Submission to the UN Human Rights Committee
115th Session, 19 October 2015 - 6 November 2015
Republic of Korea

Freedom of Opinion and Expression, Right to Privacy

[omitted and abridged: an individual report prepared by PSPD Law Center and Open Net Korea and submitted by PSPD Law Center on October 17, 2015]

Right to Privacy and Family Life (Article 17)

Issue 20(b) Warrantless Seizure of Subscriber Identifying Information

- In the Government's reply to the list of issues (para. 63), the Government argue that investigation agencies' requests for provision of subscriber information are permitted only when necessity, the principle of proportionality, and legitimate purpose are satisfied. The Government's response cannot be true because Telecommunications Business Act Article 83(3) simply provides "the investigatory purpose" as the only requisite for obtaining subscriber information warrantlessly, and there is no procedural requirement what-so-ever for the telecoms or Internet companies to meet in releasing the subscriber information. As a result, almost all data requests (higher than 99.5%) are being automatically filled by the operators without any evaluation and this easy access has given the investigatory authorities an incentive to make even more data requests. As a result, more than 6 million people's subscriber information was accessed warrantlessly by the investigative authorities in 2011,[1] and that number has only increased to reach close to 10 million in 2013.[2] Considering that the Republic of Korea is roughly a country of 50 milion people, the majority of Korean citizens may have been the targets of surveillance, essentially bein treated as "potential criminals".
- SPO has insisted on maintaining the warrantless seizure of subscriber information based on Telecommunications Business Act 83(3), arguing that requiring warrant for acquisition of the subscriber information would severely harm efficient criminal investigation. However, after the portals announced that they will no longer fill the warrantless requests for such acquisition, the authorities acquired the same data simply by obtaining warrants without suffering any delay or loss on the integrity of their investigations. This experience shows that it is okay to require a warrant for acquisition of the subscriber identifying data.
- In April 2014, National Human Rights Commission of the Republic of Korea has made recommendations to the Minister of Science, ICT and Future Planning to require court permission for acquisition of subscriber data, and to require more

[1] Official Site of the then relevant Korean Communication Commission, http://bit.ly/1Fk34P8(korean only)
[2] Official Site of the now relevant Ministry of Science, ICT, and Future Planning. http://bit.ly/1KpEp7Z(korean only)

requisites such as 'relevance to the crime' and 'relatedness of the required material to the case',[3] however the Minister didn't accept the recommendation.

- The only change to this dismal state of affairs happened in 2012 when PSPD Public Law Center filed a damages suit against a major portal for providing subscriber information of a netizen involved in the defamation investigation into a video clip featuring the then cultural minister. After losing in the court of first instance, the netizen won a damage award of about US$500 in the High Court for Seoul District.[4] Within two weeks, all major portals and Internet companies stopped altogether complying with Article 83(3) data requests.[5] The decision was promptly appealed to the Supreme Court where the case is pending.
- The telecoms, responsible for 90% of subscriber data disclosure in the Republic of Korea, still insist on continuing to comply with Article 83(3) requests. What is more, the telecoms refuse to disclose to their customers whether the Article 83(3) data disclosures have been made when the customers asked, which means that the victims cannot file a suit, because they do not know whether they are victims. The Government (para. 63) replied that the statistics on the provision of the subscriber information to investigative agencies were disclosed to the public twice a year, but through these general statistics, one cannot find out whether *his/her* information was provided or not, therefore cannot be regarded as an appropriate measure to protect privacy.
- Even though subscriber data has been given the least legal protection around the world, the clear trends focusing on the sensitivity and importance in privacy of the subscriber data are arising. The representative case would be the Canadian Supreme Court case which has struck down the police' warrantless acquisition of subscriber data as unconstitutional.[6] The Snowden revelations also highlight the importance of the subscriber information. It is theorized that the ready availability of the subscriber information makes it very profitable for the authorities to engage in non-individualized, massive surveillance on the content and the metadata.[7] Chile has for long required court approval for such access.[8] In October 2015, California also passed the California ECPA that explictly required warrant for the identifying information of the parties to electronic communications.[9]

---

[3] Press release of NHRCK, "Amendment to Protection of Communication Secrets Act is needed to better protect personal information during investigation"(http://bit.ly/1NG9k71)

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

[5] Sunsik Kim and Soonhyeok Lee, *Susagigwane Gogaegjeongbo Tedeo Isang Jegong Anhae* [*Cusomer Information No Longer Given to Law Enforcement Agencies*], HANKYOREH NEWSPAPER (November 1, 2012), http://bit.ly/1OAW0zT

[6] R. v. Spencer, 2014 SCC 43. The Court ruled that "[P]articularly important in the context of Internet usage is the understanding of privacy as anonymity. The identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address and telephone number found in the subscriber information. Subscriber information, by tending to link particular kinds of information to identifiable individuals may implicate privacy interests relating to an individual's identity as the source, possessor or user of that information. Some degree of anonymity is a feature of much Internet activity and depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure."

[7] http://opennetkorea.org/en/wp/main-privacy/internet-surveillance-korea-2014

[8] https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf

[9] https://www.eff.org/cases/californias-electronic-communications-privacy-act-calecpa

Suggested Recommendations

- The government of the Republic of Korea should take active steps to reduce the number of the subscriber data acquisitions, including requiring a warrant for such acquisition.
- The government of the Republic of Korea should strengthen data protection laws so that any disclosure of personal data be notified at least upon the data subject's demands.