J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

A Study on the Improving Information Investigation Techniques to guarantee Internet Safety and Personal Privacy☆

배 초 희[1] 이 지 우[1] 이 경 렬[2*]
Chohee Bae Jiwoo Lee KyungLyul Lee

ABSTRACT

Through the ex post facto restraints, the Constitutional Court ruled that the investigative agency's right to request communication data stipulated in the TBA §83 violates the right to self-determination of personal information and the due process. As legislators must revise related laws to conform to the Constitutional Court ruling by 2023.12.31, it is urgent to prepare legislative measures that meets the PCSA § 13, the TBA § 83, and the PIPA §18. On the other hand, the U.S. is implementing revere-location search warrant based on geo-fencing technology, a technology that sets a virtual boundary and provides a service to record or reprocess the location based on recorded information. It caused legal problems, such as collecting a large amount of location information kept by ISPs or platform companies, and indiscriminately collecting information of unrelated individuals. Accordingly, New York has proposed a revised Criminal Procedure Act to limit the indiscriminate collection of personal information. The problem of extensive search and seizure of digital data can also arise from trans-border access to cloud servers. The way to decide the place is different between GPS and the base station method. Also, the accuracy is low at the base station. According tothe current rule of the warrant, the investigative agency can only use the base stations' information for investigation. Also, they must specify the subject of the search and seizure and cannot collect unrelated information. Through a comparative analysis of the problem of widely collecting and tracking individual location information with geo-fencing technology in the U.S., this study aims to prepare improved legislative measures that put the brakes on the current investigation practice of indiscriminately collecting telecommunication data. According to the law, a warrant cannot be issued unless the suspect can be identified; however, preliminary information should be gathered for the investigation to identify the culprit. This study therefore proposes the retention of a warrant system that was supervised by prior judicial institutions while introducing warrants for information gathering at a level that is laxer than the current one. By proposing the modification of search and seizure warrants for digital evidence, this study expects to enhance the effectiveness of forced investigations that meet due process and the right to self-determination of personal information.

☞ keyword : communication data, privacy in internet, self-determination of personal information, improved legislative measures, geo-fencing technology, warrant of digital evidence

1. Introduction

The Constitutional Court ruled on July 21, 2022, using ex post facto restraints, that the investigative agency's right to request communication data stipulated in the Telecommunications Business Act (TBA) §83 violates the right to self-determination of personal information and due process. The communication data includes information that can identify individuals, such as names, registration numbers, addresses, and phone numbers, which can be obtained through random requests from telecommunication business without a warrant. This has been controversial since the owners of the information are not notified of such disclosure. Thus, the Court demanded that the improvement legislation should be made by Dec 31st, 2023 [1] [2].

A mobile phone may track an individual'slocation by backtracking the facts communicated with a base station. With the development of technology, the problem of infringement of personal information has reached a serious level due to collecting more accurate user information by using GPS-based virtual fence designation. The legal restrictions are needed to guarantee rights to citizens as possibility of indiscriminate use

1 Dept. of Law, Graduate School of Sungkyunkwan University, Seoul, 03063, Rep. of Korea
2 Law School of Sungkyunkwan University, Seoul, 03063, Rep. of Korea
* Corresponding author: KyungLyul Lee (klee04@skku.edu)
[Received 3 April 2023, Reviewed 11 April 2023(R2 June 19 2023), Accepted 21 June 20]
☆ A preliminary version of this paper was presented at ICONI 2022.

of information of non-suspects increases. Thus, this study aims to review the inconsistency between the TBA §83, the Protection of Communication Secrets Act(PCSA)[3], and the Personal Information Protection Act(PIPA)[4], thereby presenting problems and legislative solution if geo-fencing is used in Korea. This study will also analyze the U.S. system in comparative perspective to propose possible solution.

2. Domestic Laws related to utilization of personal information

2.1 Combination Order 2016Hun-Ma388

In this Constitutional Court case, the claimants argued that it was unconstitutional to provide communication data related to the claimant to the investigative agency in accordance with the TBA §83. The Court ruled that even though the provision limits the right to self-determination and does not apply the rule of warrant, it does not violate the proportionality principle since it leads to the discovery of substantive truth in the early stages of criminal investigation. However, the Court also ruled that even though the notification to users can be omitted due to the confidentiality of investigation and the rapidity of information collection, it can still violate the due process in that there was no post-notification procedure [1]. Thus, the Court requested to amend the law by Dec 31st, 2023.

