Additional NGO Report on the Right to Privacy in the Republic of Korea

Issue:
1. Notification to the Subject of Wiretapping
2. Communications Surveillance Based on Search and Seizure
3. Mobile Phone Real-name System

Written by: Open Net

1. Notification to the Subject of Wiretapping

This issue was raised in the urgent appeal by Open Net in 2016. However, it was left out in the NGO report submitted in June 2019. This is to inform your excellency with the recent development and request the issue to be addressed in the final report.

"Communication Restricting Measures" (hereinafter "wiretapping") under the Protection of Communications Secrets Act refer to acquiring *real-time* the contents of the communications by a person subject to the investigations upon written permission from the court. According to the latest statistics, from 2013 to 2018, 382 cases of wiretapping for all communications were conducted for 6,538 accounts per year on average. 98.8% of all wiretappings are made by the National Intelligence Service and seem to be employed for national security investigations.[1] In 2011 alone, 7,167 accounts were wiretapped in a country with a total population of about 50 million. So per capita, the number of accounts wiretapped was about 9.5 times the United States including the ones issued by Foreign Intelligence Surveillance Court (2,732 + 1,789 = 4,521) and about 800 times Japan (25) in the same period.[2] In 2018, 6760 accounts were wiretapped in Korea[3] and in the United States[4] the number was [2,937[5] + 1,248[6] = 4,185]. and therefore, still the number of accounts wiretapped in Korea are about 10.2 times the U.S. numbers.

What makes the situation worse is that the suspects are given very late notification or no notification at all. The Protection of Communications Secrets Act requires the investigatory authorities to notify the suspect of the fact of wiretapping within 30 days after the indictment decision has been reached, not 30 days after

---

[1] Executive Summary of the Korea Internet Transparency Report 2019 http://transparency.or.kr/notice/2509 (Korean). For English Report, see http://transparency.kr/notice/2387 (2018 version)
[2] K.S. Park, Communications Surveillance in Korea (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2748318
[3] The population of Korea as of December 2018 was 51,826,059 http://27.101.213.4/
[4] The population of the US as of December 31, 2018 was 328,226,532 https://www.census.gov/popclock/
[5] https://www.uscourts.gov/statistics-reports/wiretap-report-2018
[6] https://www.uscourts.gov/sites/default/files/fisc_annual_report_2018_0.pdf

the wiretapping is done.[7] This means most people receive notifications 1-2 years after the wiretapping, substantially later than in other countries. Those indicted often find the fact of the wiretapping in court when the prosecutors read the wiretap transcript, significantly interfering with the suspect's right to prepare for a trial. Because the notifications are scheduled to be given very late in time, more than 60% of the notifications are never given, substantially blinding people to the scope and reach of the state surveillance.[8] What is even worse, even such notice can be deferred not by judges but by the heads of the local prosecutors' office, in complete contradiction of the warrant doctrine.

In 2010, the Constitutional Court reviewed one National Security Law investigation that involved 14 consecutive extensions of a wiretapping warrant (two months the maximum period each extension, adding up to 30 months).[9] According to the Protection of Communications Secrets Act, wiretapping for a criminal investigation can be extended for two months, and wiretapping for national security can be extended for four months without limitation on the total number or total duration of extensions.[10] In an unprecedented advance beyond an international norm, the Court struck down the provision that allowed extension without any limitation. The government recently proposed an amendment in March 2019 to reflect the Constitutional Court's decision. The government proposed the duration of the extension to be two months for all wiretappings and limited the total duration for a criminal investigation to one year and national security to three years. However, the National Human Rights Commission of Korea ("NHRC") commented that the limitation should be stricter.[11]

As described above, improvements regarding the extension of wiretapping are underway. However, the notification provision is still neglected. Notification to the party subject to surveillance is a basic matter of transparency and due process. All dispositions taken in regards to criminal proceedings must be given notification 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 notification is based on the day of the indictment, the subject of surveillance cannot become aware of the privacy violation during the period of investigations. Therefore, the procedures must be improved to ensure that notification is given at the time the surveillance has been conducted.

---

[7] Japan requires the notice to be given 30 days after the wiretapping is done, just as the United States requires the notice to be given 90 days after the wiretapping is done.

