Case on Request for Communications Data by Investigative Agencies

[2016Hun-Ma388, 2022Hun-Ma105, 2022Hun-Ma110, 2022Hun-Ma126 (consolidated), July 21, 2022]

Complainants

The same as listed in Appendix 1

Respondents

The same as listed in Appendix 2

Decided

July 21, 2022

Holding

1. The part of Article 83, Section (3) of the Telecommunications Business Act (wholly revised by Act No. 10166 on March 22, 2010) relating to "a request for communications data from a prosecutor, the head of an investigative agency (including the head of a military investigative agency), or the head of an intelligence and investigative agency to collect information for investigation, execution of a sentence, or prevention of harm to the guarantee of national security" does not conform to the Constitution. The above statutory provision continues to apply until the legislature amends it by December 31, 2023.

2. The claim of Complainants listed in Appendix 3 and Appendix 4 against acts of acquiring communications data and that of Complainants Y.B., P.H., S.S., K.J., and J.M. are dismissed.

Reasoning

I. Overview of the Case

A. *2016Hun-Ma388*

1. Complainants are users of the telecommunications service provided by telecommunications business operators, Companies A, B, and C.

2. In accordance with Article 83, Section (3) of the Telecommunications Business Act, Respondents asked Companies A and B to provide for investigation the "name, resident registration number, address, phone number, date of subscription" of Complainants J.S., K.J., C.Y., K.M., H.J., A.H., P.C., Y.S., and L.G. described in Appendix 3, and the above telecommunications business operators provided Complainants' communications data as described in Appendix 3 to Respondents. Through this, Respondents obtained the communications data of Complainants listed in Appendix 3 from May 21, 2015, to March 4, 2016.

In addition, Respondents, prosecutors belonging to prosecutors' offices at each level, and the heads of investigative agencies requested Companies A, B, and C to provide communications data of Complainants other than those listed in Appendix 3 and obtained their communications data.

3. In response, on May 18, 2016, Complainants filed the constitutional complaint in this case against Article 83, Section (3) of the Telecommunications Business Act which stipulates when a prosecutor, the head of an investigative agency including the head of a prosecutor or military investigative agency, or the head of an intelligence investigation agency (hereinafter referred to as "the investigative agency et al.") requests the telecommunications business operator to provide communications data, the telecommunications business operator may comply with the request, while Complainants listed in Appendix 3 filed

the constitutional complaint in this case against acts of acquiring communications data. Complainant K.M. filed the constitutional complaint in this case, adding, in addition to his claim against the abovementioned Article 83, Section (3), a claim against the proviso of Article 83, Section (4) of the Telecommunications Business Act, which prescribes that if there is an urgent reason, the head of the investigative agency et al. may request, without resorting to writing, telecommunications business operators to provide communications data.

B. ***2022Hun-Ma105***

1. On December 23, 2021, Complainant asked Company B, a telecommunications business operator, to confirm whether or not his communications data had been provided to an investigative agency, and on December 27, 2021, Company B confirmed that Complainant's communications data containing his name, resident registration number, address, phone number, subscription date, and termination date were given to the *** District Prosecutor's Office three times between February 23, 2021 and June 28 of the same year.

2. In response, on January 25, 2022, Complainant filed the constitutional complaint in this case, asserting that Article 83, Section (3) of the Telecommunications Business Act, which prescribes that telecommunications business operators may furnish users' personal information at the request of the investigative agency et al. violated the principle of warrant and infringed upon his fundamental rights.

C. ***2022Hun-Ma110***

1. Complainant's communications data, specifically his name, resident registration number, address, phone number, subscription date, and termination date, were supplied to the investigative agency et al., such as a district prosecutor's office and a police station, four times between

February 23 and November 8 in 2021.

2. In response, on January 26, 2022, Complainant filed the constitutional complaint in this case, arguing that Article 83, Section (3) of the Telecommunications Business Act, which sets forth that telecommunications business operators may provide users' personal information at the request of investigative agencies, violated the rule against excessive restriction, rule of clarity, and principle of warrant and, thus, infringed upon his fundamental rights.

D. *2022Hun-Ma126*

1. Complainants are people who use the telecommunications service provided by telecommunications business operators, Companies A, B, and C.

2. Complainants became aware of the fact that Respondents had acquired their communications data as described in Appendix 4, and filed the constitutional complaint in this case on January 28, 2022, alleging that their right to informational self-determination, etc. are infringed both by Respondents' communications data acquisition activities listed in Appendix 4 and by Article 83, Section (3) and the proviso of Article 83, Section (4) of the Telecommunications Business Act, which are the legal basis of the acquisition.

II. Subject Matter of Review

A. *2016Hun-Ma388*

1. Complainants J.S. et al. are challenging the constitutionality of the communications data acquisition activities listed in Appendix 3.

2. Furthermore, Complainants are also challenging the constitutionality

of the whole of Article 83, Section (3) of the Telecommunications Business Act. However, in this case, the investigative agency et al. asked the telecommunications business operators to provide Complainants' communications data for an investigation, and subsequently, the operators provided the investigative agency et al. with the communications data which contained Complainants' personal information at their request (the investigative agency et al.'s acquiring communications data through their "request for provision of communications data" and telecommunications service providers' "provision of communications data" is hereinafter referred to as "the act of acquisition of communications data"). Thus, the subject matter of review is limited to the part of Article 83, Section (3) of the Telecommunications Business Act relating to "a request for communications data from a prosecutor, the head of an investigative agency (including the head of a military investigative agency), or the head of an intelligence and investigation agency." Complainants also argue that the legislative inaction that the Telecommunications Business Act did not establish ex-post notification procedures violates the Constitution, but this is a challenge to the failure of Article 83, Section (3) of the Telecommunication Business Act to establish ex-post notification to users—in other words, a challenge to insufficient and incomplete legislation. As such, since Complainants ultimately dispute the constitutionality of Article 83, Section (3) of the Telecommunications Business Act, the legislative inaction thereof is not included in the subject matter of review.

3. Meanwhile, Complainant K.M. argues that if Article 83, Section (3) of the Telecommunications Business Act is unconstitutional, then the proviso of Article 83, Section (4) of the Telecommunications Business Act is also unconstitutional, and the above provision should be declared unconstitutional by expanding the scope of a decision of unconstitutionality pursuant to Article 45 of the Constitutional Court Act. Since this is not an independent argument against the constitutionality of the proviso of Article 83, Section (4) of the Telecommunications Business Act,

however, it is not included in the subject matter of review.

4. On that account, the subject matter of review is whether each act of acquisition of communication data of Complainants listed in Appendix 3 and the part of Article 83, Section (3) of the Telecommunications Business Act (wholly revised by Act No. 10166 on Mar. 22, 2010) relating to "a request for provision of communications data from a prosecutor, the head of an investigative agency (including the head of a military investigative agency), or the head of an intelligence and investigative agency to collect information for investigation, execution of a sentence, or prevention of harm to the guarantee of national security" infringe on the fundamental rights of Complainants.

B. ***2022Hun-Ma105***

Complainant is challenging the constitutionality of the whole of Article 83, Section (3) of the Telecommunications Business Act, but as he is a person whose communications data were provided to a prosecutor, the subject matter of review is limited to the part relating to Complainant. Therefore, the subject matter of review is whether the part of Article 83, Section (3) of the Telecommunications Business Act (wholly revised by Act No. 10166 on March 22, 2010) concerning "a request for provision of communications data from a prosecutor to collect information for investigation" violates the fundamental rights of Complainant.

C. ***2022Hun-Ma110***

Complainant is challenging the constitutionality of the whole of Article 83, Section (3) of the Telecommunications Business Act, but as his communications data were furnished to prosecutors and police, the subject matter of review is limited to the part relating to Complainant. Therefore, the subject matter of review is whether the part of Article 83, Section (3) of the Telecommunications Business Act (wholly revised by

Act No. 10166 on March 22, 2010) concerning "a request for provision of communications data from a prosecutor or the head of an investigative agency to collect information for investigation" infringes on the fundamental rights of Complainant.

