Self-Quarantine System and Personal Information Privacy in South Korea

Sun Goo Lee¹ and Eunsoo Kim²
¹Underwood International College, Yonsei University, Seoul; ²Seoul National University Law Research Institute, Seoul National University, Seoul, Korea.

The purpose of this study is to present a legal system in which information is actively collected and utilized to monitor the location and health of self-quarantined persons through IT, to identify loopholes in the law and regulatory system in view of data protection and utilization, and to propose a legislative solution for those loopholes. In Korea, the Infectious Disease Control and Prevention Act (“the Prevention Act”) regulates all matters related to the prevention and management of infectious diseases, including the use of information on self-quarantine apps. Article 42(2) of the Prevention Act states that local governments are authorized to collect the location and health information of a quarantined citizen; however, the law does not elaborate on how this information can be used and what other information can be used in combination with the collected information. Thus, the Personal Information Protection Act (“the Protection Act”), as a general privacy law, is applied supplementarily. However, since the Protection Act is very general and does not have accumulated cases, there is uncertainty about how governments can utilize the collected information. Therefore, it is necessary to consider a legislative solution that includes a direct and clear basis for the use of personal information collected under the Prevention Act in consideration of Korean privacy regulations.

Key Words: COVID-19, quarantine, information technology, jurisprudence, South Korea

INTRODUCTION

Nearly 2 years have passed since COVID-19 was first reported in January 2020 in South Korea. Since then, there has been a growing body of research on the virus, as well as many changes, such as free vaccinations for all people aged 18 years or older. Nonetheless, the influence of COVID-19 continues due to breakthrough infections among the vaccinated and the emergence of variant viruses. With increasing social and economic fatigue from intensive social distancing, the Korean government has moved forward with the “Living with COVID-19” policy as of November 1, 2021. However, it remains to be seen whether it will be possible to return to pre-pandemic daily life until COVID-19 treatments are commercialized. Therefore, there is an increasing need to establish a health care system capable of managing coronavirus from a long-term perspective.

Currently, Korea’s infectious disease prevention system is largely based on personal hygiene practices, such as mask-wearing, vaccination, and preventive self-quarantine. Korean citizens have shown a high level of compliance with mask-wearing; in a national observation survey, 97.9% of citizens were found to wear masks when they leave home, and 92.3% were found to properly wear masks that cover both mouth and nose.¹ In regards to vaccination, even though it has been implemented successfully, with the vaccination rate reaching 84% as of December 15, 2021,² it reportedly has had a limited effect on preventing severely ill patients.³ In this context, this study focuses on finding a way to better implement the self-quarantine system.

As the number of individuals self-quarantining swelled, arguments were raised over the limits of traditional face-to-face management of the quarantined, that is, the monitoring of the quarantined using human resources of public health authorities.⁴ This study discusses a non-face-to-face management sys-
tum that utilizes IT devices, such as mobile phones or wearable devices with self-quarantine management apps. Currently, the Ministry of Interior and Safety of Korea, which is in charge of disaster management, is in charge of self-quarantine management with local governments, and the Ministry requires those self-quarantining to install the “self-quarantine safety protection” app on their mobile phones. The app has three key features: the first is to register the location of individuals in self-quarantine and track their movement so that a notification rings when they leave their designated area. The second is a function that allows those in self-quarantine to assess their “body temperature,” “cough,” “sore throat,” and “difficulty breathing (shortness of breath)” on their own and enter them into the app to share the data with local government officials. The third is a function that provides guidance on rules of living for those in self-quarantine. However, since the purpose of the app when initially introduced was to facilitate location tracking to prevent those in self-quarantine from leaving their quarantined area, the health management functions beyond that original function may be quite insufficient. This is because those in self-quarantine must enter the information themselves. As such, there may be cases where they have difficulty entering information on their own or may not be able to enter it accurately, and even if they do enter it correctly, the items they enter are limited. Therefore, their app is insufficient to monitor the health status of those in self-quarantine. In addition, our newly proposed system enables round-the-clock monitoring of quarantined people so that public health authorities can detect acute symptoms early and deploy timely intervention. This attribute could prevent the worsening of illness or even deaths that occur during self-quarantine.

