[Government access to personal data and ISP's response]

Supreme Court Decision 2012Da105482 decided March 10, 2016

Regarding the case claiming damages arising out of provision of communication data.

Facts - Minister-Avoiding Yuna Case

In March 2010, Yuna Kim, the Olympic ladies figure skating gold medalist, was warmly welcomed by the Minister of Culture, Sports and Tourism at the airport. At that time, a gesture of Kim that could be interpreted as 'trying to avoid' the Minister Yu In-chon was captured by some video cameras.

An Internet user posted the funny picture on the Internet bulletin board as a satire, and the Minister alleged that this constituted libel and slander against him (potential criminal offences). The chief of the competent police station requested "N" compant, the operator of the site where the clip was uploaded, to disclose the identity of the relevant user. "N" company informed the investigator of the name and ID of the user, apparently in accord with the Telecommunications Business Act. The user filed a lawsuit against "N" company asking for compensation, arguing that his personal information was provided to police without his consent.

In the appellate court, the Seoul High Court (Seoul High Court Decision 2011Na19012, decided October 18, 2012) pointed out that even though the Telecommunications Business Act allows the telecommunications carrier to

deliver personal information to the police, it does not punish the carrier for failing to comply with the request. As such, telecommunications carriers had no obligation to disclose personal data merely because of requests by an investigative agency. However, making such disclosures breached its customers' constitutional right to self-determination of personal information and anonymous speech. Therefore, the telecommunications carrier must have internal process to determine whether such delivery is necessary. However, the appellate court found that NHN did not have such process in place, and accordingly ordered payment of compensation.

Legal issues

What is the scope of the personal information subject to the right to self-determination of personal information?

Is the freedom of anonymous expression ensured by Article 21 of the Constitution on the freedom of expression? Is it allowed to restrict by law subject to Article 37(2) of the Constitution, if necessary, for national security, the maintenance of law and order or for public welfare?

3. At the request of a prosecutor or investigation agency, is it allowed for the telecommunications business operator to provide the communication data for investigation pursuant to the relevant provisions of the Telecommunications Business Act even without court warrants? Does the telecommunications carrier's supply of the communication data to the investigation authority violate the right to self-determination of personal information or the freedom of anonymous expression of the user?

Summary of Decision

[1] The right to self-determination of personal information, which derives from human dignity and value, and the right to pursue happiness under Article 10 of the Constitution and the freedom of privacy under Article 17 of the Constitution, means the right of a data subject who may determine when, to whom and to what scope to make his/her personal information known and used. Such personal information as protected by the said right shall mean the whole information which makes an individual identifiable by characterizing the personal identity including individual body, belief, social position, status, etc. It does not limit the information to one's interior private data but includes publicly accumulated information and already disclosed personal information.

And the freedom of expression protected by Article 21 of the Constitution is indispensable freedom for an individual to preserve the dignity and value as a human being and to realize the national sovereignty. It surely covers the freedom of anonymous expression that anyone may express his/her idea or opinion or disseminate it with an anonym or pseudonym by keeping his/her own identity undisclosed to others

On the other hand, the exercise of fundamental rights under the Constitution shall be implemented so that it may make the community life possible and ensure other constitutional values or the law and order of the nation not to be jeopardized in a State community. Therefore, the right to self-determination of personal information or the freedom of anonymous expression may be restricted by law subject to Article 37(2) of the Constitution, if necessary, for national

security, the maintenance of law and order or for public welfare.

[2] When a prosecutor or the head of an investigation agency requested a telecommunications business operator to provide the communication data for the purpose of investigation pursuant to Articles 54(3) and (4) of the Telecommunications Business Act (the previous Act before it was wholly amended by Act No.10166 on March 22, 2010), and the telecommunications business operator responded to such request after examining the formal and procedural requirements, the telecommunications business operator's supply of the communication data to the prosecutor or the head of an investigation agency does not seem to illegally violate the right to self-determination of personal information or the freedom of anonymous expression of the user of the telecommunication service; provided, that it shall not apply if special circumstances are found that it was explicitly apparent that the prosecutor or the head of an investigation agency has abused the authority to request the supply of communication data thus violating improperly the interests of the data subject or a third party.