D. ***2022Hun-Ma126***

Complainants are challenging the constitutionality of each act of acquisition of communications data described in Appendix 4 and the constitutionality of Article 83, Section (3) and the proviso of Article 83, Section (4) of the Telecommunications Business Act. However, Complainants are those whose communications data have been provided to investigative agencies such as prosecutors or *** Agency. Thus, the subject matter of review is limited to the part of Article 83, Section (3) of the Telecommunications Business Act relevant to Complainants. Since Complainants made no independent argument against the constitutionality of the proviso of Article 83, Section (4) of the Telecommunications Business Act, the proviso thereof is excluded from the subject matter of review. Therefore, the subject matter of review is whether each act of acquisition of communications data of Complainants listed in Appendix 4 and the part of Article 83, Section (3) of the Telecommunications Business Act (wholly revised by Act No. 10166 on March 22, 2010) concerning "a request for provision of communications data from a prosecutor or the head of an investigative agency to collect information for investigation" violate the fundamental rights of Complainants.

E. ***Sub-conclusion***

As a consequence, the subject matter of review in this case is whether each act of acquiring communications data of Complainants listed in Appendix 3 and Appendix 4 (hereinafter referred to as the "Act of Acquiring of Communications Data") and the part of Article 83, Section

(3) of the Telecommunications Business Act (wholly revised by Act No. 10166 on March 22, 2010) concerning "a request for provision of communications data from a prosecutor, the head of an investigative agency (including the head of a military investigative agency), or the head of an intelligence and investigative agency to collect information for investigation, execution of a sentence, or prevention of harm to the guarantee of national security" (hereinafter referred to as the "Act Provision") infringe on the fundamental rights of Complainants.

The provision at issue and related provisions are as follows:

Provision at Issue

Telecommunications Business Act (wholly revised by Act No. 10166 on March 22, 2010)

Article 83 (Protection of Confidentiality of Communications)

(3) A telecommunications business operator may comply with a request for the perusal or provision of any of the following data (hereinafter referred to as "provision of communications data") from a court, a prosecutor, the head of an investigative agency (including the head of a military investigative agency, the Commissioner of the National Tax Service, and the Commissioner of a Regional Tax Office; hereinafter the same shall apply) or the head of an intelligence and investigation agency, to collect information for trial, investigation (including the investigation of a violation committed by means of a telephone, the Internet, etc. among the offenses prescribed in Article 10 (1), (3) and (4) of the Punishment of Tax Offenses Act), execution of a sentence, or prevention of harm to the guarantee of national security:

1. Names of users;
2. Resident registration numbers of users;
3. Addresses of users;
4. Phone numbers of users;

5. User identification word (referring to the identification codes of users used to identify the rightful users of computer systems or communications networks);
6. Dates on which users subscribe or terminate their subscriptions. (Emphasis added.)

Related Provisions

Former Telecommunications Business Act (wholly revised by Act No. 10166 on March 22, 2010, and before amended by Act No. 17347 on June 9, 2020)

Article 83 (Protection of Confidentiality of Communications)

(4) The request for provision of communications data under Section (3) shall be made in writing (hereinafter referred to as "Written Request for Provision of Data"), which states a reason for such request, relation with the relevant user and the scope of necessary data: *Provided*, That where it is impossible to make a request in writing due to an urgent reason, such request may be made without resorting to writing, and when such reason disappears, a Written Request for Provision of Data shall be promptly filed with the telecommunications business operator.

Telecommunications Business Act (wholly revised by Act No. 10166 on March 22, 2010)

Article 83 (Protection of Confidentiality of Communications)

(5) Where a telecommunications business operator provides communications data according to procedures under Sections (3) and (4), he or she shall retain the ledgers prescribed by Presidential Decree, which contain necessary matters, such as records indicating that communications data are provided, and the related materials, such as a Written Request for Provision of Data.

(7) A telecommunications business operator shall, in accordance with the methods prescribed by Presidential Decree, notify details

entered in the ledgers under Section (5) to the head of a central administrative agency whereto a person requesting the provision of communications data under Section (3) belongs: *Provided*, That where a person who requests the provision of communications data is a court, the relevant telecommunications business operator shall notify the Minister of the National Court Administration thereof.

Former Telecommunications Business Act (amended by Act. No 11690 on March 23, 2013, and before amended by Act. No. 14839 on July 26, 2017)

Article 83 (Protection of Confidentiality of Communications)

(6) A telecommunications business operator shall report on the current status, etc. of provision of communications data, to the Minister of Science, ICT and Future Planning twice a year, in accordance with methods prescribed by Presidential Decree, and the Minister of Science, ICT and Future Planning may check whether the details of a report submitted by a telecommunications business operator are correct and the management status of related materials under Section (5).

Former Telecommunications Business Act (wholly revised by Act No. 10166 on March 22, 2010, and before amended by Act. No. 16019 on December 24, 2018)

Article 94 (Penalty Provisions)

Any of the following persons shall be punished by imprisonment with labor for not more than five years or by a fine not exceeding 200 million won:

5. A person who provides communication data, and a person who receives communications data, in violation of Article 83 (3).

Telecommunications Business Act (amended by Act No. 17352 on June 9, 2020)

Article 104 (Administrative Fines)

(5) Any of the following persons shall be subject to an administrative

fine not exceeding 10 million won.

13. A person who fails to retain related materials or retains false materials in violation of Article 83 (5).
14. A person who fails to notify details of the ledgers which include the provision of communications data, etc. to the head of a central administrative agency, in violation of Article 83 (7).

III. Arguments of Complainants

A. *2016Hun-Ma388*

1. *Arguments on Justiciability*

(a) The Act of Acquiring Communications Data as an *in rem* investigation on Complainants' communications data conducted by the investigative agency et al., unilaterally in a superior position, is a *de facto* exercise of power, and as the investigative agency et al. are State agencies, which can cause a chilling effect that the telecommunications business operators would be disadvantaged if they do not respond to their request, the Act of Acquiring Communications Data amounts to an exercise of governmental power subject to a constitutional complaint.

(b) Even where the investigative agency et al. acquire communications data in accordance with the Act Provision, the users whose information has been provided will not know about the investigative agency et al.'s request for provision of communications and telecommunications business operators' provision of such data, and there is no way to challenge the act of acquisition of communications data itself. Therefore, the Act Provision expects an act of execution, but it falls under the case where there is no remedy procedure for the act of execution or no possibility of expecting remedies of rights, and thus the directness of infringement of fundamental rights must be acknowledged. In addition,

although it is true that some Complainants' complaints were filed one year after the date of the act of acquisition of communications data, where they were unaware of the fact that their communications data were submitted to the investigative agency et al. due to a lack of ex-post notification procedures, etc., the limitation period for filing should be judged based on whether 90 days have expired from the date of actual knowledge.

2. *Arguments on Merits*

(a) Although the act of acquisition of communications data by the investigative agency et al. under the Act Provision constitutes a compulsory measure subject to the principle of warrant, the Act of Acquiring Communications Data by Respondents was carried out without a warrant. In addition, in the case of Complainants J.S. et al. listed in Appendix 3, the acts of acquisition of their communications data were performed without a reason specified by the Act Provision, and in particular, the investigative agency obtained the communications data of Complainant L.G. seven times. Respondents argue that they obtained the communications data to achieve the purpose of the investigation because there were records of phone conversations between Complainants and the suspect or person of interest, but they did not prove anything about whether the act of acquisition of communications data of Complainants was indispensable.

Therefore, the Act of Acquiring Communications Data is in violation of the principle of warrant and the rule against excessive restriction and infringes on the right to informational self-determination of Complainants J.S. et al. listed in Appendix 3.

(b) The act of acquisition of communications data pursuant to the Act Provision amounts to a compulsory measure as the investigative agency et al. conducted it in a superior position, and thus the Act Provision in effect permits search and seizure without a warrant. What's more, the

act of acquisition of communications data can be carried out in an extensive and broad manner, targeting virtually all the citizens, and the Act Provision does not only very broadly and vaguely set forth the reasons for the investigative agency et al. to request the provision of communications data, but also does not have any procedures such as notifying users that their telecommunications business operator has supplied their communications data at the request of the investigative agency et al. Therefore, the Act Provision violates the rule against excessive restriction, rule of clarity, and principle of warrant, infringing on the right to informational self-determination of Complainants.

B. *2002Hun-Ma105*

As the Act Provision allows an investigative agency to obtain communications data that can identify the user's personal details, without a warrant, in a simple way, it is in violation of the confidentiality of communications and the principle of warrant.