According to a recent survey by Yonsei University of 300 people with experience in self-quarantine (unpublished data), self-quarantine may lead to mental and physical health problems. The survey was conducted from November 1, 2020, to August 31, 2021. It was approved by Severance Hospital, Yonsei University Health System (IRB Number: 4-2020-0025). The researchers recruited participants by distributing posters at the hospital, announcement boards in city halls across the country, and a residential treatment center. The included participants were over 19 years old and underwent self-quarantine. Some were confirmed with infection, and others were not. Participation was voluntary, and the online survey required approximately 30 minutes to complete. Survey participants were compensated by Starbucks gift cards worth USD 4. According to the survey results, those in self-quarantine reported experiencing considerable anxiety and nervousness during quarantine, and all but 23.4% answered that, “They are worried about their health conditions/whether they are infected.” This is in line with the fact that 58.6% of the respondents said that they thought “the prognosis of COVID-19 was very serious or that it was a serious disease.” Of the respondents, 84.8% expressed their intention to wear smart devices to manage self-quarantine. When asked why they could wear the devices (multiple choice question), the great majority answered that they expect the devices to help health care of the quarantined during quarantine (60%) and monitoring of health or the infected (57%). In addition, 84.8% of the respondents agreed to receive telemedicine from medical personnel based on the information collected through this system.

However, it should be noted that there are as many concerns about such health management systems as there is demand. First, respondents against wearing devices pointed out the possibility of invasion of privacy due to the sharing of location information and health information (27%), the possibility of personal information leakage due to poor information management (22.5%), and the possibility of the government monitoring individuals based on collected information (17.6%). In order for health management to be performed through wearable devices or sensors, considerable health-related information must be collected and shared with local government officials from time to time. Therefore, it is necessary to reorganize legislation so that ICT-based management systems can efficiently manage health while protecting the health-related information of those in quarantine. This raises several questions: What regulations are being prepared by the current legal system for an ICT-based self-quarantine management system? What can local governments do with health information, and how much power do those in quarantine have to make decisions about the use of such information? Can the information collected by local governments be shared with top organizations, such as the Korea Disease Control and Prevention Agency? What about other local governments?

The purpose of this study is to present a legal system in which information is actively collected and utilized to monitor the location and health of self-quarantining persons through mobile phones or wearable devices, but with such information being protected. To this end, this study will examine the information necessary in an ICT-based self-quarantine management app (Section II) and the contents of the current law applied to the collection and management this information (Section III). After that, problems that could arise under the current legislation will be analyzed (Section IV). Finally, the discussion will be concluded by proposing the contents of the legal system that must be improved in order to introduce a successful management system (Section V).

THE COLLECTION OF INFORMATION ON SELF-QUARANTINE APPS

The information collected from the ICT-based self-quarantine health management system would be identification information, such as the quarantining person’s name, quarantine location (address), date of birth, and gender, as well as health-related information, such as blood pressure, body temperature,
pulse, sleeping pattern, and physical activity. In addition, information on the individual’s location should be collected to notify when the person leaves the designated location. There are three methods of collecting and using health information on those in self-quarantine: first, central agencies, such as the Korea Disease Control and Prevention Agency, can collect information and transfer it to local governments to which the self-quarantining person belongs. Second, local governments can collect information from those in their jurisdiction and share it with higher institutions if necessary. Third, local governments and central agencies can each collect information. The Infectious Disease Control and Prevention Act (the “Infectious Disease Prevention Act”) stipulates the third method.

