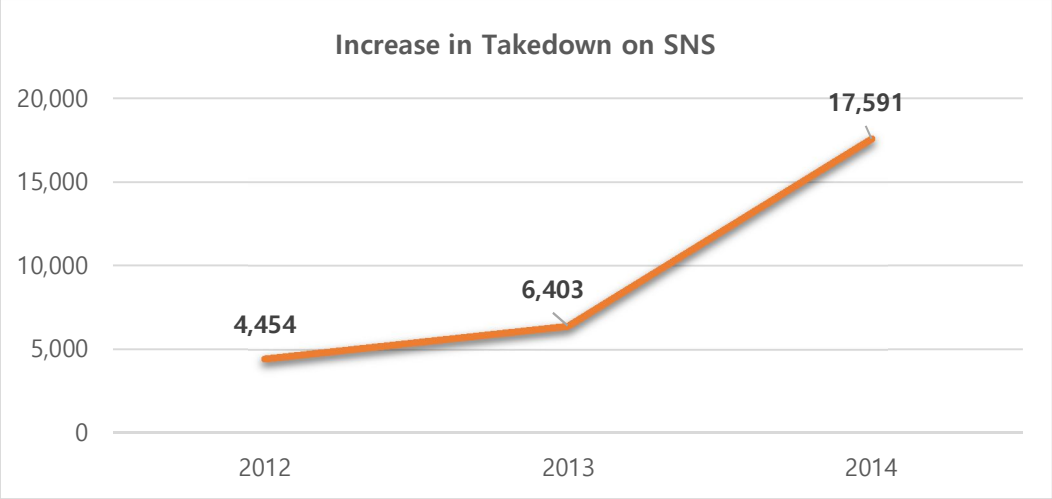
	2011		2012		2013		2014	
Blogs, etc.	4,301	**8%**	4,757	**7%**	12,483	**12%**	10,800	**8%**
Community, etc.	2,142	**4%**	4,664	**6%**	5,473	**5%**	11,556	**9%**
Sites	45,011	**85%**	55,423	**77%**	75,437	**73%**	87,675	**66%**
Others (P2P, Webhard)	1,259	**2%**	2,775	**4%**	3,517	**3%**	5,262	**4%**
SNS	/	**/**	4,454	**6%**	6,403	**6%**	17,591	**13%**
Mobile, such as Apps	/	**/**	0	**0%**	87	**0%**	/	**/**
Total	52,713	**100%**	72,073	**100%**	103,400	**100%**	132,884	**100%**

TABLE 14. INFORMATION SUBJECT TO TAKEDOWN REQUESTS, BY LOCATIONS, 2011-2014

- Majority of location of the information subject to takedown requests in 2014 is website, with 87,675 cases or 66% of the total. This is probably because the whole site is shut down by the KCSC's takedown requests if related to obscene or speculative information, which take up the largest portion of the total.

- In 2014, excluding websites, SNS number 17,591 (13.2%) and blogs number 10,800(8.1%). It is worrisome that these medias, which are considered to be places of privacy, are increasingly subject to KCSC's deliberations.

- Especially SNS, after the first deliberation on "New Media" began in 2012, was subject to increasing number of takedown requests, with 4,454 cases in 2012, 6,403 cases in 2013, and 17,591 cases in 2014.



5. Rate of Compliance with the Takedown Requests

	2011	2012	2013	2014	Total
Portals	99.3%	100%	99.9%	99.7%	**99.73%**
Network Providers	100%	100%	100%	100%	**100.00%**
Others	77.6%	98.2%	94.4%	97.9%	**92.03%**
Total	92.3%	99.4%	98.1%	99.2%	**97.25%**

TABLE 15. RATIO OF COMPLIANCE WITH TAKEDOWN REQUESTS, 2011-2014

- The rate of compliance for service providers and board admins in 2014 is 99.2%.

- 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.