C. *2022Hun-Ma110*

The Act Provision prescribes the objectives of personal information collection and the scope of the affected in an overly broad manner and does not establish *ex-ante* or *ex-post* judicial controls. Even though personal information has been provided to an investigative agency, nevertheless, the Act Provision does not have a procedure to notify individuals who are the subjects of the information and permits indiscriminate acquisition of personal information by the investigative agency. Therefore, the Act Provision violates the right to informational self-determination and confidentiality of communications and is contrary to the rule against excessive restriction, rule of clarity, and principle of warrant.

D. ***2022Hun-Ma126***

1. ***Act of Acquiring Communications Data***

(a) The Act of Acquiring Communications Data was an exercise of governmental power by Respondents, in a superior position, against Complainants listed in Appendix 4 through the telecommunications business operators, and this is a *de facto* exercise of power which already terminated, which in turn makes it highly likely for a court to deny justiciable interests. In this sense, the exception to the requirement of exhaustion of prior remedies is recognized. In addition, considering the importance of personal information protection and the practice of reckless information acquisition by an investigative agency through telecommunications business operators, the need for a constitutional explanation is acknowledged.

(b) Since the act of acquisition of communications data by an investigative agency is conducted without consent of the data subject in the absence of *ex-ante* or *ex-post* judicial control or even *ex-post* notification, it should be considered a compulsory criminal investigation to which the principle of warrant applies. Therefore, the Act of Acquiring Communications Data of Complainants listed in Appendix 4 is not only against the principle of warrant, but also against their right to informational self-determination and is also against the principle of due process of law as the data subject was not guaranteed to participate in the process of the investigative agency's acquiring communications data nor were there remedy procedures under which Complainants are notified of such acquisition and may challenge it.

2. ***Act Provision***

(a) The Act Provision is so broad in its purposes and the scope of affected that it enables investigative agencies to indiscriminately collect

personal information. Unlike the fact that strict regulation is in place for obtaining communications data through communications data restriction measures, searches and seizures, requests for provision of communications confirmation data, etc., the Act Provision allows an investigation agency to obtain information without any judicial controls, which is inconsistent with the aforementioned legal system. In addition, even though less restrictive means are available, such as subjecting the acquisition of communications information to judicial controls, notifying the data subject of the acquisition thereof, and limiting the scope of the affected and the purposes of the collection, the Act Provision excessively infringes upon the confidentiality of communications and right to informational self-determination.

(b) Although it is beyond dispute that the Act Provision should clarify its legal basis by specifying in detail actors, purposes, the affected, scope, etc., of the collection, storage, and use of personal information, it describes the reasons for the request of provision and the possibility for a telecommunications business operator to reject the request in an unclear way, violating the rule of clarity. Furthermore, it is against the principle of due process of law as it does not establish any measures to ensure procedural appropriateness, such as *ex-ante* or *ex-post* judicial controls or *ex-post* notification. It also violates systematic legitimacy by making it unclear whether the act of furnishing communications data falls under an investigation, while the Act Provision distinguishes communications data from communications confirmation data and regulates communications data in the Telecommunications Business Act, which does not fit its legislative objectives. Furthermore, it is contrary to the principle of statutory reservation by enacting the law without a notification procedure to the data subject, which is key to the right to informational self-determination.

IV. Assessment on Justiciability

A. *Claim against Act of Acquiring Communications Data*

Article 68, Section (1) of the Constitutional Court Act provides that "any person whose fundamental rights are infringed due to exercise or non-exercise of the governmental power" may file a constitutional complaint. Here, "governmental power" refers to the sovereign operation of all State agencies and public organizations that exercise legislative, executive, and judicial powers, and their exercise or non-exercise creates direct legal effects on rights and duties of the citizens and puts a complainant's legal status in an unfavorable position (*see* Constitutional Court 2010Hun-Ma439, August 23, 2012; Constitutional Court 2016Hun-Ma483, Aug 30, 2018).

Upon examination, the Court finds that the request for provision of communications data from the investigative agency et al. pursuant to the Act Provision falls under a non-compulsory criminal investigation and that the Act of Acquiring Communications Data was enabled as the telecommunications business operators, which are not a public authority but a private entity, voluntarily supplied the data in response to Respondent's request for provision of communications data of Complainants listed in Appendix 3 and Appendix 4. The Telecommunications Business Act stipulates that a telecommunications business operator may comply with a request for provision of communications data from the investigative agency et al., granting telecommunications business operators the authority to legally furnish users' communications data in response to requests from the investigative agency et al., and leaving whether to furnish the communications data at the discretion of telecommunications business operators while not specifying the duty for telecommunications business operators to cooperate. Additionally, there is no legal provision at all on compulsory measures in the case a telecommunications business operator does not respond to the request for the provision. There is no hierarchy

between Respondents and telecommunications business operators, and the operators would not suffer any legal disadvantages for not following Respondent's request for the provision. Even if the operators feel psychological pressure due to the request from the investigative agency et al., this is only an indirect and factual, not a legal, disadvantage. Even if operators had not complied with the request of the investigative agency et al. and Respondents had obtained communications data by getting a search and seizure warrant, it would not have caused any disadvantages to the business of the operators (*see* Constitutional Court 2010Hun-Ma439, August 23, 2012).

Therefore, the Act of Acquiring Communications Data does not amount to the exercise of governmental power, which is the subject of a constitutional complaint under Article 68, Section (1) of the Constitutional Court Act, and for this reason, the claim against the acts of acquisition of communications data of Complainants listed in Appendix 3 and Appendix 4 is non-justiciable.

B. ***Claim against Act Provision***

1. ***Assessment on Directness***

In order for a statute or a statutory provision to be subject to a constitutional complaint, the statute itself must result in restrictions on freedom, imposition of duties, or deprivation of rights or legal status without a subsequent, concrete act of execution by the statute or the statutory provision (*see* Constitutional Court 2017Hun-Ma1299, December 27, 2019). However, where there is a specific act of execution but no remedy for it; where a remedy exists but there is no possibility it works, forcing a complainant whose fundamental rights were violated to make a detour to an unnecessary procedure (*see* Constitutional Court 96Hun-Ma48, August 21, 1997); or where the content of the legal norm directly changes the citizens' rights or decisively determines the citizens' legal status

before the act of execution, fixing the citizens' rights in the state of being determined to the extent that it will not be influenced by the existence or content of the execution itself (*see* Constitutional Court 2003Hun-Ma337, August 26, 2004), the requirement of directness to fundamental rights infringement is exceptionally acknowledged.

As the Act Provision presumes the investigative agency et al.'s requesting a telecommunications business operator to provide communications data, the investigative agency et al.'s making the request itself does not bring about the effect of restraining the fundamental rights of the telecommunications service users. The user's fundamental rights are inhibited only when a telecommunications business operator, which is not a public authority but a private entity, supplies the user's communications data to the investigative agency, et al., in response to their request. In other words, in order for the Act Provision to restrict fundamental rights in a concrete way, the telecommunications business operator, which is not a public authority but a private entity, should voluntarily furnish the communications data, which constitutes an essential element. However, it is unclear whether there are direct measures to oppose the Act of Acquiring Communications Data. Moreover, since a user is not the direct respondent of the investigative agency et al.'s request for provision of communications data, it is highly likely that the user will not find any remedies through other procedures.

In addition, Complainants assert that allowing the investigative agency et al. to ask telecommunications business operators to provide telecommunications data without a warrant while there is no *ex-post* notification procedure does not conform to the Constitution, and the Act Provision seems to affect the legal status of Complainants by means of the law itself, at least as for the violation of the principle of warrant and principle of due process of law.

Therefore, we recognize the directness of the Act Provision to fundamental rights infringement. 2010Hun-Ma439, the decision made on

August 23, 2012, where in a different view, this Court held that the part of Article 54, Section (3) of the former Telecommunications Business Act (wholly revised by Act No. 9919 on January 1, 2010, and prior to amended by Act No. 10166 on March 22, 2010) relating to "when the request for provision of communications data from the head of an investigative agency is received," which was the legal basis for the request for the provision and the provision of communications data, did not meet the requirement of directness to the fundamental rights violation, is overruled to the extent that the previous one conflicts with this decision.