Currently, the Infectious Disease Prevention Act covers all matters related to the prevention and management of infectious diseases in Korea. The Infectious Disease Prevention Act took effect on December 30, 2018, pointing out that the contents of the Contagious Disease Prevention Act enacted in 1957 alone had limitations in preventing and managing infectious diseases. In order to efficiently prevent and manage infectious diseases, the Parasitic Disease Prevention Act and the Contagious Disease Prevention Act were combined and renamed the Infectious Disease Control and Prevention Act, and the term “contagious diseases” was reorganized into “infectious diseases” to include diseases that do not spread among people. The Act was established with the aim of efficiently responding to new infectious diseases and bio-terrorist infectious diseases by allowing preventive and therapeutic drugs and equipment to be stocked in advance or contracted for purchase if there are concerns about a pandemic.

Article 42-2 of the Infectious Disease Prevention Act stipulates that the head of the Korea Disease Control and Prevention Agency and the mayors of the city, county, and district (local governments) can all check the presence or absence of infectious disease symptoms and collect location information using wired and wireless communication technology, as shown in Table 1.

The Infectious Disease Prevention Act gave both the central agency and relevant local governments the authority to collect information because Korea’s self-quarantine management is thoroughly carried out at the local government level. Under the Infectious Disease Prevention Act, the local government level (or jointly by local governments and the Korea Disease Control and Prevention Agency) set and operate all matters concerning self-quarantine, infectious disease monitoring and epidemiological investigations, vaccinations, disclosure of information during pandemics, quarantine facility designation, storage of medical and quarantine items in preparation for infectious diseases, quarantine measures against infectious disease outbreaks, such as self-quarantine or facility quarantine, closure, and movement restrictions, preventative measures, such as restrictions against gatherings or listing of visitors, wearing of masks, etc., and disinfection-related matters. Therefore, the self-quarantine management app is designed to establish an interface between the self-quarantining person and the public health centers housed under each local government. Accordingly, it is possible to make it mandatory to install and subscribe to apps for self-quarantine health management at the local government level regardless of the consent of the app subscribers.

Through the app, local governments can collect information on the quarantined citizen’s location and symptoms of infectious diseases. The Act, however, does not define the use of non-health-related personal identification information (name, quarantine address, etc.) at the local government level. Personal identification information is presumed to be collected during epidemiological investigations of infected people, but specifically, there are no stipulations regarding the use and disposal of information on self-quarantining persons, that is, information on close contacts, etc. Matters that are not precisely defined are ultimately supplemented by the Personal Information Protection Act, which generally regulates domestic privacy (Personal Information Protection Act, art. 6).

### Table 1. Article 42-2 of the Infectious Disease Prevention Act

| Article 42 (Compulsory Dispositions with respect to Infectious Diseases) (2) Where any Class 1 infectious disease breaks out, the Commissioner of the Korea Disease Control and Prevention Agency, a Mayor/Do Governor, or the head of a Si/Gun/Gu may have the relevant public official take any of the following measures for persons suspected of contracting the infectious disease. In such cases, the relevant public official may conduct a necessary investigation or medical diagnosis to confirm the presence or absence of infectious disease symptoms: |
|---|
| 1. Quarantine at home or in a facility; |
| 2. Checking the presence or absence of symptoms of an infectious disease based on wired or wireless communications, or using devices based on the information and communications technology, etc. |
| 3. Testing of infection |

### LEGAL CONSIDERATIONS FROM THE PRIVACY PERSPECTIVE AND ISSUES WITH THE CURRENT REGULATORY SYSTEM

In Korea, the Personal Information Protection Act is generally applied to personal information. Since it is a general law in the privacy regulation system, provisions on personal information sporadically stipulated by other laws have the status of sectoral laws according to Article 6 of the Personal Information Protection Act. In other words, Article 6 of the Personal Information Protection Act can be interpreted as having a structure in which the Infectious Disease Prevention Act applies first as
the legal basis for processing personal information in self-quarantine apps, with the areas not regulated by the Infectious Disease Prevention Act being supplemented by the Personal Information Protection Act.