2.2 Problem of the incompatibility between the Laws

The TBA § 83 stipulates that the telecommunication business holders can voluntarily follow the investigative agencies'request of communications data. This Act does not require warrant and a notification of inspection facts. Thus, there is a room for due process violation since there is a possibility of infringement of rights such as self-determination of personal information and privacy. The essence of the warrant requirement is to go through a non-biased judge's decision on compulsory dispositions such as search and seizure and arrest [1]. Under the current PCSA, the investigation of base station is subject to warrant as it is a compulsory disposition. Considering that communication data can infer sensitive personal information when combined with other information and that the acquisition and use of irrelevant information can be problematic, compulsory disposition should be applied rather than arbitrary disposal. In addition, the acquisition, use, and storage of irrelevant and separate information can be a problem rather than the vastness of information in requesting communication data [5]. As a result, it is necessary to restrict the acquisition or storage of irrelevant information.

The PCSA was partially revised in 2005 to ensure the fundamental rights by establishing strict procedures for requesting an access and provision of communications data. The revision includes mandatory 'permission from the court' and post-notification when requesting communication information confirmation data. As a result, investigative agencies often use data provision request stipulated under TBA rather than obtaining the permission from the court under the PCSA. After the introducing the warrant system, it is assumed that the investigative agencies are gathering information in a manner that is not limited by a warrant [6].

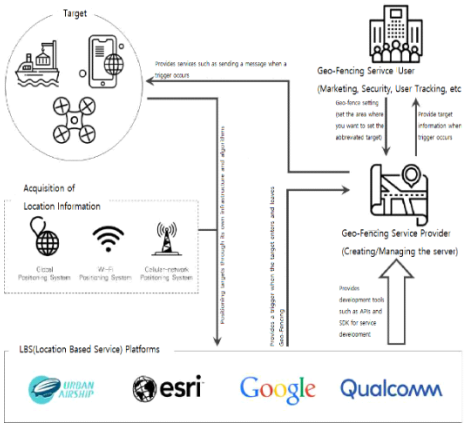
Personal information, defined as "all information on a specific individual's physical and personal relationship,"[7]can be protected by the PIPA if communication data is converted into specific information. Furthermore, under the current PIPA § 18(2), protections are excluded if there are special provisions in other laws. However, because there are no related laws, information and communication businesses are more likely to break the law. However, these communication data are required for investigative agencies to prevent crime and resolve cases as soon as possible. When restrictions or the subsidiarity principle areadded, difficulties in investigation are to be expected, thereby potentially posing a risk to public safety. As a result, it seems necessary to have a plan that encompasses both crime resolution and personal information protection.

3. Location Information: Technology and Utilization

3.1 Geo-fencing technology

Geo-fencing works by recording the response of mobile device, RFID, and apps as present when someone enters a virtual boundary set by an administrator [8][9]. Geo-fencing is inexpensive and does not require any additional applications

[10]. Beacon is similar in that it interacts with mobile devices in the designated area, but it is also different in that it requires device installation and lacks sophistication [11]. Furthermore, the process of creating geofences and setting up algorithms focuses on combining the users'interest in collecting current location information with the perception of proximity [12]. The information used during this process, such as GPS, Wi-Fi, and cellular data, follows the format of latitude and longitude coordinates taken from GPS devices. And these coordinates generate trigger events according to the boundary defined as geofence [13]. To leverage geo-fencing, administrators or developers must first set virtual boundaries around specific locations in GPS or RFID-enabled software, and virtual geo-fence responds when authenticated devices enter or leave the designated area [8].