6. Objections to the Takedown Requests and Withdrawal of Requests[21]

	2011			2012			2013			2014		
	Submissions	Accepted	Refused	S	A	R	S	A	R	S	A	R
Objections	9	1 (11%)	8	28	0	28	65	1 (1.5%)	64	24	0 (0%)	24
Withdrawal	21	21 (100%)	0	23	21 (91%)	2	23	20 (87%)	3	26	23 (89%)	3

TABLE 16. OBJECTIONS AND WITHDRAWALS, 2011-2014

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

- Among 362,694 Takedown Requests during the period of 4 years, only 219 cases (0.06%) have been subject to objections or requests for withdrawal. In 2014, only 50 cases (0.4%) of withdrawal or objections have been made among 132,884 cases of Requests. This seems to be because the owner of the information (poster or the admin of an overseas website) 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.

- Objections have an average success rate of 3%, and was 0% in 2014. On the other hand, request for withdrawal was successful for 92% of the time, which seems to be because this request is made for using the blocked URL for other purposes after deleting all illegal information.

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

Ⅶ. Censorship – Problematic Cases and Issues[22]

1. Analyses of Main Issues and Problematic Cases

A. Removal and Blocking of "Harmful Contents"

The scope of KCSC's takedown requests is not limited to illegal contents, but also "harmful contents". The latter is determined by KCSC, based on various reasons such as excessive cursing, violence, cruelty, or repugnance. This 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 contents by KCSC is problematic for the following reasons. (The KCSC's "request for correction" is de facto binding on the recipients, as evidenced by the compliance rate, which is almost 100%)

Harmful contents, while arguably not educational or helpful, are still protected by the 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 the emotions lying therein. Also they directly reflect the awareness and opinion of a person, thereby stimulating evaluation and discussion of such thoughts in the "free market of ideas".

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

Let us look at past examples of KCSC's takedown requests. A Twitter account "2mb18noma", which can be interpreted to sound like cursing the Korean president, was blocked because it was

[22] 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).

"repugnant due to excessive curses and vulgarity"(16th Communications Sub-Committee, 2011).[23] Recent posts that contained abusive words towards the current president Park and the ruling party was also removed, citing same reasons(16th, 36th Communications Sub-Committee, 2014)[24]. A video clip showing a drunken person, excreting while unconscious was removed because it was repugnant(7th Communications Sub-Committee, 2012).[25] An animation parodying the cartoon "Tiny Hippo and Tiny Train" which had achieved some internet fame in Korea was removed because it had violent contents, despite the fact that the animation exhibited considerable creativity(30th Communications Sub-Committee, 2012).[26] An internet homepage, which made a play, among others, of connecting various expressions to create and evaluate abusive expressions, without targeting anyone in particular, was also blocked as a whole(42nd Communications Sub-Committee, 2014)[27]. These cases are an example of how accusatory expressions and artistic expressions are all censored by an arbitrary standard.

B. Determination of "Illegality" by the KCSC

KCSC, as an administrative body, not a judicial one, routinely determines whether certain content is "illegal". The determination of illegality should be left to an independent judicial body because (1) an administrative body is not an expert in law, and (2) it may be influenced by the government. Nonetheless, the KCSC has taken upon itself to determine the fine line of illegality and makes decisions to remove or block illegal contents. This is especially problematic in the following circumstances.

---

[23] Chico Harlan, "In S. Korea, a shrinking space for speech," The Washington Post, December 22, 2011, http://www.washingtonpost.com/world/asia_pacific/in-s-korea-a-shrinking-space-for-speech/2011/12/21/ gIQAmAHgBP_ story.html

[24] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7308&page=1 (Korean)
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7660&page=1 (Korean)

[25] http://blog.naver.com/kyungsinpark/110131805176 (Korean)
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=4996&page=1 (Korean)

[26] http://blog.naver.com/kyungsinpark/110140161605 (English)
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=5508&page=1 (Korean)

[27] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7733&page=1 (Korean)

1) 'Obscenity'

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 as obscene 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.

2) 'Defamation'

Korean defamation law prosecutes truth as well as falsehood, a trap which accusatory or critical articles can often fall into. If a statement of fact is published solely for public interest without purpose to 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. Among the removed articles, many were accusations of corruption by public figures, their actions in the past, or a consumer report of bad service / product.