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

[9] The Constitutional Court, December 28, 2010, 2009Hun-Ga30

[10] Article 6(7) and Article 7(2) of the Protection of Communications Secrets Act

[11] NHRC, "Opinion on the Amendment to the Protection of Communications Secrets Act", July 22, 2019. https://www.humanrights.go.kr/site/program/decision/viewDecision?menuid=001003001002001&id=4714&searchdetail=N&searchradio=&searchtype=&searchyear=&searchselect=&searchword=&pagesize=10&currentpage=2 (Korean)

2. Communications Surveillance Based on Search and Seizure

Your excellency mentioned in the media statement published on 26 July, 2019, "[t]he figures of metadata requests considered non-sensitive and therefore not requiring a court warrant, however, are staggering, ranging from 6.4 million to 9.3 million per annum and suggest that access to such data is sometimes requested casually and most probably in many cases without being really necessary. It would prima facie appear that the number of requests for access made is possibly much higher than in most other democracies." We would like you also to take notice of the staggering figures related to communications surveillance based on search and seizure warrants.

There are four major measures employed for communications surveillance in South Korea. The first is wiretapping or "Communication Restricting Measures" mentioned above. The second is the provision of communications metadata, referred to as "Communication Confirmation Data" in the Protection of Communications Secrets Act that requires prior permission from the court. The third is the provision of subscriber data, referred to as "Communication Data" in the Telecommunications Business Act. Subscriber data, i.e. personal information of communications service users (subscribers) such as names, resident registration numbers, addresses, etc., may be accessed without a warrant at a communications service provider's compliance. Fourthly, the government may conduct surveillance on communications with a search and seizure warrant according to the Criminal Procedure Act. Search and seizure is the most powerful as it enables law enforcement to access contents, metadata, and subscriber data.

The most recent statistics of communications surveillance showed that while the total numbers of provision of metadata and subscriber data have been decreasing, the number of search and seizure of Internet companies are rapidly increasing. In the end, the total number of people under communications surveillance is increasing.

The provision of metadata for all communications numbered 286,030 cases (number of requests) for 5,846,958 accounts per year on average. Among them, the provision of metadata for the Internet numbered 37,672 cases for 133,907 accounts per year on average, which is approx. 2% of the total in terms of the number of accounts. The reason seems to be that metadata requests are mainly made to the mobile telecommunication service provider, and focused on cell tower search (referred to as "base station investigation" in the first NGO report). While the number of cases or requests is on the rise, the number of accounts has been sharply decreasing since it peaked in 2013 (16,114,668 accounts). The number would not likely to increase as the Constitutional Court found "cell tower search" and "real-time location tracking," which take a large part of the provision of metadata, unconstitutional in 2018.[12]

Provision of Communication Confirmation Data

(unit: number of accounts)

2013	2014	2015	2016	2017	2018
16,114,668	10,228,492	5,484,945	1,585,654	1,052,897	555,091

[12] The Constitutional Court, June 28, 2018, 2012Hun-Ma191·550 and 2014Hun-Ma357. Please refer to 2) Communication Confirmation Data in the NGO Report June 2019 for more details.

Provision of subscriber data numbered 1,024,110 cases for 8,972,965 accounts per year on average. For internet service subscribers, the number is 89,191 cases for 352,901 accounts respectively. This accounts for about 3.93% of the total in terms of a number of accounts. As it does not require court permission, investigatory agencies abuse the measure at a large scale. Although the number has been gradually decreasing, it is greatly disconcerting that intimate personal information of about 8.9 million accounts, which constitute 17.3% of the total population, are accessed without a warrant. After the Seoul High Court's decision in 2012 that ordered the largest web portal Naver to pay damages for providing subscriber data negligently, major Internet portals ceased to provide subscriber data from 2013, which was a welcome improvement. And now it seems most of the subscriber data of Internet users are being provided by the internet service providers (ISPs).

The data for search and seizure on communication service providers (which can be used for acquiring communications contents, metadata, and subscriber data) are not available from the government. The analysis relies on the data disclosed in the transparency reports of two major online service providers, web portals, Naver and Kakao. According to the reports, search and seizure on two companies numbered 9,538 for 10,791,104 accounts in 2017 alone. The number of cases decreased by 27% from 2016, but the number of accounts jumped 14.9 times. Then it declined to 17,020 cases for 8,299,512 accounts in 2018. For 2018, the total number of accounts subject to communications surveillance other than search and seizure (wiretapping, provision of metadata, and warrantless access to subscriber data) is 18,687. The analysis clearly shows that search and seizure is the most commonly used Internet surveillance method. Although search and seizure requires a warrant, if applications are numerous beyond scalability, it is inevitably impossible for judges to thoroughly examine warrant applications, making it hard to protect citizens from excessive surveillance of their communications.