Legal issues related to information collection

**Does the collected information fall under the concept of "personal information" as the subject of regulation?**

The ICT-based self-quarantine management system largely requires three types of information: first, location information; second, personal identification information; and third, health-related information. First, the information collected based on Article 42 of the Infectious Disease Prevention Act is stipulated as “location information,” and matters concerning the protection, use, storage, etc. of location information are subject to the Act on the Protection and Use of Location Information [Infectious Disease Prevention Act, art.42(1)]. Therefore, it can be interpreted that the concept of location information stipulated by the Act on the Protection and Use of Location Information also applies to Article 42 of the Infectious Disease Prevention Act (Table 2).

As the Infectious Disease Prevention Act does not have any applicable regulations or its own definition regulations for information besides location information, the Personal Information Protection Act is applied supplementarily to the second and the third type of information being collected by self-quarantine apps. The Personal Information Protection Act presents “information on living individuals” as a common requirement for personal information [Personal Information Protection Act, art. 2(1)a].

To specify this further, personal information must be 1) information, 2) regarding an individual, 3) who is currently alive. Based on these common requirements, personal information can be divided into three categories: personal identification information, identifiable information, and pseudonymous information. Personal identification information is information that identifies an individual through their name, resident registration number, video footage, etc. and is evaluated as personal information in itself [Personal Information Protection Act, art. 2(1)a]. Identifiable information is defined as “information that may be easily combined with other information to identify a particular individual” [Personal Information Protection Act, art. 1(b)]. Pseudonymous information is “personal identification information or identifiable information that is pseudonymized so that the information cannot identify a particular individual without additional information by deleting in part, or replacing in whole or in part, such information [Personal Information Protection Act, art. 2(1-2)] that makes one incapable of identifying a particular individual without the use or combination of additional information for restoration to the original state” [Personal Information Protection Act, art. 2(1)c]. Through the attribute classification of information, the expressions “indirect identifier,” “attribute value,” and “quasi-identifier” are also used in contrast to “direct identifiers” such as the unique identification information described above.9

Here, “other information” corresponds to all information that is easily combined with identifiable information so that individuals can be identified.10 A typical example is a well-known fact generally used in society or background knowledge obtained by the personal information controller through other channels. The criterion for determining whether such information falls under personal identifiable information under the Personal Information Protection Act is that the information is “easy to combine with other information,” that is, easiness of combination [Personal Information Protection Act, art. 2(1)a]. As a specific factor for determining the ease of combination, the Personal Information Protection Act stipulates that “whether or not there is easiness of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured” [Personal Information Protection Act, art. 2(1)b].

Although there is no Supreme Court decision explicitly presenting the above criteria for easiness of combination, lower court rulings that explain this criterion are as follows.

>“Even if other information can be objectively combined to identify specific information, if there are circumstances in which it is difficult for a personal information controller to obtain other information to combine with the information in his or her possession through a reasonable method, it cannot be considered as personal information as the ‘easiness of combination’ criterion has not been fulfilled” (Seoul Central District Court Decision, 2015Gohap665, dated Feb. 14, 2020).

>“The question of which information can be easily combined with other information should not be determined...”

**Table 2. Article 2 of the Act on the Protection and Use of Location Information**

| Article 2 (Definitions) The definitions of the terms used in this Act shall be as follows: |
|-----------------------------------------------|
| 1. The term “location information” means information about a place where a portable object or an individual exists or has existed at a certain time, which is collected using telecommunications equipment facilities or telecommunications line equipment and facilities prescribed in subparagraph 2 or 3 of Article 2 of the Telecommunications Business Act; |
| 2. The term “personal location information” means the location information regarding a particular person (including information readily combinable with other information to track the location of a particular person even though location information alone is not sufficient to identify the location of such person); |
simply based on the information provider, but by reasonably considering the content of the information, the relationship of the persons receiving and providing the information, the purpose and method of use of the information recipient, the degree of effort and cost needed to combine the information, the benefit to the other party from combining such information, etc.” (Suwon District Court Decision, 2017No7275, dated Apr. 12, 2018).