2. *Assessment on Time Limit for Filing Complaint*

(a) The adjudication on a constitutional complaint under Article 68, Section (1) of the Constitutional Court Act shall be requested within 90 days after the cause of action is known and within one year after the cause occurs (Article 69, Section (1) of the Constitutional Court Act). However, to allow the filing of a complaint despite the expiration of the filing period if there is a justifiable ground for the expiration is the interpretation consistent with the objectives of a constitutional complaint and with the proviso of Article 20, Section (2) of the Administrative Litigation Act, which is applied *mutatis mutandis* by Article 40 of the Constitutional Court Act. Here, a "justifiable ground" means the case where it is reasonable in terms of social norms to allow a delayed request for adjudication, considering various circumstances, including the cause of the expiration of the filing period. It includes reasons for objective causes beyond reasonable controls, such as force majeure and other unavoidable circumstances, reasons comparable to them, and reasons for the failure to satisfy the time limit requirement even if the complainant exercises ordinary care (*see* Constitutional Court 2001Hun-Ma39, December 20, 2001).

(b) The cause of action, or the infringement upon fundamental rights by the Act Provision, arose when the investigative agency et al. acquired

the communications data of Complainants from the telecommunications business operators, and Complainants became aware of the cause of action at the time when the telecommunications business operators gave them the notice of the provision of their communications data.

Nonetheless, as the Telecommunications Business Act does not adopt procedures to notify users when a telecommunications business operator furnishes communications data to the investigative agency et al., there is no way for users to know whether their communications data were submitted to the investigative agency et al. unless they ask the operator for the information of current status of provision of personal information to a third party in accordance with Article 35, Section (1) of the "Personal Information Protection Act."

In this case, some Complainants filed the complaint after one year had elapsed from the time the investigative agency et al. obtained the communications data, but as the Telecommunications Business Act does not implement an *ex-post* notification procedure under which Complainants would become aware of the provision, Complainants were not negligent nor responsible for not recognizing that the cause of action, or the fundamental rights violation, had occurred. Therefore, although some Complainants filed the complaint after one year had elapsed from the date on which the cause of action, or the fundamental rights infringement, had occurred, justifiable grounds for the delay should be acknowledged.

However, Complainants Y.B., P.H., S.S., K.J., and J.M. in 2016Hun-Ma388 received the notice of the provision of their communications data by the telecommunications business operators and filed the complaint after 90 days had elapsed from the date on which the cause of action, or the violation of their fundamental rights, arose. Since there are no justifiable grounds for the delay, they failed to satisfy the time limit requirement for filing, and their complaint is, thus, non-justiciable.

3. Sub-conclusion

Accordingly, Complainants' claim against the acts of acquisition of communications data described in Appendix 3 and Appendix 4 is non-justiciable. Complainants Y.B., P.H., S.S., K.J., and J.M.'s claim is also non-justiciable, and complaints of the other Complainants against the Act Provision are justiciable.

V. Assessment of the Merits

A. *System for Investigative Agency et al. to Request Provision of Communications Data under Telecommunications Business Act*

1. The provision allowing a demand for submission of relevant data to be made to a person providing telecommunications service for investigation needs was first introduced in Article 82, Section (2) of the Public Telecommunications Business Act that was enacted by Act No. 3686 on December 30, 1983. When the Public Telecommunications Business Act was wholly revised by Act No. 4394 on August 10, 1991, whose name was changed to the Telecommunications Business Act, Article 54, Section (3) of the same act stipulated "when related authorities ask for perusal or submission of documents regarding telecommunication service for investigation needs in writing, then telecommunication business operator or the one entrusted with partial treatment of telecommunication service under Article 12 of the same act may accede to the demand." However, at that time, the act did not distinguish communications data and communications confirmation data.

It was Article 54, Section (3) of the Telecommunications Business Act amended by Act No. 6230 on January 28, 2000 that allowed the investigative agency et al. to ask telecommunications business operators to provide communications data distinct from communications confirmation

data. Since then, in the process of several amendments, a requester of communications data has been extended to include the court, the head of the National Tax Service, the head of a regional tax office, etc., and trials and investigations on some penalty cases under the Tax Crime Punishment Act have been added as a new reason for requesting communications data. Later, the Telecommunications Business Act was wholly revised by Act No. 10166 on March 22, 2010, and the same article found its place in Article 83 as of now.

2. The request to provide communications data is mainly made in the early stage of an investigation to identify a suspect and victim of a crime. The Act Provision endows the investigative agency et al. with the authority to request a telecommunications business operator to give communications data without taking a separate procedure such as obtaining a warrant or court permission, while it grants the operator the authority to legally provide users' communications data in response to a request from the investigative agency (*see* Constitutional Court 2010Hun-Ma439, August 23, 2012), in order to promote speedy and efficient investigation and information gathering activities by the investigative agency et al. and to prevent further crimes.

When the investigative agency et al. make a request for provision of communications data, it shall be made in writing (hereinafter referred to as "Written Request for Provision of Data"), which states reasons for such request, relevancy to the user, and the scope of necessary data. *Provided*, That where the urgency of the situation makes it impossible to make a request in writing, such request may be made other than in writing, and when such reason ceases to exist, a Written Request for Provision of Data shall be submitted to the telecommunications business operator without delay (Article 83, Section (4) of the Telecommunications Business Act). Where a telecommunications business operator gives communications data, it shall retain the ledgers which contain the necessary information, such as records indicating that communications data were provided and the related materials, including a Written Request for Provision of Data

(Article 83, Section (5) of the Telecommunications Business Act), and the ledgers on provision of communications data shall be kept for one year (Article 53, Section (1) of the Enforcement Decree of Telecommunications Business Act).

A telecommunications business operator shall report on the current status, etc. of the provision of communications data, to the Minister of Science and ICT twice a year, within 30 days after the end of each half year (Article 83, Section (6) of the Telecommunications Business Act and Article 53, Section (2) of the Enforcement Decree of Telecommunications Business Act) and shall establish and maintain a department dedicated to the affairs related to users' communications confidentiality (Article 83, Section (8) of the Telecommunications Business Act and Article 53, Section (3) of the Enforcement Decree of Telecommunications Business Act).

3. The Telecommunications Business Act does not have procedures to notify provision of communications data to the users, who are the subjects of communications data provided to the investigative agency et al., or separate measures for users to challenge the act of acquisition of communication data. However, under Article 35, Section (1) of the "Personal Information Protection Act" and Article 41, Section (1) of the "Enforcement Decree of Telecommunications Business Act," users may ask to peruse the information of the "current status of provision of personal information to third parties."

B. *Summary of Issues*

1. The right to informational self-determination, as the right of a data subject to decide for himself or herself when, to whom, and to what extent information about him or her will be known and used, is guaranteed as a general right to personality derived from the first sentence of Article 10 of the Constitution, and as secrecy and freedom of privacy under Article 17 of the Constitution. In principle, activities such as investigation,

collection, storage, processing, and use of personal information constitute restrictions on the right to informational self-determination (*see* Constitutional Court 2010Hun-Ma153, December 27, 2012; Constitutional Court 2016Hun-Ma483, August 30, 2018). A user's name, resident registration number, address, phone number, ID, and date of subscription or termination, provided by the telecommunications service operator to the investigative agency et al. upon the request of the government agencies, corresponds to the personal information that can identify Complainants; thus, the Act Provision restricts the right to informational self-determination.

2. Complainants argue that it is against the principle of warrant to allow the investigative agency et al. to acquire communications data from telecommunications business operators without judgment of a court, despite the fact that the act of acquiring communications data under the Act Provision virtually equates to a search and seizure. Therefore, the issue is whether the Act Provision violates the principle of warrant.

3. Since Complainants assert that the meaning of "harm to the guarantee of national security" in the Act Provision is ambiguous and thus violates the rule of clarity, whether the Act Provision violates the rule of clarity is also the issue.

4. Complainants contend that the Act Provision violates not only the rule against excessive restriction but also the principle of due process of law since it defines, in an overly extensive and broad way, the objectives of the collection of personal information and the scope of people whose communications data may be requested and since it does not adopt procedures under which notification is made after the provision of the data. As Complainants allege violation of the rule against excessive restriction and the principle of due process of law for practically the same reason, the claim against the extensive and broad restrictions on personal information due to the provision of communications data will be judged by the adjudication on whether the rule against excessive

restriction is violated; and the claim on the lack of procedures to notify the provision of communication data will be judged by the adjudication on whether the principle of due process of law is violated.