3) 'National Security Act – Praising and Inciting'

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 attacks on its unconstitutionality. UN Human Rights Council has also recommended its deletion. 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. Disregarding the Court's decision however, KCSC frequently applies this article to expressions that praises the North Korea or the ruler family, and to simple quotations of the official newspaper of North Korea. Censored statements include a post criticizing the Reserve Army practicing shooting on photos of the ruler family, memorial tributes to the late Kim Jung Il(23rd Communications Sub-Committee, 2011), or recent interviews of pro-North Korea long-term prisoners who elected to be transported to North Korea(34th Communications Sub-Committee, 2012)[28]. Recently, KCSC has removed a post that quoted a North Korean newspaper article, which denied the South Korean government's announcement that it has found remnants of air drones operated by North Korea(48th Communications Sub-Committee, 2014)[29].

4) Contents that 'may be used illegally'

The KCSC's takedown requests must be conducted based on whether the contents of the post itself are illegal. If a statement is censored because of the possibility of illegality, then the right to know and to use such statement to lawful purpose is violated. Actual cases include a blog of a middle school student demonstrating how to create an explosive(19th Communications Sub-Committee, 2012)[30], a webpage showing how to use a proxy connection to bypass KCSC's blockade of a website(4th Communications Sub-Committee, 2013)[31], and a post that introduces how to use one-time anonymous email service(11th Communications Sub-Committee, 2012)[32].

C. Blocking the entire site/account, rather than individual information

KCSC sometimes cites the impracticality of reviewing individual multiple contents within a single account of site, and blocks the whole account / site. In such cases, even legal contents within the account/site will be blocked as well. Actual cases include the following. A blog that contained some

[28] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=5580&page=1 (Korean)

[29] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7739&page=1 (Korean)

[30] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=5360&page=1 (Korean)

[31] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=6118&page=1 (Korean)

[32] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=5182&page=1 (Korean)
http://blog.naver.com/kyungsinpark/110140849196 (English)

posts that were in violation of the National Security Act was deleted in its entirety (41st Communications Sub-Committee, 2011)[33]. File sharing sites (e.g. Grooveshark, 4shared, bitsnoop) were wholly blocked because some contents violated copyright law (72nd Communications Sub-Committee 2013[34], 19th standing committee 2014[35]).

2. Latter half of 2014 – first half of 2015

A. Deletion of posting that included curses to the president and high ranking officials (the 36th Communication Sub-Committee, 2014[36])

- A citizen, while watching the Sewol Ferry Tragedy unfold, criticized the incompetence of the government in rescuing and coping with the aftermath, using repetitive strong swear words for the president and high ranking officials. As the actual content was criticism for the president and the government, deleting such post citing abstract and vague standard has a risk of being abused for regulating any criticisms against the government.

B. Blocking access to a website due to violations of National Security Act (39th Communications Sub-committee, 2014[37])

- The sub-committee resolved to give a Takedown Request to block access to the "Korea News Dot Com' website, for the reasons of violations of National Security Act. The postings related to North Korea within the site was mostly praises for the Kim Family, recent news of Kim Jong-Eun, reports by the Chosun Central News Agency, movies produced by North Korea, and anti-war / anti-US postings criticizing the Korea-US joint military training; in sum they were internal praises or defensive writings, and there is room for discussion on whether such expressions should be considered a violation of Article 7 of the National Security Act.

[33] http://blog.naver.com/kyungsinpark/110117052953 (Korean)

[34] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=6837&page=1 (Korean)

[35] http://www.kocsc.or.kr/02_infoCenter/Commission_View.php?ko_board=Commission&ba_id=7813&page=1 (Korean)

[36] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7660&page=1 (Korean)

[37] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7663&page=1 (Korean)

- Moreover, the site includes not only North Korea-related writings, but also posts quoting South Korean media, analysis of South Korean issues such as Sewol Ferry Tragedy, international news regarding the shoot down of the Malaysian Air, etc., news of international sport events, which were clearly not illegal posts, but with the access blocked for the whole website, these legal postings were blocked as well, and this action by the KCSC was criticized as being overbroad.