In the end, communications surveillance is actually increasing in South Korea. We would like your excellency to take into account this trend in your final report.

3. Mobile Phone Real-name System

We would like to remind your excellency about the implications of the mobile phone real-name system in South Korea so that the problems of the system would be addressed in the final report.

First of all, the law requires telecoms to check the resident registration certificate or a driver's license for identification and made it necessary for telecoms to collect and store the user's resident registration number ("RRN"). The restriction on privacy by the indiscreet collection of RRNs outweighs the public interest of the facilitation of crime, and therefore the system is not proportionate. Especially in Korea, the RRN is not merely a piece of personally identifiable information. It became the standard identification number, ultimate key data integrating all personal information. Furthermore, since various types of personal information is exposed to limitless collection, disclosure, and use at the hands of others in contemporary society, if the RRN, functioning as the key data, is illegally leaked or abused, not only the right to privacy but also life,

body, and property of the individual may be encroached[13]. In fact, the RRN, which has such a great value, continues to be the target of crime, and large-scale data breaches continue to occur. Leaked RRNs are used for marketing purposes, abused for crimes such as voice phishing, and even put on the market. Therefore, the state should thoroughly manage and protect the RRNs and should improve and supplement the system so that the damage caused by data breaches could be minimized. However, the mobile phone real-name system is in violation of those constitutional obligations of the state and therefore makes the public interest disproportionate.

Secondly, there is no evidence that the mobile phone real-name system is effective in preventing crime. Anyone who conspires to commit crime usually borrows a mobile phone from another person or registers under someone else's name to conceal his/her identity. So, it may be difficult to identify a criminal immediately if he/she had used a borrowed-name mobile phone. However, such difficulty caused by criminals trying to conceal their identity also arises from other common illegal activities and could be easily overcome by advanced investigation tools to track the real user of a mobile phone such as call history analysis, cell tower searches, location tracking, etc. Investigation tactics based on the assumption that the name holder is a suspect is ineffective and delays the investigation process.

For this reason, Mexico introduced the SIM card registration system in 2009 only to repeal the regulation three years later. Countries such as the UK, Canada, the Czech Republic, New Zealand, and Romania have considered the merits of the prepaid SIM card registration but subsequently concluded against introducing it. And in 2012, Cecilia Malmström, European Commissioner for Home Affairs noted, "At present, there is no evidence, in terms of benefits for criminal investigation or the smooth functioning of the internal market, of any need for a common EU approach in this area."[14]

Moreover, the facilitation of investigation only concerns a very small number of criminals, when the system applies to all citizens without exception as we have seen above. It considers anyone using a mobile phone as a potential criminal to be monitored. There are many countries allowing the use of prepaid phones without requiring identity verification or SIM card registration despite the possibility of phones being used for crimes because introducing the real-name system that restricts the fundamental rights of the people is a heavy burden. Adoption of such a system is only justified by critical public interests such as national security. For example, when Poland adopted the anti-terrorism law in 2016, the law made prepaid SIM card registration mandatory. Although users don't have to provide real names and could exchange SIM cards without restriction, the law faced fierce opposition because it amounts to state surveillance and infringes on the right to anonymous communication.[15]

Personal information controllers such as mobile carriers, internet service providers, and financial service providers have accumulated personal information of the majority of the nation due to the identity verification requirements in various fields that require them to collect and store personal information. As a result, large-scale data breaches continue to occur every year, and the cumulative number of compromised accounts reported to the Korea Communications Commission ("KCC") over the past five years has reached

[13] The Constitutional Court, December 23, 2015, 2013Hun-Ba68 and 2014Hun-Ma449

[14] GSMA, "White Paper: The Mandatory Registration of Prepaid SIM Card Users", November 2013, p10.

[15] Anna Obem, "9 controversies about obligatory prepaid registration", January 31, 2017. https://en.panoptykon.org/prepaid (last accessed on September 15, 2019)

72 million. Thus, the identity verification system is not an appropriate means as it countervails the purpose of crime prevention by increasing the risk of crimes such as hacking for data or identity theft through the mandatory accumulation of personal information.

The UN Special Rapporteur on the freedom of opinion and expression in the report on encryption and anonymity[16] said that "blanket prohibitions" on anonymity fail to be necessary and proportionate and recommended States to refrain from making the identification of users a condition for access to digital communications and requiring SIM card registration. It is because such mandatory SIM card registration may provide governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest and severely restrict the fundamental rights of the people.

[16] A/HRC/29/32, para. 60