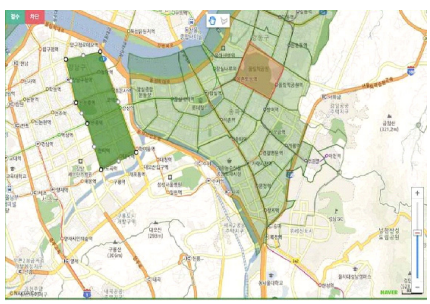
(Figure 1) Diagram of Geo-Fencing Technology

3.2 Trax: App for storing location information

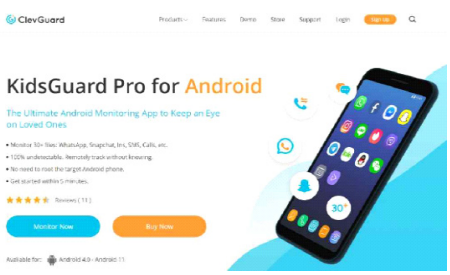
Trax, created by a former police officer in the United States, recognizes all types of mobile phone data received from an information provider, stores wireless bass station locations, visualizing call information, and creates an investigation warrant. It enters into the program after collecting records, and generates KML file that retrieves all used base station information located in the area in chronological order. In addition, the information between base stations is combined to show the users'location by backtracking the distance of cell signal and the call length. As a result, phone records can be analyzed to show people's whereabouts and where they spend a lot of time, as well as to track the location of specific incidents like murder and theft [14].

3.3 The Use of Geo-Fencing Technology

Geo-fencing technology is used in various fields. In the United States, large shopping malls are marketing themselves by providing customers discount coupons of nearby stores based on the customer location collected with the utilization of geo-fencing technology [15]. In case of delivery apps, radius of stores is set to provide services based on actual location of customers [16]. Also, an app that can track children in real time is being used by utilizing geo-fencing technology [17]. It seems possible to establish a notification service for pre-designed memo when a user approaches the location using geo-fencing technology[18]. In addition, the university attendance system, which uses contactless RF cards or barcodes, can make attendance through records of access to and from the relevant classroom if geo-fencing technology can lead to a development of system that divides each classroom into virtual boundaries [10].



(Figure 2) Use of Geo-Fencing in Delivery Apps



(Figure 3) Example of Children-Tracking App that utilizes Geo-Fencing

4. Geo-Fencing Technology in the U.S.

4.1 Reverse Location Search Status

Based on Google Maps, GPS, and recently Trax technology, the United States has begun to actively utilize geo-fencing or reverse location search [19]. Since 2016, the number of geo-fencing warrants executed by the U.S. investigative agencies against the Internet Service Providers (ISPs) such as Google has steadily increased, especially from 982 in 2018 to 8,396 in 2019, and 11,554 in 2020[20]. Currently, the United States is using reverse location tracking in states such as Arizona, Florida, Maine, New York, North Carolina, Texas, Virginia, and Washington D.C, as well as the FBI [21].

4.2 Reverse Location Search Warrant Execution

The following is the procedure for carrying out the U.S. investigative agency's reverse location search warrant. First, the investigative agency executes an initial warrant to retrieve location information of smartphones around the crime scene from ISPs such as Google. Based on this information, the investigative agency analyzes individual movement patterns to identify potential suspects and executes a second warrant for more specific information. The first warrant provides only anonymous information, whereas the second warrant includes personal name and account information as well [19] [20]. Thus, reverse location search warrant is executed through multiple executions rather than one process.

4.3 Related Issues in the U.S.

4.3.1. Possible Violation of the 4th Amendment

The 4th Amendment's basic goal is that peoples'right is violated when there is a search and seizure and arrest by the government without a probable cause. The Supreme Court, through the Brinegar case, stated that simple suspicion is not enough to determine the probable cause [22]. The court also stated through the Carpenter case that the 4th Amendment, which can only be protected with the prevention of infringement of high-tech technology, is legal only when the location information is collected through a warrant [23].

Reverse location search is useful in the cases that only has few or zero suspects or evidence [20]. The fact that a warrant is issued without a suspect is a big difference from the traditional warrant. In other words, unlike traditional warrant, it is executed by obtaining location information of all individuals at a specific time and location and tracking it reverse [20]. However, this leads to criticisms that it lacks a probable cause since the criteria of issuing is ambiguous [20] and non-related individuals are subject to such comprehensive collection of information [19]. But the Supreme Court has not yet specifically addressed the reverse location search warrant, although it should [20].

4.3.2. Limits caused by Technology

There is an opinion that the reason for lack of probable cause is due to the limitation of technology. For example, Google claims that their location accuracy is 93%, while 2018 report shows that there is a radius error of 50 meters [19]. This leads to a problem as it can increase the possibility of collecting information of non-related individuals.