According to commentary on personal information protection laws, guidelines, and notices, whether information can be easily combined with other information depends, in addition to the possibility of acquisition, on the combination not being unreasonably excessive in terms of time, cost, or effort in consideration of the current technology level or sufficiently predictable technological advances. For example, if the combination requires a computer that is so expensive to the point it is difficult for a business operator to purchase, one must conclude there is no “easiness of combination.” Location information and health information, which are the main target information collected by self-quarantine apps, are not direct identifiers, but because they can be viewed as information that can identify individuals through combination with other information held by the information controller, there is a high possibility they would be included under the scope of personal identifiable information.

As mentioned above, the self-quarantine app can collect identification information such as the name, address, date of birth, and gender of the quarantining person, as well as health-related information, such as the blood pressure and body temperature of the person to be managed. Unique identification information, such as name and address, and identifiable information, such as date of birth and gender, are subject to the Personal Information Protection Act as personal information under the Act. The health-related information, such as blood pressure and body temperature themselves, are less likely to identify individuals, compared to the unique identification information and identifiable information, since they are time-varying, but it is reasonable to assume they would be subject to the Personal Information Protection Act if they could be used to identify individuals by combining them with other information in a particular data environment.11

Is prior consent necessary as a legal basis for collection?

As mentioned above, Article 42(2) of the Infectious Disease Prevention Act provides the basis for local governments to collect a large portion of personal information without the consent of the subject of the information pursuant to Article 15(1)(2) of the Personal Information Protection Act. This is information to check “the presence or absence of symptoms of an infectious disease.” Therefore, what is the scope of information that can confirm the presence or absence of symptoms of an infectious disease? Common sense is that health-related information is naturally included. However, it is unclear whether unique identification information or identifiable information is included here and to what extent such information is allowed. If it does not fall within the scope prescribed by Article 42(2) of the Infectious Disease Prevention Act, the Personal Information Protection Act applies, and the requirements for information collection prescribed by this Act must be met.

The Personal Information Protection Act provides six general legal grounds for personal information collection, and even if the collection of unique or personal identifiable information does not fall under “special provisions that exist in other laws,” such as the “confirmation of symptoms of infectious diseases,” there is leeway for the collection to fall under “cases where it is inevitable to observe legal obligations” or “cases where it is inevitable for a public institution’s performance of its duties under its jurisdiction as prescribed by statutes, etc.” [Personal Information Protection Act, art. 15(1)]. This is because names, addresses, etc. are indispensable information to check whether or not the self-quarantining person has left the designated location. If this is the case, local governments may collect this information without the consent of the self-quarantining person. However, if this interpretation is not applied in the absence of precedent for Subparagraphs 2 and 3 of Article 15(1) of the Personal Information Protection Act or if only a small portion of information excluding information, such as name, gender, age, etc., is subject to Subparagraph 2 or 3, the criterion in Subparagraph 1 is applied to the rest of the information (name, date of birth, gender, etc.), so the consent of the data subject, that is, the self-quarantining person, must be obtained to collect information [Personal Information Protection Act, art. 15(1)], as described in Table 3. Whether the personal information collected is based on the consent of the self-quarantining person or based on the special provisions of the Infectious Disease Prevention Act, the “minimum collection principle” stipulated in the Act applies, as shown in Table 4 [Personal Information Protection Act, art. 3(1), 16].