5. In addition, Complainants assert that the Act Provision does not limit the scope of "investigation" and of "execution of a sentence"; that it violates the rule of clarity because the words "investigation," "trial," "execution of a sentence," etc. in it are, by themselves, not sufficient to make it clear when the investigative agency et al. can make a request for provision of communications data or whether a telecommunications business operator can reject the request therefor; that it is against the systematic legitimacy to prescribe communications data in the Telecommunications Business Act, whose legislative purpose does not fit those data, and at the same time to not clearly provide whether the act of acquisition of communications data is an investigation; and that the Act Provision infringes the principle of statutory reservation because it does not establish procedures to notify the data subject. All these arguments of Complainants are not substantially different from the argument that the Act Provision violates the rule against excessive restriction due to its extensive regulation, and the principle of due process of law due to the absence of procedures of notification to users. Thus, we will review these issues together while determining whether the rule against excessive restriction or principle of due process of law is violated.

6. Consequently, the question is whether the Act Provision does not conform to the principle of warrant, the rule of clarity, the rule against excessive restriction, and the principle of due process of law, thereby violating Complainants' right to informational self-determination, and these issues are carefully examined in the following paragraphs.

C. *Whether Principle of Warrant under Constitution Is Violated*

Article 12, Section (3) of the Constitution stipulates that "warrants issued by a judge through due procedures upon the request of a

prosecutor shall be presented in cases of arrest, detention, seizure or search," and Article 16 of the supreme law prescribes that "in case of search or seizure in a residence, a warrant issued by a judge upon request of a prosecutor shall be presented," which indicates that the principle of warrant is guaranteed at the constitutional level. The principle of warrant adopted by the Constitution is that compulsory measures such as arrests, detentions, and searches and seizures in relation to criminal procedures must be carried out with a warrant issued by a judge whose status is guaranteed by judicial independence. Therefore, the essence of the principle of warrant under the Constitution is that a warrant must be issued by a neutral judge based on his or her concrete judgments in order to conduct compulsory disposition that restrains fundamental rights such as arrest, search, and seizure (*see* Constitutional Court 2010Hun-Ma672, May 31, 2012).

Upon examination, the Court finds that the Act Provision only sets forth that a telecommunications business operator may "comply with the request" while granting the investigation agency et al. the authority to ask the operator for the provision of communications data. It imposes on the telecommunications business operator no obligation to accede to or cooperate with the request for provision of communications data from the investigative agency et al., and does not put measures in place to compel the provision of communications data by the operator. Thus, the request for provision of communications data pursuant to the Act Provision falls under a non-compulsory criminal investigation, which does not involve coercive force, and the principle of warrant does not apply to the act of acquisition of communications data by the investigative agency et al. Hence, the Act Provision conforms to the principle of warrant under the Constitution.

D. *Whether Rule of Clarity Is Violated*

The rule of clarity, an expression of the rule of law, is basically

necessitated for all laws restricting fundamental rights. Whether a legal norm is clear or not depends on whether it provides predictability through fair notice so that the persons subject to it can understand the meaning of the statute and on whether the legal norm explains its meaning sufficiently enough for the relevant agencies not to arbitrarily interpret or enforce it. In other words, what matters is whether predictability and exclusion of arbitrary law enforcement are guaranteed. Since the meaning of a legal norm is specified by the interpretation that comprehensively considers not only the text but also the legislative objectives, intent, and history, the systematic structure of a legal norm, etc., whether a legal norm violates the rule of clarity hinges on whether such interpretation method gives standards of interpretation that help to reasonably understand the meaning of the legal norm (*see* Constitutional Court 2014Hun-Ba405, April 27, 2017; Constitutional Court 2012Hun-Ma191, June 28, 2018).

Complainants maintain that the meaning of "harm to the guarantee of national security" in the Act Provision is unclear and violates the rule of clarity. Yet the "guarantee of national security" is a concept that involves the existence of the State and the maintenance of the basic order of the Constitution; in turn, it can be understood as national independence, territorial integrity, proper functions of the Constitution and laws, and maintenance of State institutions established by the Constitution (*see* Constitutional Court 89Hun-Ka104, February 25, 1992; Constitutional Court 2011Hun-Ba358, September 25, 2014). Any "harm" to the guarantee of national security represents creating a risk to the guarantee of national security; so, in the end, "harm to the guarantee of national security" can be interpreted into a case that can cause danger to the existence of the State or the basic order of the Constitution.

In particular, Article 83 of the Telecommunications Business Act serves to protect the confidentiality of communications, and Sections (1) and (2) of the same article state that no person shall divulge the confidentiality of communications carried by telecommunications business

operators, and no person who is engaged in telecommunications services shall divulge a third party's confidential information with respect to communications obtained in the course of performance of his or her duties. In light of the objectives of Article 83 of the Telecommunications Business Act, providing for strict protection of the confidentiality of communications, "information collection aimed at preventing any harm to the guarantee of national security" is interpreted as the minimum information collection necessary to achieve the purpose of preventing danger to the existence of the State, or to the basic order of the Constitution.

Therefore, as a person with sound common sense and a general sense of justice can fully predict what the Act Provision intends, it is not violative of the rule of clarity.

E. *Whether Rule against Excessive Restriction Is Violated*

1. *Legitimacy of Purpose and Appropriate Means*

In modern society, the rapid development of information and communications technology makes it possible for third parties to extensively collect, store, process, and make use of various types of personal information including personal details, regardless of the intent or awareness of data subjects. Such information can be significant for the investigative agency et al. to collect and preserve information, to locate and secure the suspected, to execute sentences, and to prevent harm to the guarantee of national security (*see* Constitutional Court 2012Hun-Ma191, etc., June 28, 2018). In particular, the use of mobile phones and the Internet has become commonplace, which enables the investigative agency et al. to quickly secure information that can identify individuals through telecommunications business operators that offer these services. In addition, such data are utilized in the early stage of criminal investigation or information collection.

As such, the Act Provision permits the investigative agency et al. to obtain the user's communications data by making a request for the provision of communications data to a telecommunications business operator so as to promote promptness and efficiency in investigations, execution of sentences, or activities to guarantee national security activities, thereby contributing to the discovery of substantive truth, the proper exercise of the authority of the State to impose criminal penalties, and the guarantee of national security; consequently, we recognize the legitimacy of its legislative purpose. In addition, acquiring users' communications data, if necessary, through the investigative agency et al.'s request for provision of communications data to the telecommunications business operator is an appropriate means to achieve the above purposes; thus, the appropriateness of the means is recognized, too.

2. *Least Restrictive Means*

(a) Necessity and Limitations of Provision of Communications Data

Communications data serve as a very valuable clue in a criminal investigation. The number of subscriptions to mobile communications services in Korea exceeds that of registered residents, and with the expansion of high-speed Internet networks and the spread of smartphones, the use of communications devices in Korea is incomparable to that of the past, and the significance of communications data in investigations is growing. In view of the change of the direction of investigation to reduce dependence on *in personam* investigations and to secure objective evidence through *in rem* investigations, it is necessary to permit the investigative agency et al. to acquire communications data through telecommunications business operators. In particular, in some criminal cases, promptly obtaining communications data is essential to averting additional crimes and to defending the public interest. Although, in some way, it is unavoidable for the investigative agency et al. to acquire communications data through telecommunications business operators,

their acquisition of personal information without the consent of data subjects should be strictly limited to cases necessary to serve the public interest.

(b) Scope of Data Subject to Provision of Communications Data

The Act Provision limits the scope of information that the investigative agency et al. can request to furnish.

