Abstract

Government Access to Personal Data and ISPs' Response

Park, Whon-Il*

In March 2016, the Supreme Court rendered a noteworthy decision that an Internet portal service provider (ISP) need not pay compensation to the plaintiff who argued the ISP had provided his personal data to police without his consent. The highest court reversed the appellate court ruling which said ISP's provision of such personal data required the court warrant on account of customers' constitutional rights of self-determination and anonymous speech. The above Supreme Court decision came right after the National Assembly passed the controversial Anti-terrorism Act, which authorizes the head of the National Intelligence Service (previously known as the Korean CIA) to collect personal information as well as location information of a certain terrorist suspect from ISPs pursuant to the existing laws.

Since Edward Snowden disclosed the global surveillance (PRISM) programme of the National Security Agency to the world in June 2013, the government accesses to personal data in the private sector have been a hot issue around the world. At this juncture, the Court of Justice of the European Union declared the Safe Harbor Agreement between the European Union and the United States invalid. In December 2015, the General Data Protection Regulation, which is legally binding all member states and strictly limiting government accesses to personal data, was consolidated to become effective in May 2018.

The main question of the six-year long "Minister Avoiding" Yuna litigation seemed to be to what extent the government investigation agency may access to personal data stored by ISPs, and whether the government agency may request ISPs to provide simple personal data without court warrants. The Telecommunications Business Act provides the statutory ground for ISPs to respond to such requests. The scope of

* Ph.D., Professor of Law at Kyung Hee University Law School.

personal data requested by the prosecutors or police officers is the personal information including name, address, telephone number and email address, which is usually contained in an ordinary business card.

It should be noted that personal information is no more sacrosanct right in the Information Age. Historically, the right to privacy has changed from the right to be let alone (as termed by Warren and Brendeis) to the right of self-determination of personal information. Nowadays personal information, subject to appropriate processing of de-identification or anonymization, has become inevitable to Big data and Fintech businesses. Then the right to privacy has turned out to be an individual privilege to enhance IT convenience. Also any data subject should be ensured the rights to access, rectification, cancellation and objection (ARCO) relating to his/her personal data and the effective administrative and judicial remedies including pecuniary compensation and punitive damages, if necessary, in case of abuse or misuse of personal information.

At the moment, the above mentioned Supreme Court decision is not supposed to change the year-long practices that government agencies need to obtain warrants in order to have personal data disclosed by ISPs. After the said Supreme Court decision, big portal operators seem to maintain their policy of no-more-cooperation with the investigation authority. It's because they know the failure to disclose personal data to the government agency would cause no punishment but clamorous requests from investigators while any delivery of personal data would bring avalanche of users' lawsuit for damages. In the long run, the awareness of privacy or increasing inclination towards IT convenience on the part of users could determine the future of the relevant provisions of the Telecommunications Business Act and the prevailing government practices.

Key Words : government access to data, request of communications data, right to privacy, individual privilege to enhance IT convenience, ARCO rights