C. Posting claiming that 'drone not sent by North Korea' deleted for violations of National Security Act (48th Communications Sub-Committee, 2014[38])

- In Apr 2014, crashed drones near Paju and Baengnyeongdo Island was initially announced by South Korean government as being sent by North Korea. A post that quoted a Chosun Central News Agency's report criticizing the South Korean government's announcement and strongly claiming that it was not sent by North Korea was subject to Takedown Request for deletion due to violations of Article 7 of the National Security Act.
- The post did not include any aggressive expressions to South Korea, and only quotes explanatory and defensive report by the North Korea arguing that South Korean's posture is pushing the two Koreas into an adversarial situation, and defensive posture. As such, there is no expression therein that can be considered as a clear and present danger to the safety of the state and the democratic order, but the KCSC still considered the post to be a violation of the National Security Act, which certainly invites questions.

D. Deletion of the photos of Yoo Byung-Uhn (41st, 45th Communications Sub-Committee, 2014[39])

- As the owner of the Sewol Ferry, ex-CEO Yoo could not escape responsibility. However, the 86 photos of Mr. Yoo's corpse was subject to Takedown Request (deletion, blocking access) for the reasons of 'graphic expression of a persons' physical pains, thereby provoking disgust, or being cruel'.
- The photo of the corpse shows that the corpse was too decayed to fit into the police's announcement that he has been dead for less than 20 days, and suggests a possible human intervention by showing that the shirt was rolled up, and the legs were set straight. The posters in most cases did not only post the photos, but also wrote the above analysis and others, and engaged in discussions with the users in the comments section, but the posts were all deleted

[38] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7739&page=1 (Korean)

[39] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7732&page=1 (Korean)

nevertheless. Regulating information, which enables people to analyze important social issues and raise their opinions thereon, as well as exercising their right to know, simply because it is 'disgusting' and 'harmful' is questionable.

E. Blocking Access for 4shared.com (19th standing committee, Oct 16 2014[40])

- 4shared.com is a website that provides web hard (data storage) and streaming service. KCSC, upon report by the Ministry of Culture, Sports, and Tourism (Korea Copyright Commission), decided to block the access because it was a website in violation of copyrights, with illegal copies being distributed.
- 4shared.com is a search-based website, providing contents on a search basis without a list of the whole contents, and thus even the amount of the whole contents has not been determined. Copyright Commission simply searched a number of 'Korean copyrighted materials', found that most of them are illegal, and argued the website should be blocked for that reason.
- Also, 4shared.com has a filtering system in place that prevents copyright violations, and a Notice & Takedown process. Furthermore, they gives copyright owners accounts with takedown authorities. Therefore, 4shared.com is an online service provider that cannot be held accountable for violations of copyright laws.
- As such, Copyright Commission and KCSC seems to have acted upon bureaucratic laziness, and violated legal right of Korean users to use the services of websites and web services through indiscreet report and access block. For the same reasons, Bitsnoop, a torrent website, and Grooveshark, a streaming site has been blocked.

F. Access Block for Lezhin Comics (webtoon platform service site) (22nd Communications Sub-Committee, 2015[41])

- Lezhin Comics was blocked due to distribution of obscene contents, in violation of Article 44-7 (1) 1. However, the next sub-committee found that webtoons that do not have obscene contents are being distributed by the same website, and that blocking the whole site was not the right decision, and withdrew the decision voluntarily (23rd Communications Sub-Committee, Mar 26 2015[42]).
- The foremost party being affected by the KCSC's decision to delete or block access is the poster,

[40] http://www.kocsc.or.kr/02_infoCenter/Records_View.php?ko_board=Records&ba_id=7905&page=1 (Korean)

[41] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8730&page=1 (Korean)

[42] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8731&page=1 (Korean)

and in case of access block, the owner of the site. Despite the well-recognized principle of providing the affected party a prior notice and an opportunity to defend itself for administrative dispositions, such principle has not been followed for KCSC's takedown requests, which led to the recent revision to the Act On The Establishment And Operation Of Korea Communications Commission (Article 25(2)), that requires the KCSC to give prior or post-notice as well as an opportunity to submit its opinion to the target of the KCSC's takedown requests. However, KCSC still continues to interpret the Act unilaterally and is of the position that notice is unnecessary for the poster of 'clearly illegal information such as obscenity, etc.' In this case, only the internet network service providers were given notice of access block for information on overseas server, and the Lezhin Comics was not given prior notice nor opportunity for submission of opinion, which gave rise to questions of KCSC's procedural violations.