4.4. Attempted Solutions

The Supreme Court ruled that in circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative [24]. In accordance with the court, laws were tried in both state and federal levels.

New York is the first state to come up with the law that prevents entire geo-fencing [20], and it is still in discussion [25]. In federal level, Geolocation Privacy and Surveillance Act was discussed in 2011. Though it was not passed, there was an attempt to pass this law again in 2017 [26].

There were also attempts to impose the different standard of probable cause requirement for geo-fencing [19][20]. The Supreme Court has already recognized exceptions such as emergency tracking [27] and the urgency of the issue [28][29]. Thus, there is a room for an interpretation that reverse location search warrant can fall into such urgency exception [19].

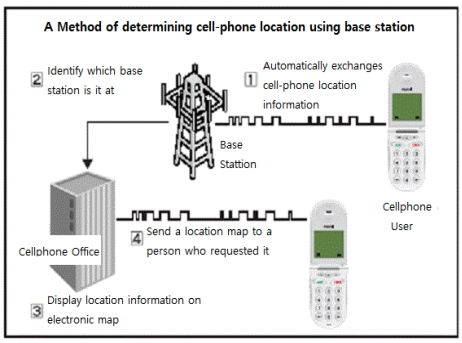
4.5 Implication to Korea

In the U.S, there is a claim to abolish the reverse location search warrant since it is unconstitutional. However, since its necessity is recognized in terms of investigation process, revision, which includes re-interpreting the 'probable cause' of the 4thamendment, is proposed. Applying a separate and mitigated requirement of probable cause is tantamount to creating a separate requirement that is applied specifically to tracking of location information. This means that it is possible to consider introducing another independent warrant system. If these separate and independent requirements can be recognized, then the reverse location warrant can be introduced in Korea.

5. Proposed Legislative Improvement Measures for Protection of Personal Privacy

5.1. Acquisition of Location Information using Base Stations under current PCSA

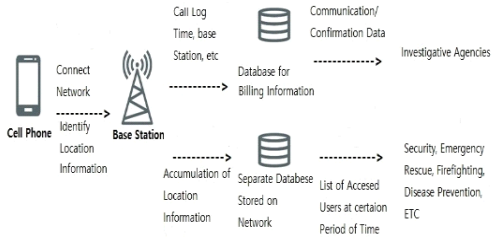
Currently, investigative agencies can only acquirelocation information by using base stations, since there is no reverse location warrant and investigativeagencies are not allowed to use real-time GPS tracking system. The process of acquiring location information using base stations is described as below.



(Figure 4) A Method of determining Location Information by using Base Station

When a user uses a cell phone, it connects through a nearby base station. And when the base station connects the cell phone network, it records the connection history. Thus, the fact that investigative agencies use the base station means that they use the connection history stored in the base station. It is possible to ex post-mortem the approximate location of the user through the location of the used base station.

Both GPS tracking/geo-fencing and base station search are similar since both are used for collecting location information. However, base station is different from GPS tracking since ①¨ç base station can only provide non real-time approximate information and ②¨è GPS tracking is not allowed for investigation purposes. The difference in terms of information collected for different purposes are described as below.



(Figure 5) Difference in Collected Information according to Utilization Purposes.

Currently, GPS tracking is only allowed for purposes such as security[30][31], firefighting[32], disease contamination and tracking infection routes[33], emergency rescue[32], etc. Real-time GPS tracking cannot be utilized through current warrant system, and thus, only base stations can be used under PCSA or TBA. And as mentioned in Figure 5, the information collected via base stations are not real-time and only contains communication data. Thus, investigative agencies can only infer approximate location information through the stored communication records. Therefore, the proposed legislative improvements to be descried below aim to dissolve the discrepancy and incoherency between the different information collected according to different purposes. Since the communication records of base stations are only approximate, the collected GPS information should also be used in investigation via new warrant system when there is an allegation. And the aforementioned geo-fencing warrant utilized in the U.S. can serve as a leading example or guidance.