Reasoning

Questions 1 and 2 have been answered in the foregoing summary of the decision.

With respect to Question 3, whether the telecommunications business operator is required to conduct substantive examination of the investigation agency's

request of the communication data depends on the legislative purport of the Telecommunications Business Act, which is quite different from that of the Protection of Communications Secrets Act.

While the “communications data” under the previous Act are the name, resident registration number, address, phone number, and ID of the user, and contract period of subscription, the “communication confirmation data” under the latter Act are the date of telecommunications by subscriber, duration time of the telecommunications in question, the communications number of outgoing and incoming call, etc. and the subscriber's number of the other party, the frequency of use, computer communications or Internet log-records, location data, and the data on tracing a location of connectors capable of confirming the location of information communications apparatus to be used by the users.

Under the Protection of Communications Secrets Act, the investigation authority, seeking communication confirmation data, shall obtain permission of the court in writing describing the reason for such seeking, the relation with the relevant subscriber, and the scope of necessary data. However, if the urgent grounds exist that make it impossible to obtain permission from the court, the prosecutor or chief investigator shall obtain permission immediately after asking for the provision of the communication confirmation data and then shall send it to the telecommunications business operator.

The same procedure is required for the communication-restricting measures equipped to each suspect under investigation of a certain category of crimes.

In case of communications already completed, a warrant issued by the judge is necessary for seizure under the relevant provisions of the Criminal Procedure

Act.

Accordingly, the aforementioned simple communications data related with personal data of telecommunication service users may, without any permission of a court or warrant issued by a judge, be provided by the telecommunications business operator in receipt of a written request from the investigation authority. It is for speedy investigation and prevention of other crimes depending upon the content and nature of the relevant personal data.

In terms of proportionality, such communications data are sought for public interest like swift response to crimes in the initial investigation at the cost of private interest in private matters. Since the private matters acquired in the course of investigation shall be kept confidential, any violation of privacy of the user of telecommunication services seems to be relatively small. Therefore, it is proper and subject to legislative purports for the telecommunications business operator to provide the communications data in response to the request of the investigation authority satisfactorily in writing and under due process.

Out of question, if the investigation authority requests the communications data possibly in abuse and misuse of its authority, the fundamental right related with personal information of the user could be violated improperly.

However, any control of such abuse and misuse of authority should be done directly toward the State or the relevant investigation authority not the telecommunications business operator, which results in the extraordinary burden of the private party. If any possibility of violation of fundamental right related with personal information is found shall be sought directly from the State or the relevant investigation authority, not the telecommunications carrier.

In this case, if special circumstances are not found that it was explicitly apparent that the prosecutor or the head of an investigation agency has abused the authority to request the supply of communication data, it cannot be interpreted to have violated illegally the right to self-determination of personal information or the freedom of anonymous expression of the relevant user.

One thing is particularly argued that email address was provided by the defendant beyond the scope of such communications data. The said email address is nothing but the user ID attached to '@naver.com', and cannot be assessed as different personal information beyond the said scope.

Conclusion

In conclusion, the defendant's provision of communications data was legal pursuant to the relevant law, and not subject to compensation of damage incurred to the plaintiff. The original court misinterpreted the relevant provisions of the Telecommunications Business Act.

So the original court decision on the part of the defendant's responsibility for damages shall be reversed unanimously by Justices concerned without further deliberation of other cause of appeal and sent to Seoul High Court.

Comments by Prof. Whon-il Park

This is 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 a warrant issued by the judge 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 U.S. 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 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 personal data requested by the prosecutors or police officers is the personal information including 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 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 practices.