- Also, KCSC does not follow the standards set out by previous caselaw in determining 'obscenity', but instead relies on a simple test of whether there is 'description of sexual activities' or 'display of the genitals'. This stance does not change for access block of the whole website, resulting in excessive measures violating one's right to use legal materials within the website. The incident of the Lezhin Comics can be said to be a reflection of all of the above issues.

G. Deliberation on adult comics in webtoon platform sites (27th, 29th, 32nd, 34th Communications Sub-Committee, 2015[43])

- KCSC deliberated on the 'obscenity' of 8 Japanese adult cartoons (published and sold in Japan) that were being distributed in Lezhin Comics. After discussions with the Lezhin Comics, 5 of the cartoons have been voluntarily taken down, closing the case, but the standard KCSC uses for determining 'obscenity' for cartoon contents was put into question.
- Regulation of obscene materials, in which display of sexual activity (activity by itself is legal) is illegal, holds a very narrow and exceptional place in the regulations of freedom of speech. It should not be enough to simply graphically describe sexual activities, but a material must have such harmful contents that even adults should not see or show, in order to be regulated as illegal obscene material. Korean Supreme Court, considering the distinct characteristics of

[43] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8800&page=1 (Korean)
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8802&page=1 (Korean)
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8805&page=1 (Korean)
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8882&page=1 (Korean)

regulating obscenity, has defined the illegal 'obscenity' narrowly. 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 three criterions must be all satisfied before being prohibited as an obscene material.

- Cartoon, by its nature has narrative and artistic creativity and work is put into describing the narrative in form of pictures. Therefore, cartoon cannot be considered as not having "any artistic value", and determining its obscenity must be done more carefully.
- Also, cultural contents, for which the determination of artistic value must be carefully conducted, should not be blocked after a simple test by the KCSC, for the sole reason of being distributed through internet.

H. Deletion of posting claiming ''NIS' involvement in the Sewol Ferry Tragedy', for the reason of 'incitement of social unrest' (33rd Sub-Committee, 2015[44])

- A post that claimed that NIS was involved in import and maintenance of the Sewol Ferry, and was responsible for the cause and aftermath of the incident, was deleted for reasons of being 'information that may significantly incite social unrest'.
- However, a government body such as KCSC regulating expressions of people raising doubts on a public issue, with abstract and authoritarian standard such as 'may incite social unrest', can be viewed as an abuse of the deliberation procedures in order to block criticisms of the government and controlling public opinion.

I. Deletion of posting that mentioned an article under embargo (33rd Communications Sub-Committee, Apr 30 2015[45])

- A posting that linked an article reporting on a Philippines Islamic military organization called Abu Seif, follower of Islamist State, abducting and a Korean hostage was deleted due to

[44] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8806&page=1 (Korean)

[45] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8806&page=1 (Korean)

reasons of the disseminating information on criminal activities of a criminal organization following the IS, and because the post 'may significantly harm international peace and order'

- The article linked in the post was on the Abu Seif disclosing on their Twitter of their abduction of a Korean, and the Ministry of Foreign Affairs and Trade and the police placed an embargo on this issue while they investigated the matter. However, embargo is for reporters to suspend reports on a specific issue related to national security or significant public interest, and is simply an agreement regarding 'media reports', and does not by itself bind the public in their sharing of knowledge through internet and other media.
- Also, the post mentioned that the incident was under investigations by the MOFAT, and was written to urge caution for Koreans living in Philippines.
- Alerting others to criminal activities conducted by criminal organizations is necessary to evaluate and study their acts. Prohibiting the public from becoming aware about terrorist activities, for reasons of 'international peace and order' is an overextension of KCSC's deliberation regulations. Also, such censorship may increase the risk posed to Korean nationals' life and well-being.