5.2. Development of Legislation for using GPS information

As described above, the investigative agencies can use the location information from base stations for investigation purposes. This method deduces the location by overlapping the radius of base stations', so it has lower distance accuracy than using GPS. GPS information is regulated under the Act On The Protection And Use Of Location Information(Location Information Act)[32]. The § 15(1) of the Location Information Act prohibits the use, provision and collection of information without individual consent. However, a proviso clause of § 15(1) allows related agencies or thepolice to collect and use GPS information for emergency purposes. Also, this information cannot be used except forpurposes under §29(8) of Location Information Act. Even within the police, investigation and emergency rescue are operated separately, and GPS information collected for emergency purposes cannot be used for investigation purposes. However, the ultimate purpose of emergency rescue and that of investigation are the same in that they both concern public safety.

The § 6(1)(e) of the EU General Data Protection Regulation(GDPR), allows for non-purpose use without individual consent when "processing is necessary for the performance of a task carried out in the public interest"[34]. And the U.S. stipulates that such information can be used for non-purpose use or in the same ways as subpoenas without individual consent for the national priority purpose[35]. Both GDPR and the U.S. allow non-purpose use without individual consent for public interests. In Korea, §18(2)7 of PIPA stipulates that personal information can be used for investigations, but Paragraph 2 stipulates that may use personal information or provide it to a third party for other purposes unless doing so is likely to unfairly infringe on the interests of a data subject or third party. Thus, even when used in the public interest, it may not be used in an investigation if there is a risk of infringing on the interests of the suspect. In this respect, it is different from the EU-GDPR and theU.S. described above. In other words, using the information for purposes other than those prescribed by current law is prohibited without a warrant.

Under current regulations, a warrant cannot be issued unless the suspect can be specified. However, the basic data collection for the investigation to identify the suspect should be carried out. Thus, this paper proposes the introduction of warrants for collecting information at a level that is more relaxed than the current one while maintaining a warrant system controlled by prior judicial agencies. If a warrant with relaxed conditions is introduced, it is expected that information necessary for the investigation can be collected while minimizing the infringement of legal interests through the control of judicial agencies. The § 6 and § 7 of the EU's Second Additional Protocol to the Convention of Cybercrime (Budapest Convention) provide prestigious regulations that allow signatories to directly request information from service providers in other countries that possess the necessary information. Contracting countries are also expanding their methods of collecting information for investigations within the scope of the law by allowing direct requests from service providers in other countries. Like a convention that allows information sharing among the parties, information sharing within state institutions may be possible based on the introduction of the relaxed warrant system. It is expected that a better investigative cooperation system can be established by creating an exchange and cooperation system for GPS information collected and stored within state agencies based on the introduction of a relaxed warrant system.

5.3. Modification of Current Warrant System

5.3.1. Introduction of a Relaxed Warrant System

There is no significant difference between the information provided through TBA and PCSAin terms of the content. However, there is a procedural difference in the rule of warrant and post-notification. Under the current warrant system, warrant can be requested only when the subject or the accused is identified. But this leads to the problem that such procedure cannot be used to track a wide range of location information or collect communication data to identify the subjects in the early stage of investigation. Since the need to identify the subjects in the early stage is recognized, it is possible to consider the introduction of a new relaxed warrant system that can be issued without specifying the target. Considering the aforementioned 'reverse location search warrant'of the U.S. as an example, it is possible to introduce a relaxed warrant with less regulations and conditions to collect location information.

5.3.2. The Expansion of the Current Warrant System to Collect Information

Due to the nature of the data, there may be more than one information holder. In the case of a cloud server, for example, the cloud service provider may also have access to the data stored on the cloud server. Thus, the information that should be requested to the individual can also be provided by the service provider.

Even under current warrant system, information may be provided to a third party. The tracing of the bank accounts is based on the Criminal Procedure Act § 215 and the Act on Real Name Financial Transactions And Confidentiality §4 (1) 1[36][37]. The investigative agency can choose the provider between the suspect or a third party like a bank. Therefore, by introducing a relaxed warrant system, it would be possible to request information from a third party except tracking the bank account as well.

5.4. Post-control Measures for Acquired Information

5.4.1. Control from the Subject of Information

The TBA § 83 received ex post facto restraints on the grounds that even if the communication data was disclosed to a third party, the party was not notified of the disclosure [1]. The subject of the disclosed information can plead through objection process when realizing such disclosure, but it is practically difficult to protestthe disclosure when it is not notified to the subject. If communication data was provided for investigation, those who are not related to the crime should also be notified of the facts after disclosure. If a certain period of time is set to the extent that does not affect the investigation and then notify the disclosure of information after certain period, it will not affect the confidentiality and will guarantee individual rights.