In general, it is natural for people to share basic information such as names and job titles in their social life for the purpose of identification or communication, and the State also needs to amass and utilize such information in order to properly perform its functions. Unless such information plays a role as an identifier to get access to other dangerous information or is used to extract the whole or partial personality of an individual by combining it with other pieces of personal information, it is difficult to say that such information itself is always subject to strict protection (*see* Constitutional Court 2003Hun-Ma282, July 21, 2005; Constitutional Court 2016Hun-Ma483, Aug 30, 2018)

The communications data asked for under the Act Provision are mainly used to identify a suspect and a victim of a crime in the early stage of an investigation. The information acquired by the investigative agency et al. through the request for provision of communications data includes the user's "name, resident registration number, address, phone number, ID, or date of subscription or termination," and it is the information very basic to identify suspects or victims and, if necessary, to contact them, which means the minimum, basic information unavoidable to obtain for investigation or maintenance of national security. In particular, in the initial stage of an investigation, there is a great need to discover whether a crime is actually committed and to narrow down the scope of those involved by receiving information that can identify suspects or victims.

Certainly, it is understandable that phone numbers, addresses, etc.

necessitate considerable protection in that such information, in the event of its leakage or abuse, can give access to personal information whose subject does not want to reveal. Furthermore, as resident registration numbers are information that can act as a connector that integrates other pieces of personal information, they also need special protection. However, at the same time, promptness and accuracy are also required when the investigative agency et al., identify a suspect or a victim for investigation, execution of a sentence, and prevention of harm to the guarantee of national security, and it is inevitable to ascertain a phone number, address, or resident registration number in order to quickly conduct an investigation without needless investigation or additional information acquisition on a person with the same name. Particularly, considering that phone numbers or addresses themselves do not directly contain the personal information or personality of the individual, just including phone numbers, addresses, and resident registration numbers cannot be seen as an excessive restriction.

(c) Reasons for Request for Provision of Communications Data

The Act Provision limits the reasons for which the investigative agency makes the request for provision of communications data to "information collection for investigation, execution of a sentence, or prevention of any harm to the guarantee of national security."

First of all, when there is a suspicion of a crime, an investigation is carried out by an investigative agency to confirm whether a crime has actually been committed, to locate and secure the suspected, and to collect and preserve evidence. In light of the recent tendency of the investigation to minimize human rights violations in the process of the investigation, by reducing *in personam* investigations and expanding *in rem* investigations in the early stage of an investigation, communications data are acknowledged to be necessary as they are of help not to cause unnecessary misunderstanding and anxiety that a person is a target of an investigation whilst they serve to identify who are related to the users of

the communications data and to decide whether to be used in an investigation. In addition, the Telecommunications Business Act first prescribes the general duty to protect communication secrets handled by telecommunications business operators in Article 83, Sections (1) and (2), and then the request for provision of communications data as an exception in Section (3) of the same article. This indicates that the Act intends that under the premise of strictly protecting communications privacy, personal communications data can be provided to the investigative agency et al., only in exceptional cases, in a limited manner. Therefore, the act of acquisition of communications data for investigation is permitted only within the minimum range necessary for the identification of a suspect or a victim or the collection and discovery of evidence in a situation where there are reasonable grounds for a suspicion of crime.

Next, with regard to communications data for the execution of a sentence, the execution of a sentence means executing a sentence when the sentence is imposed by judgment of a court, etc. While most of the decisions contain information about the defendant against whom a sentence is executed, if the defendant flees after the sentence is finalized, it is necessary to acquire communications data of the defendant or people around him or her to secure him or her. Therefore, communications data for the execution of a sentence is allowed only within the minimum extent necessary to execute a sentence.

On the other hand, Complainants argue that it is excessive to permit the request for provision of communications data even for simple information collection to prevent harm to the guarantee of national security. However, “harm to the guarantee of national security” does not mean minor violations of public order or criminal acts, but an act that poses a danger to the existence of the State or the basic order of the Constitution. In this regard, it is essential to quickly identify those involved in such act and prevent any harm in advance. Thus, we acknowledge the necessity for the request of the provision of communications data to the minimum

extent necessary to collect information for the purpose of preventing any harm to the guarantee of national security.

(d) *Ex-ante and Ex-post* Management of Communications Data

The Act Provision is mainly used to "identify" those involved in a crime at the initial stage of investigation or information collection. Although the Telecommunications Business Act does not ask for a user's consent in advance, nor a court's permission, in consideration of the promptness and secrecy required in the early stage of such investigation or information collection, it manages communications data by regulating the ways to request the provision of communications data, or by mandating reports on the current status of the provision of communications data.

First of all, the request for provision of communications data pursuant to the Act Provision shall be made in writing, which states a reason to request the data, its relevancy to the user, and the scope of necessary data (main clause of Article 83, Section (4) of the Telecommunications Business Act). Where it is impossible to make a request in writing due to urgency, such request may be made other than in writing, and when such reason is resolved, a Written Request for Provision of Data shall be promptly filed with the telecommunications business operator (proviso to Section (4) of the same article). When a telecommunications business operator provides communications data, it shall retain a ledger containing necessary matters such as the provision of the communications data and related data such as Written Requests for Provision of Data (Article 83, Section (5) of the same act). Also, the operator shall report on the current status of the provision of communications data to the Minister of Science and ICT twice a year, and the Minister thereof may check the management status of ledgers and requests for data provision, etc. and whether the details of a report submitted by a telecommunications business operator are correct (Section (6) of the same Article). A telecommunications business operator shall notify the head of a central administrative agency whereto a person requesting the provision of

communications data belongs of the fact of the provision of communications data (main text of Article 83, Section (7)).

In addition, with respect to the acquired communications data, an investigative agency shall keep the secret known to him or her in the course of the investigation in accordance with Article 198, Section (2) of the Criminal Procedure Act. Also, the staff of National Intelligence Service Korea shall not divulge secrets learned in the course of performance of their duties pursuant to Article 17, Section (1) of the National Intelligence Service Personnel Act, and if they reveal, they shall be punished for the offense of divulgence of official secrets (Article 127 of the Criminal Act).

(e) Therefore, in light of these considerations, the Act Provision does not violate the least restrictive means, as it ensures that the request for provision of communications data by the investigative agency et al. is made to the minimum extent necessary to achieve the purpose of information collection, such as investigation.

3. Balance of Interests

The personal information provided to the investigative agency et al. pursuant to the Act Provision is limited to the most basic information necessary to identify an individual, such as his or her name, and does not include any sensitive information. Furthermore, the reasons for requesting the provision of communications data are limited to information collection for investigation, execution of a sentence, or prevention of harm to the guarantee of national security. Therefore, taking into account the public interest, such as the necessity for prompt and efficient investigation, the execution of a sentence, the discovery of substantive truth, the proper exercise of the State's punitive authority, and the guarantee of national security, all of which are to be achieved by the Act Provision, it is hard to say that restricted private interest outweighs the public interest of the provision of communications data to

the investigative agency, et al. under the Act Provision. The Act Provision satisfies the test of balance of interests.

4. Sub-conclusion

Therefore, it does not seem that the Act Provision infringes on Complainants' right to informational self-determination by violating the rule against excessive restriction.

F. *Whether Principle of Due Process of Law Is Violated*

1. The principle of due process of law of Article 12 of the Constitution applies not only to criminal proceedings but also to all State actions. Important procedural requests that also derive from the principle of due process of law include properly notifying the party and giving him or her opportunities to submit his or her opinions, relevant data, etc. However, what procedures are specifically required by this principle and to what extent should be decided individually by comparing various factors, such as the nature of the matter regulated, the rights and interests of the parties concerned, the value to be enhanced by the implementation of the procedures, the efficiency of State action, the cost of the procedures, the opportunity for objection, etc. (*see* Constitutional Court 2014Hun-Ma1178, April 26, 2018).

2. If a request for provision of communications data is made pursuant to the Act Provision, a user, or the data subject of the communications data, will not be given advance notice of the making of the request, and where a telecommunications business operator provides communications data to the investigative agency et al., it will not separately notify users of the provision; thus unless he or she separately demands the telecommunications business operator to let him or her peruse the information of the provision of communications data in accordance with Article 35, Section (1) of the Personal Information Protection Act, the

user will never know whether his or her communications data have been submitted to the investigative agency et al. However, the notification to the party is very important in that it is a prerequisite for the party to confirm restrictions on his or her fundamental rights and to dispute its legitimacy. Therefore, it is not permitted to ignore the constitutional procedural request just owing to the necessity to promote promptness and confidentiality of activities such as investigation or information collection.