J. Other cases

1) Defamation of Seung-Hwan Park, former Director of Korea Environment Corporation (79th and 80th Communications Sub-Committee, 2014[46])

- Several article and postings on claims that prosecutors conducted search and seizure for allegations of commissioning bribes on, not the Corporation's office as was officially announced, but the Director's office, was deleted and blocked access due to the reasons that it was defamatory towards the former Director Park. 158 postings in 2012 were blocked[47], and this year saw a resurgence of reports, by which 31 postings were blocked.

[46] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8114&page=1 (Korean)

[47] http://blog.naver.com/kyungsinpark/110140672254 (English)
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=5522&page=1 (Korean)

2) Blocking access to IS related postings (6th, 8th, 10th, 13th, 18th Communications Sub-Committee, 2015[48])

- 18 year old Kim was assumed to have joined the IS in Turkey, and in order to prevent further recruitment, series of IS related information was blocked.
- Recruitment posting, posting with positive evaluation of IS, such as the IS marching songs, postings stating his/her admiration for Kim, postings that linked the propaganda Twitter of IS, etc. were blocked for reasons of being 'information that may significantly harm international peace and order'; 'information that glamorize criminal organizations and crimes'; or 'other information that encourage crimes', and beheading videos uploaded by IS were blocked because they were 'violent and cruel information'.
- However, the actual harm caused by these postings, and the proximity between the harm and the posting have not been substantiated. If all IS-related information is blocked because of abstract deliberation regulations, people's right to know and research / evaluate IS may be violated.

3) Suspension of Use for a BJ (Broadcasting Jockey) of a Real-time internet broadcasting (Africa TV) for using curses (18th Communications Sub-Committee, 2015[49])

- IDs of Africa TV BJs, who used curses during their broadcasts, were subject to suspension of service (measure to suspend the use of the service, by intervening in the service agreement between the service provider and users), for the reason of being 'causing disgust or discomfort by using vulgar language or excessive cursing'.
- However, internet broadcasts are only open to those who voluntarily want to watch and wait for the specific contents that broadcast is providing. As such, it is questionable whether (1) it is acceptable to regulate free flow of expression on internet just because of 'excessive cursing,

[48] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8189&page=1
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8191&page=1
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8596&page=1
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8599&page=1
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8726&page=1 (Korean)

[49] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8726&page=1 (Korean)

vulgar language', when there is no illegality involved; (2) whether the government can consider previous and finished internet broadcasting, which by definition is provided in real-time, as 'information being distributed on internet', and regulate it as such; (3) whether KCSC's authority of takedown request encompasses its active intervention into the contractual relationship between the service provider and the users, and imposing injunction in personam to the users.

4) Deletion of a posting that claims the physical assault on the US Ambassador to Korea was self-fabricated (23rd Communications Sub-Committee, 2015[50])

- Deleted for being 'information that may significantly incite social unrest'

5) Cancellation of Contract for Jaju Minbo (23rd Communications Sub-Committee, 2015[51])

- After the decision to revoke Jaju Minbo's registration of an internet media, due to its articles that were found to be 'enemy's expressions', its site was closed (cancellation of contract)

6) Access block for posting that discloses information spilled from the Korea Hydro & Nuclear Power Co's intranet (80th Communications Sub-Committee, 2014[52])

- An organization claiming to oppose nuclear power plants hacked information from the KHNP's intranet, including screen capture of the nuclear reactor control system, manual of the nuclear reactor control system. 16 postings that mentioned such leaked data was blocked because they were in violation of the Act On The Protection Of Information And Communications Infrastructure, which prohibits accessing critical information and communications infrastructure by any person who has no access authority, or manipulating, destroying, concealing or leaking stored data by any person who exceeds his/her access authority.

[50] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8731&page=1 (Korean)

[51] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8731&page=1 (Korean)

[52] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=8115&page=1 (Korean)

7) Access block of information on Spy App (50th, 54th Communications Sub-Committee, 2014[53])

- Spy Apps are installed on smartphones or PCs to collect call details, emails, text messages, location information and contacts. A webpage that shows the price and functions of a Spy App was blocked because it was 'information that aids and abets violations of Protection Of Communications Secrets Act (prohibiting Interception)'.