5.4.2. Deletion of Collected Information

Clear rules and regulations of information management is needed in terms of storing the collected information and discarding then after a certain period of time. Since the information collected under the TBA is likely to contain easily replicable and movable information that are not related to crime, clear necessity and limitations should be established for the management and storage of collected information.

5.4.3. Report to the Third Party

Current PCSA stipulates that telecommunication business holders are required to semiannually report arequest and a ledger for data provision to the Minister of Science and ICT. In case of the already existing communication data, according to TBA, certain post-restrictions can be imposed by reporting to a third-partyinstitution even if a new relaxed warrant system is introduced. Also, in case of telecommunication business holders that have provided information about specific person, it is reasonable to report a data provision request at the same level as protection under the PCSA to National Assembly. In addition to the request and a ledger for data provision, the transparency of information management should be ensured by regularly supervising the storage, disposal, and deletion of information through periodical management report.

6. Conclusion

Through the decision of 2016Hun-ma388, the problem of collecting communication information based on the Telecommunications Business Act, and the inconsistency of the Communications Secret Protection Act and the Personal Information Protection Act were examined. It is not desirable to construct and amend by adding only notification regulations based on the fact that more detailed location information has been tracked through the geo-fencing technology. In the United States, where related warrants exist, they are also legally restricted due to privacy issues.

If the investigation is under way, 13 bills, including a proposal to notify within 30 days after one year from the date of receiving the communication data, are currently proposed. The investigative agency says that if the relevant person is notified of the communication inquiry while the investigation is underway, there is a possibility of running away or destroying evidence, and that a careful revision of the law is needed. As there is a need to notify within the scope that does not harm or jeopardize the confidentiality of investigations, it seems desirable to designate the period beyond the usual

time during which the investigation usually proceeds.

In addition, as it is an investigation to specify the subject, it is time to introduce a warrant method that does not specify the subject, not the existing warrant method for specific people. The existing seizure and search warrant must be written in advance with the name of the Defendant, the object to be confiscated, and the place, body, and object to be searched and obtain permission from the court. However, in the case of communication information, it seems necessary to introduce a warrant system that is somewhat more relaxed (relaxed in terms of not specifying the accused)than the existing warrant, considering that the content is aninformation not specified by an individual. In the case of the United States, location information is collected using a 'reverse location search warrant' that can track mobile phone communication information in a specific location [38].

In order to protect personal information and guarantee basic rights, it is necessary to collect information through warrants. The relaxed warrant eases the specificity of the suspect and the criminal charge. With this proposed warrant, it is possible to prevent indiscriminate information collection by imposing restrictions while leaving open the possibility of receiving massive quantity of information from telecommunications operators to specify suspected criminals. Therefore, it is expected that the current seizure and search warrant can be used separately to collect information when a suspect is specified, and the proposedrelaxed warrant can be used separately to collect information to specify a suspect to a telecommunication business such as a server or cloud. To protect the collected location information, it is also possible to consider preparing post-control measures, such as a third-party reporting method by stipulating the National Assembly's obligation to control and notify users afterwards as stipulated in the Communications Secret Protection Act [6].

References

[1] Constitutional Court of Korea, Decision of 21 July 2022, 2016Hun-Ma388, 2022Hun-ma105·110·126.

[2] Telecommunications Business Act(TBA), https://elaw.klri.re.kr/kor_service/lawView.do?hseq=59855&lang=ENG (Date accessed: 2022.10.26.)

[3] Protection of Communications Secrets Act(PCSA) https://elaw.klri.re.kr/kor_service/lawView.do?hseq=59856&lang=ENG (Date accessed: 2022.10.26.)

[4] Personal Information Protection Act(PIPA) https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG (Date accessed: 2022.10.26.)