Given the need for efficient investigation, prompt and covert information collection, etc., it can be said that the request for provision of communications data under the Act Provision should not be notified to the user, or the data subject, in advance of the provision of the data requested. However, after the investigative agency et al. have acquired the communications data, it is possible to notify the acquisition of communications data to the user to the extent that it does not interfere with information collection purposes, such as investigation. By notifying the acquisition of communications data by the investigative agency et al., users would check whether both the request of provision and provision of communications data were made in accordance with lawful procedures, or whether the communications data were used in accordance with the purpose of the provision. If they found any illegal or unfair act of the investigative agency et al., they could control the illegal or unfair use of their personal information by taking appropriate remedy procedures.

If concerns exist that such notification causes difficulties in investigation or information collection activities, or that it violates others' fundamental rights, such concerns can be resolved to some extent by the following means: by carving an exception to notification for cases with a high probability of crime that establish objective reasons, such as evidence destruction, escape, etc.; by requiring, in principle, to inform about communications data acquisition within a certain period after the acquisition, while, if there are special reasons, such as the need for

security maintenance, mandating notice be given of such acquisition within a certain period after investigation or information collection activities are completed; or by requiring to give notice of the fact that a request for provision of communications data and the requested provision were made, while allowing not to inform about the specific reason for the request when the disclosure of the specific reason for the request is likely to infringe the fundamental rights of others. Nevertheless, the Act Provision does not adopt any notification procedure, keeping the user, or the data subject, from being aware of the fact that his or her personal information was provided to the investigative agency et al., and seizing the opportunity of controlling his or her personal information.

Certainly, in accordance with Article 35, Section (1) of the "Personal Information Protection Act," the user can demand the telecommunications business operator to let him or her peruse the details of the provided communications data. However, in such case, the user can inspect the details of the communications data provided for one year prior to the request (Article 53, Section (1) of the Enforcement Decree of the Telecommunications Business Act). The information that can be perused through this procedure includes what is recorded and stored by the telecommunications business operator in the communications data provision ledger, i.e., the "date of the provision, requesting institution, reason for request, details of the provision, etc." (Article 83, Section (5) of the Telecommunications Business Act.) Moreover, the reason for the request is conventionally described as "Article 83, Section (3) of the Telecommunications Business Act"; so it makes it difficult for users to know the exact reason their information was provided. Since in most cases, without special reasons, the citizens do not suspect that their communications data have been provided to the investigative agency et al., and just because some active data subjects can inspect the details of the provided communications data through the "Personal Information Protection Act," such procedure cannot be substituted for *ex-post* notification procedures under statutes and regulations.

3. Therefore, the Act Provision that does not provide for *ex-post* notification procedures for the acquisition of communications data violates the principle of due process of law and thus infringes on Complainants' right to informational self-determination.

G. *Necessity for Constitutional Nonconformity Decision*

In principle, if a law is in violation of the Constitution, it must be declared unconstitutional. However, if there is a concern that removing a statutory provision from the legal order through a decision of unconstitutionality would cause a legal vacuum or confusion, this Court may make a decision of nonconformity, ordering the provisional application of the unconstitutional provision (*see* Constitutional Court 2018Hun-Ma927, August 28, 2020; Constitutional Court 2020Hun-Ma895, January 27, 2022).

The Act Provision is unconstitutional not because the acquisition of communication data *per se* does not conform to the Constitution but because it fails to establish *ex-post* procedures to give notice of the acquisition thereof; so, if we rendered a decision of simple unconstitutionality on the Act Provision, and it lost its effect immediately, there would exist no legal grounds for the acquisition of communications data, creating a legal vacuum. Therefore, instead of declaring the Act Provision simply unconstitutional, we deliver a decision of nonconformity and order that it continues to be applied until its amendment. The Legislature shall revise the Act Provision as soon as possible, at the latest by December 31, 2023.

VI. Conclusion

In conclusion, as the claim against the Act of Acquiring Communications Data and the claims of Complainants Y.B., P.H., S.S., K.J., and J.M. are

non-justiciable and the Act Provision does not conform to the Constitution, the Court makes a decision of nonconformity and concludes, at the same time, that the Act Provision continues to apply on a temporary basis until the Legislature amends the provision by the deadline of December 31, 2023, as set forth in the Holding. This decision was made with a unanimous opinion of participating Justices, except Justices Lee Suk-tae, Lee Youngjin, Kim Kiyoung, Moon Hyungbae, and Lee Mison, who filed a concurring opinion as to the Act of Acquiring Communications Data in this case, as set forth in VII below, and Justice Lee Jongseok, who filed a concurring opinion on the Act Provision, as set forth in VIII below.

VII. Concurring Opinion of Justice Lee Suk-tae, Lee Youngjin, Kim Kiyoung, Moon Hyungbae, and Lee Mison on the Act of Acquiring Communications Data

We agree with the conclusion that the claim against the Act of Acquiring Communications Data is non-justiciable, but we believe that this Court should recognize the Act of Acquiring Communications Data as an exercise of governmental power but dismiss the claim against it for lack of justiciable interest. Our concurring opinion is as follows:

A. First, we examine whether the Act of Acquiring Communications Data constitutes an exercise of governmental power that is subject to a constitutional complaint.

The investigative agency et al.'s request under the Act Provision for provision of communications data is a way of a non-compulsory criminal investigation. As such, when considering the textual structure of the Act Provision alone, it seems that a telecommunications business operator voluntarily determines whether it will provide the requested communications data. However, if the investigative agency et al., having investigative power, which is the governmental power, ask a

telecommunications business operator to furnish communications data, the request itself greatly burdens the operator. Furthermore, if the operator does not accede to the request, the investigative agency et al. may obtain the communications data of users by executing a search and seizure warrant, and this can interfere with the business of the operator, which makes it less likely for the operator to deny the request for provision while bearing such burden.

Even though the Act of Acquiring Communications Data *in personam* was performed not on Complainants listed in Appendix 3 and Appendix 4, the users of the telecommunications service, but rather directly on the telecommunications business operators, the Act of Acquiring Communications Data *in rem* was directed at the communications data of the above Complainants, inhibiting Complainants' fundamental rights, not those of telecommunications business operators. Thus, this Court should judge whether the Act of Acquiring Communications Data caused direct legal effects on rights and duties of the citizens and constituted an exercise of governmental power that put Complainants' legal relations or status in an unfavorable position, in consideration of the above Complainants, who are users, and not in consideration of the telecommunications business operators. Nonetheless, as the Act of Acquiring Communications Data was conducted, regardless of the will of the above Complainants, who are data subjects, there was no room for those Complainants to intervene in preventing the telecommunications business operators from providing the data and the legal status of Complainants became disadvantaged upon the investigative agencies' acquisition of their communications data.

As a consequence, the Act of Acquiring Communications Data constitutes a *de facto* exercise of power as being an *in rem* investigation of communications data, personal information of Complainants listed in Appendix 3 and Appendix 4, by Respondents in a superior position (*see* dissenting opinion by Justices Kim Jong-Dae, Song Doo-Hwan, and Lee Jung-Mi, Constitutional Court 2010Hun-Ma439, August 23, 2012), and

so is an exercise of governmental power subject to a constitutional complaint.

B. Next, we examine whether the claim against the Act of Acquiring Communications Data is recognized as having a justiciable interest.

Since the Act of Acquiring Communications Data had already been finished, the subjective justiciable interest of the Act of Acquiring Communications Data did not exist when Complainants filed the constitutional complaint. As a constitutional complaint functions not only as a guarantee for a remedy of subjective rights but also as a guarantee for constitutional order, a justiciable interest is recognized when a violation of the same type is likely to be repeated in the future, and the constitutional clarification on it is crucial, and therefore we will review this matter (*see* Constitutional Court 2009Hun-Ma527, December 29, 2011; Constitutional Court 2016Hun-Ma263, August 30, 2018).

As the Act of Acquiring Communications Data was conducted pursuant to the Act Provision, similar infringements on fundamental rights are likely to be repeated because the Act Provision exists. Moreover, Complainants listed in Appendix 3 and Appendix 4 complained of the Act Provision as well as the Act of Acquiring Communications Data, but when considering the purpose of their complaint, what they ultimately challenge is the constitutionality of the Act Provision that allows the investigative agency et al. to acquire communications data of users without their consent by requesting telecommunications business operators to provide the communications data. Thus, taking together, *inter alia*, the purport of the argument of the above Complainants and the effectiveness of remedies for rights, there is no actual gain in recognizing a separate justiciable interest with respect to the claim against the Act of Acquiring Communications Data, since the claim against the Act Provision is acknowledged as justiciable and proceeds to the merits (*see* Constitutional Court 2016Hun-Ma263, August 30, 2018).