8) Access block of a site for 'making new curses' (42nd Communications Sub-Committee, 2014[54])

- A website, the purpose of which was to make new, provocative and lengthy curses was blocked because it was 'information that causes disgust by using excessive cursing and vulgar language'.
- Cursing at no one in particular does not entail any illegality or harm, and cursing by its nature is an efficient medium of expression of extreme emotions, and as such this site can provide a forum for people to enjoy their right and pleasure of cursing. Also, this site is a community that is only open to those who voluntarily wish to participate therein and thus has no risk of causing disgust to those who did not want to participate. Finally, there are normal conversations between users in the board. Therefore, blocking the whole website is excessive.

[53] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7785&page=1 (Korean)
http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7789&page=1 (Korean)

[54] http://www.kocsc.or.kr/04_know/communication_SCommittee_View.php?ko_board=Communication_SCommittee&ba_id=7733&page=1 (Korean)

Ⅶ. Evaluation of Transparency

1. Surveillance

A. Information Disclosure Status

- In accordance with the current Telecommunications Business Act [55] and Protection Of Communications Secrets Act[56], Communications Service Providers have a duty to report to the Ministry of Science, ICT, and Future Planning biannually on details of communication information submitted to the government for its Interceptions (Communication Restricting Measures), Acquisition of communication metadata (Communication Confirmation Data), and

---

[55] 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 Korea Communications Commission twice a year, in accordance with the methods prescribed by Presidential Decree, and the Korea Communications Commission 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).

[56] 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, Information and Communications Technology (ICT) and Future Planning, 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, Information and Communications Technology (ICT) and Future Planning 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.

Provision of Subscriber 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

1) 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, 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.

2) Non-disclosure of status of surveillance via "Search and Seizure"

- 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 Daum Kakao, search and

seizure for Communication Service Providers seems to be the most prevalent method for internet surveillance, with massive amount of data collected.[57]

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

3) 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.[58] 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 meager 38.5%.[59] 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.[60]

---

[57] Excluding Kakao (the numbers of the affected accounts of which have not been counted), communications data for approximately 450,000 accounts of the 2 major providers have been searched and seized, and for only 2014, all accounts of the 2 providers submitted upon in regards to communications restricting measures, communications confirmation data, and communications data number only 14,000, while data for more than 400,000 accounts have been acquired with search and seizure

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

[59] "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)

[60] 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.

B. Problem and Road Ahead for Improvement

1) KCSC needs to disclose data by each deliberation

- For people to evaluate whether the deliberation procedures are utilized 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 deliberation is being conducted properly simply by attending the meeting or reviewing the minutes.

2) KCSC needs 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, 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.

Ⅷ. Conclusion

For internet surveillance, the Ministry of Science, ICT and Future Planning 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.

Nevertheless, we could confirm the comprehensive and massive surveillance practices by the investigatory agencies, and with the surveillance on the 'contents' of the communications on the rise, with the increase in the number of Interception and search and seizure, we can conclude that internet surveillance is expanding.

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

Government must realize that excessive censorship and surveillance on internet has a chilling effect on free flow of information, restricts people's freedom of expression and right to know, as well as hindering internet sector's growth. It 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 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

- KCC Status of Monitoring and Provision of Communications Confirmation Data, 1H 2011

- KCC Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 2H 2011

- KCC Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 1H 2012

- Ministry of Science, ICT and Future Planning Status of Communications Restricting Measures and Provision of Communications Confirmation Data, 2H 2012

- 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, 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, 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, 2H 2014 (Response to Information Disclosure Request)

- Naver Privacy Report 2014 (https://nid.naver.com/user2/privacycenter/info.nhn?m=viewCertReport)

- Daum Kakao Transparency Report (http://privacy.daumkakao.com/transparence/report/request)

- 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)

* The above data and other data can be found on:

http://transparency.or.kr (Korean), http://transparecy.kr (English)