The principle of restricting the collection of personal information applies to all six legal requirements collected by the Personal Information Protection Act (Personal Information Protection Act, art. 16). In particular, the commentary on personal information protection laws, guidelines, and notices explain that the OECD Privacy Principles, which are delineated in Table 5, influenced Article 3 of the Korean Personal Information Protection Act, which stipulates the eight principles of personal information protection. However, the Personal Information Protection Commission’s interpretation is that if the legal basis for collecting personal information is the consent of the data subject, the relaxed application of the minimum collection principle is possible if the requirements for consent such as autonomy are met. Therefore, it can be interpreted that the collection of location information or information to confirm the presence or absence of infection based on the Infectious Disease Prevention Act should be minimal with-
in the scope of purpose, and if additional information is collected based on individual consent, information collection within a somewhat wider scope is possible in accordance with the details of the consent.

Legal basis and method for information use

Use within the purpose of collection

In principle, someone who collects personal information may use the information without separate consent or requirements if usage is within the scope of the original purpose of collection [Personal Information Protection Act, art. 15(1)]. Article 42 of the Infectious Disease Prevention Act defines the permitted purpose of “collection,” but there are no provisions on how to use such information after collection, so the provisions in the Personal Information Protection Act apply. Article 15(1) of the Personal Information Protection Act stipulates that if the information is used within the original purpose of collection,

| Table 3. Article 15(1) of the Personal Information Protection Act |
|---------------------------------------------------------------|
| Article 15 (Collection and Use of Personal Information) |
| (1) A personal information controller may collect personal information in any of the following circumstances, and use it within the scope of the purpose of collection: |
| 1. Where consent is obtained from a data subject; |
| 2. Where special provisions exist in other laws or it is inevitable to observe legal obligations; |
| 3. Where it is inevitable for a public institution’s performance of its duties under its jurisdiction as prescribed by statutes, etc.; |
| 4. Where it is inevitably necessary to execute and perform a contract with a data subject; |
| 5. Where it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses, etc.; |
| 6. Where it is necessary to attain the justifiable interest of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the justifiable interest of the personal information controller and does not go beyond a reasonable scope. |

| Table 4. Article 3(1) and 16(1) of the Personal Information Protection Act |
|--------------------------------------------------------------------------|
| Article 3 (Principles for Protecting Personal Information) (1) The personal information controller shall specify explicitly the purposes for which personal information is processed, and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes. |
| Article 16 (Limitation to Collection of Personal Information) (1) A personal information controller shall collect the minimum personal information necessary to attain the purpose when collecting personal information pursuant to Article 15 (1). In such cases, the burden of proof that the minimum personal information is collected shall be borne by the personal information controller. |

| Table 5. Eight OECD Privacy Principles |
|---------------------------------------|
| 1. Collection limitation principle |
| There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. |
| 2. Data quality principle |
| Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. |
| 3. Purpose specification principle |
| The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. |
| 4. Use limitation principle |
| Personal data should not be disclosed, made available or otherwise used for purposes other than those specified… except: a) with the consent of the data subject; or b) by the authority of law. |
| 5. Security safeguards principle |
| Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. |
| 6. Openness principle |
| There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. |
| 7. Individual participation principle |
| An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended. |
| 8. Accountability principle |
| A data controller should be accountable for complying with measures which give effect to the principles stated above. |
collected personal information may be used without a separate legal basis or requirement. However, there is no clear interpretation of what the scope of the original purpose is under the Infectious Disease Prevention Act. For example, is sharing information with neighboring local governments for the health management of self-quarantining persons within the scope of the original purpose of data collection? Is linking other unique identification information or identifiable information with health-related information within the scope of purpose? Since answers to the questions are unclear, it is necessary to examine what legal requirements apply to the utilization of information outside the original scope of the purpose of collection.

Use outside the purpose of collection

Use based on the provisions of compatibility

Revisions to the Personal Information Protection Act in 2020 introduced provisions that allow the use of collected personal information under certain conditions beyond the purpose of collection. It is presumed that provisions similar to the EU General Data Protection Regulation (GDPR)’s compatibility provisions were also reflected in the Korean Personal Information Protection Act through the revision in 2020, as shown in Table 6 [Personal Information Protection Act, art. 15(3)].