In conclusion, we hold that Complainants listed in Appendix 3 and

Appendix 4 do not have a protectable justiciable interest in their claim against the Act of Acquiring Communications Data, and thus such claim is non-justiciable.

VIII. Concurring Opinion of Justice Lee Jongseok on the Act Provision

I believe that the Act Provision is contrary not only to the rule of due process of law but also to the rule against excessive restriction. The reasons for my opinion are explained below.

A. *Legitimacy of Legislative Purpose and Appropriateness of the Means*

The Act Provision allows an investigative agency et al.'s acquisition of communications data of users, if necessary, by requesting a telecommunications business operator to provide the data thereof so as to promote speedy and effective investigation, execution of a sentence, and preventive actions to ensure national security and to contribute to the discovery of substantive truth, and proper exercise of the State's punitive authority and national security; thus, the legitimacy of its legislative purpose and appropriateness of the means are acknowledged.

B. *Least Restrictive Means*

1. The State plays various roles as a producer and distributor of public information and as a protector of personal information. Communications data are less sensitive than communication confirmation data, but due to the recent advance in big data, one might obtain intimate and essential information of users by combining such information. Consequently, the investigative agency et al.'s securing of personal information via communications data should be limited to the minimum extent necessary,

and objective control procedures should be established.

2. First, the Act Provision sets forth the reasons for requesting the provision of communications data in an overly comprehensive and broad way.

The rapid advance of information and communications technology has increased the risk that various information including personal details can be accumulated, used, or revealed by third parties, regardless of data subjects' will or awareness. Against this backdrop, if the investigative agency et al. are allowed to acquire extensive communications data through telecommunication business operators, which hold information of numerous users in an intensive way, they can possess a huge amount of information rapidly and make use of derived information by analyzing the collected information, which may lead to significant restrictions on right to informational self-determination of individuals, as data subjects, but also on individuals' freedom of privacy and communications. Thus, the acquisition of communications data by the investigative agency et al., through the request for provision of communications data, should be restrictively allowed under strict parameters, and this is all the more so when considering the fact that the investigative agency et al. make the request of the provision of communications data without a warrant or prior authorization by a judge.

However, the Act Provision sets forth as requirements very broad grounds, i.e., collecting information for investigation, execution of a sentence, or prevention of harm to the guarantee of national security.

An investigation is an activity conducted to discover the truth of the allegation, to identify a criminal, and to collect and preserve evidence when there is a suspicion of crime. As the types of crimes become diverse, the subjects of investigation are continuously increasing, resulting in broadening the scope of investigation. Also, since there is an indistinct line between the preliminary investigation phase and the pre-investigation phase, it is, in fact, possible that all activities of the

investigation agency et al. will fall within the scope of “investigation” in the Act Provision. Furthermore, the information collection to prevent harm to the guarantee of national security has a wider area coverage. “Information collection” literally means acquiring information, and its scope is very wide as its period, start and end dates, etc., are not identified. In addition, execution of a sentence shall be carried out after the judgment has become final except as otherwise provided by statute (Article 459 of the Criminal Procedure Act), and as a written decision states most of the information of a defendant whose sentence is to be executed, an acknowledgment of a need to request communications data for execution of a sentence would be limited to cases where, *inter alia*, the defendant flees after his or her sentence becomes final so it is necessary to secure his or her person. However, the Act Provision raises the possibility of abuse by the investigative agency et al., through the broad requirement of “in the case that it is necessary to execute a sentence.”

As for the investigative agency et al.’s request for provision of communications data, they should be required to make the request in minimum, necessary cases where those data are necessary to achieve the purpose of a trial or investigation by the investigation agency et al. Such cases should be confined, *inter alia*, to those where it is necessary to investigate a crime that is considered grave given the statutory sentence therefor, etc. (significance of a crime); where exceptionally speedy investigation is needed to prevent a crime, or additional one (urgency); where other measures make it impossible or cause significant difficulties to conduct an investigation; where it is hard to execute a sentence due to the failure to secure the defendant; or where there is a realistic probability that serious harm to the guarantee of national security will be inflicted. Moreover, as the investigative agency et al. can acquire necessary communications data via a search and seizure under the Criminal Procedure Act, limiting the scope of the request for communications data, which is allowed as a way of non-compulsory criminal investigation, will

not severely hamper “information collection for investigation, execution of a sentence, or prevention of harm to the guarantee of national security.”

3. What’s more, communications data that the investigative agency et al. acquire, in accordance with the Act Provision, serve as an identifier to get access to other information or involve a risk of becoming sensitive personal information when combined with other personal information.

Among communications data provided to the investigative agency et al., names, addresses, phone numbers, IDs, or dates of subscription and termination *per se* may not be sensitive information. However, when that information is combined or analyzed with other communications metadata, it can evolve into information that details individual activity, social relationships, personal and political preference, etc. in a concrete way, beyond mere information that the content of personal communications delivers. In particular, as resident registration numbers, which can be called a master key, contain a huge amount of information, which is much more than just identifying individuals, they can serve as a connector to other sensitive information. If the Act Provision is mostly utilized to identify a suspect or a victim at the early stage of investigation or information collection, the acquisition of communications data such as names, dates of birth, addresses, and phone numbers of users will suffice to achieve its purpose.

4. Additionally, the Act Provision does not have direct rules about an *ex-post* management system of the communications data acquired by the investigative agency, et al., including retention period or disposal procedures.

The entities that may obtain the communications data of users under the Act Provision are a prosecutor, the head of an investigative agency (including the head of a military investigative agency), or the head of an intelligence and investigation agency, which herein includes executive departments vested with judicial police power, such as the Ministry of Justice, Ministry of Employment and Labor, and Ministry of Food and

Drug Safety. In a situation like this, despite a broad range of communications data collectors under the Act Provision, the Telecommunications Business Act does not have provisions for *ex-post* management of the acquired communications data, including their retention period or disposal procedure, and each collector deals with the affairs in accordance with their own practices.

In particular, today, because information can unlimitedly be stored through computing processing and be combined with other information, almost all the data regarding individuals can be aggregated and accumulated. In this situation, the leakage of communications data may wreak unexpected havoc. Furthermore, as such information can be stored without time limitations, it is undeniable that the information, if continuously amassed, can be abused, unlike the purpose of the Act Provision. Consequently, introducing clear procedural provisions regarding the retention and disposal steps of the acquired communications data and establishing strict controls are the minimum safeguards of fundamental rights with which the information can be collected and used to a necessary minimum extent. Nevertheless, the Act Provision entrusts the investigative agency et al. with storing and disposing of the collected information without any procedural controls, exposing personal data of citizens to the risk of being abused by the investigative agency et al.

5. Taking into account the abovementioned considerations, the Act Provision does not satisfy the least restrictive means test because it allows the investigative agency et al. to make the request for the information that can amount to sensitive information for extensive and broad reasons and because it lacks a mechanism for *ex-post* management of data, such as their retention period or disposal procedures.

C. *Balance of Interests*

Considering that if derivative information is combined with the communications data that are furnished to the investigative agency et al.

pursuant to the Act Provision, this poses the risk of allowing access to intimate personal information and that the communications data acquired by the investigative agency et al. may extensively be collected and used for a long time, the Act Provision, which allows communications data to be provided to the investigative agency et al. regardless of the will of data subjects, imposes significant restrictions on self-determination on personal information. The same is true when considering the public interest of guaranteeing a speedy and effective investigative or intelligence act, which the Act Provision intends to achieve. In conclusion, the Act Provision violates the principle of balance of interests as well because the private interest it restricts outweighs the public interest it intends to defend.

D. *Sub-conclusion*

Therefore, not only does the Act Provision violate the principle of due process of law by failing to establish *ex-post* notification procedures, but also it violates the rule against excessive restriction for the reasons set forth above.

Justices Yoo Namseok (Presiding Justice), Lee Seon-ae, Lee Suk-tae, Lee Eunae, Lee Jongseok, Lee Youngjin, Kim Kiyoung, Moon Hyungbae, and Lee Mison