[5] B.K. Jeong, K.L. Lee, "On the material control of telecommunications surveillance and the problems of new §12-2 of the Telecommunications Secrets Act by the decision of the BVerGE 06.07.2016 - 2 BvR 1454/13", *Korean Journal of Comparative Criminal Law*, Vol 22, No. 2, pp. 105-128, 2020. http://dx.doi.org/10.23894/kjccl.2020.22.2.005

[6] M.E. Kim, K.L. Lee, "Problem and Suggestions regarding the 'Communication Data' System - Focusing on the protection of communication information -", *SungKyunKwan Law Review*, Vol 28, No. 1, pp. 71-95, 2016. http://dx.doi.org/10.17008/skklr.2016.28.1.003

[7] G.C. Lim, "Scope of protection of personal data", *Korea and Deutschland Law Journal*, Vol 17, pp. 223-248, 2012. https://ca.skku.edu:8443/link.n2s?url=https://kiss.kstudy.com/ExternalLink/Ar?key=3036422 (Date accessed: 2023.3.31.)

[8] S.K. White, "Understanding Geofencing 'More than Geospatial Information'", CIO, 2022. https://www.ciokorea.com/news/36136 (Date accessed: 2022.10.26.)

[9] L.M. Han, "Smart Virtual Fencing, Geo-Fencing", *ilobge*, 2022. https://iropke.com/archive/geo-fencing.html (Date accessed: 2022.10.26.)

[10] S.P. Hong, T.Y. Kim, "Design of Geo-fence-based Smart Attendance System", *The Journal of theInstitute of Internet*, Broadcasting and Communication, Vol 13, No. 6, pp. 496-502, 2020. https://doi.org/10.17661/jkiiect.2020.13.6.496

[11] Y.H. Eom, Y.K. Choi, S.K. Cho, B.K. Jeon, "A Mechanism to identify Indoor or Outdoor Location for Three Dimensional Geofence", *The Journal of the Institute of Internet, Broadcasting and Communication*, Vol 16, No. 1, pp. 169-175, 2016. https://doi.org/10.7236/JIIBC.2016.16.1.169

[12] Developers, "Create and monitor geofences", 2022. https://developer.android.com/training/location/geofencing (Date accessed: 2022.10.26.)

[13] T. Nelson, "What is Geo-Fencing?", *eYewated*, https://ko.eyewated.com/%EC%A7%80%EC%98%A4-%ED%8E%9C%EC%8B%B1%EC%9D%B4%EB%9E%80-%EB%AC%B4%EC%97%87%EC%9E%85%EB%8B%88%EA%B9%8C/ (Date accessed: 2022.10.26.)

[14] M. Basich, "Trax from Zetx: Visual Analysis", *Police*, 2022. https://www.policemag.com/341174/trax-from-zetx-visual-analysis (Date accessed: 2022.10.26.)

[15] S. Murphy, "Malls Send Geo-fencing Texts to Lure Shoppers to Stores", *Mashable*, https://mashable.com/archive/geofencing-texts-shoppers (Date accessed: 2022.10.26.)

[16] H.W. Kim, "Geofencing", *Digital Today*, http://www.digitaltoday.co.kr/news/articleView.html?idxno=258597 (Date accessed: 2022.10.26.)

[17] J. Wisem, "11 BEST GEOFENCING APPS IN 2022 FOR ANDROID & IPHONE (FREE & PAID)", *Earthweb*, https://earthweb.com/geofencing-apps/ (Date accessed: 2022.10.26.)

[18] S.M. Lee, H.C. Kwon, H.T. Kim, D.H. Bong, B.W. Oh, "Time and Space Notification Service Using Geofence", *Proceedings of KIIT Conference*, pp. 315-319, 2020. https://ca.skku.edu:8443/link.n2s?url=https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10490814 (Date accessed: 2023.3.31.)

[19] M. Rathi, "Rethinking Reverse Location Search Warrants," *Journal of Criminal Law and Criminology*, Vol 111, No. 3, pp. 805-837, 2021. https://scholarlycommons.law.northwestern.edu/jclc/vol111/iss3/5 (Date accessed: 2023.3.31.)

[20] C. Zietlow, "Reverse Location Search Warrants: Law Enforcements' Transition to 'Big Brother,'", *North Carolina Journal of Law & Technology*, Vol 23, No. 3, pp. 669-700, 2022. https://heinonline.org/HOL/LandingPage?handle=hein.journals/ncjl23&div=23&id=&page= (Date accessed: 2023.3.31.)

[21] Note, Geofence Warrants and the 4th Amendment, *Harvard Law Review*, pp. 2508-2529, 2021. https://harvardlawreview.org/2021/05/geofence-warrants-and-the-fourth-amendment/ (Date accessed: 2023.3.31.)

[22] Brinegar v. United States, 165 F.2d 512 (10th Cir. 1948)

[23] Carpenter v. United States, 138 S.Ct. 2206, 2018.

[24] United States v. Jones, 565 U.S. 400, 132 S. Ct. 945, 2012.

[25] NY State Senate Bill S296A, NY State Senate, https://www.nysenate.gov/legislation/bills/2021/S296 (Date accessed: 2022.10.26.)

[26] Geolocation Privacy Legislation, GPS.gov: Geolocation Privacy Legislation, https://www.gps.gov/policy/legislation/gps-act/ (Date accessed: 2022.10.26.)

[27] United States v. Santana, 427 U.S. 38, 96 S.Ct. 2406, 1976.

[28] Brigham City v. Stuart, 547 U.S. 398, 126 S. Ct. 1943, 2006.

[29] C.S. Fishman, "Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements", *The Catholic University of America*, pp. 995-1040, 2013. https://scholarship.law.edu/cgi/viewcontent.cgi?article=1137&context=scholar (Date accessed: 2023.3.31.)

[30] POLICE ACT https://elaw.klri.re.kr/kor_service/lawView.do?hseq=48536&lang=ENG (Date accessed: 2023.6.17.)

[31] Act On The Performance Of Duties By Police Officers https://elaw.klri.re.kr/kor_service/lawView.do?hseq=55666&lang=ENG (Date accessed: 2023.6.17.)

[32] Act on the Protection and Use of Location Information, 2023. https://elaw.klri.re.kr/kor_service/lawView.do?hseq=55914&lang=ENG (Date accessed: 2023.6.17.)

[33] Infectious Disease Control and Prevention Act, 2023. https://elaw.klri.re.kr/kor_service/lawView.do?hseq=60930&lang=ENG Date accessed: 2023.6.17.)

[34] https://gdpr-info.eu/art-6-gdpr/ (Date accessed: 2023.6.17.)

[35] https://www.unco.edu/hipaa/protected-health-information/national-priority.aspx (Date accessed: 2023.6.17.)

[36] Criminal Procedure Act https://elaw.klri.re.kr/kor_service/lawView.do?hseq=60539&lang=ENG (Date accessed: 2023.6.14.)

[37] Act On Real Name Financial Transactions And Confidentiality, 2023.

https://elaw.klri.re.kr/kor_service/lawView.do?hseq=54706&lang=ENG (Date accessed: 2023.6.14.)

[38] A. Mak, "How Police Departments Try to Force Google to Hand Over Data on Anyone Near a Crime Scene", Slate Magazine, 2022. https://slate.com/technology/2019/02/reverse-location-search-warrants-google-police.html (Date accessed: 2022.10.26.)

◐ 저 자 소 개 ◑

배 초 희 (Chohee Bae)
2018년 울산대학교 법학과 및 회계학과(법학사 및 경영학사)
2020년~현재 성균관대학교 일반대학원 법학과 석박사통합과정
관심분야 : 가상자산, 압수수색, 형사법, 디지털증거법 등
E-mail: chohee1506@skku.edu

이 지 우 (Jiwoo Lee)
2016년 UC Berkeley, Legal Studies and Sociology(문학사)
2020년 성균관대학교 일반대학원 법학과(법학석사)
2022년~현재 성균관대학교 일반대학원 법학과 박사과정
관심분야 : 형법, 형사소송법, 증거법, 미국법, 비교법 등
Email : jiwoo0714@naver.com

이 경 열 (Kyung-Lyul Lee)
1998년 성균관대학교 법학과(법학사)
1991년 성균관대학교 일반대학원 법학과(법학석사)
1994년 성균관대학교 일반대학원 법학과(법학박사)
2002년 독일 Koeln대학교 법학대학원(법학박사)
2003년~2014년 숙명여자대학교 법과대학 교수
2015년~현재 성균관대학교 법학전문대학원 교수
관심분야 : 형사법, 정보형법, 디지털증거법 등
E-mail: klee04@skku.edu