According to the above provision, information can be used without the consent of the data subject even if the use is outside the scope of the purpose of collection if it is reasonably related to the purpose and if various safety measures have been applied for privacy protection. As specific considerations for use under Article 15(3) of the Personal Information Protection Act, the Enforcement Decree of the Personal Information Protection Act presents as requirements 1) whether it is related to the original purpose of collection, 2) whether it is possible to estimate the additional use or provision of personal information in light of the circumstances in which the personal information is collected or the processing procedures, 3) whether the data subject’s interests are unfairly infringed, and 4) whether the necessary safety measures, such as pseudonymization or encryption, are taken [Enforcement Decree of the Personal Information Protection Act, art. 14-2(1)]. Since this provision includes safety measures like encryption as a consideration, it can be thought that information processing such as encryption is no different from pseudonymization.13 However, there is a difference between the two in that the restrictive provisions of pseudonymization stipulated in the Personal Information Protection Act do not apply to the use of information under this provision.

According to Article 15(3), conceptually, personal information collected by this system for the purpose of preventing infectious diseases can be used within a reasonable scope and the purpose of collection of preventing infectious diseases. However, there is an uncertain aspect to using this provision as the basis for information use because there are no clear standards or precedents yet for reasonably related interpretations. A separate legal basis is required for use outside the purpose of collection that does not meet the consistency requirements. In principle, as described in Table 7, the Personal Information Protection Act requires a separate legal basis for use outside the purpose of collection [Personal Information Protection Act, art. 18(2)], and for the use of information from the self-quarantine app for which there are no separate regulations, the consent of the self-quarantining person will be required.

Use by pseudonymization

If it is unclear whether the information to be used is clearly within the scope of the collection purpose, there is the method of obtaining the consent of the self-quarantining person as described above, but there is also the method of using the information upon pseudonymization.14 Under the Personal Information Protection Act, pseudonymization means processing information so that it “becomes incapable of identifying a

Table 6. Article 15(3) of the Personal Information Protection Act

| Article 15 (Collection and Use of Personal Information) | — (3) A personal information controller may use personal information without the consent of a data subject within the scope reasonably related to the initial purpose of the collection as prescribed by Presidential Decree, in consideration whether disadvantages have been caused to the data subject and whether necessary measures have been taken to secure such as encryption, etc. |

Table 7. Article 18(2) of the Personal Information Protection Act

| Article 18 (Limitation to Out-of-Purpose Use and Provision of Personal Information) | (1) A personal information controller shall not use personal information beyond the scope provided for in Articles 15(1) and 39-3(1) and (2), or provide it to any third party beyond the scope provided for in Article 17(1) and (3) (2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, a personal information controller may use personal information or provide it to a third party for other purposes, unless doing so is likely to unfairly infringe on the interest of a data subject or third party: Provided, That information and communications service providers (as set forth in Article 2(1) 3 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply) processing the personal information of users (as set forth in Article 2(1) 4 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply) are only subject to subparagraphs 1 and 2, and subparagraphs 5 through 9 are applicable only to public institutions: 1. Where additional consent is obtained from the data subject; 2. Where special provisions exist in other laws; ... |

https://doi.org/10.3349/ymj.2022.63.9.806
particular individual without the use or combination of additional information for restoration to the original state by deleting in part, or replacing in whole or in part, such information" [Personal Information Protection Act, art. 2(1)2]. This Act specifically presents the procedure and level of pseudonymization. Pseudonymization must apply "a procedure such as deleting in part, or replacing in whole or in part, personal information," and this must be done to the degree that the information "becomes incapable of identifying a particular individual without the use or combination of additional information for restoration to the original state" to constitute pseudonymization under law [Personal Information Protection Act, art. 2(1)2].

The basic procedure of pseudonymization is to delete or replace personal identification information, such as information that can identify a specific data subject, including name, address, email address, and mobile phone number. For example, if there is no need to use the address variable of the information set for the purpose of information use, such information can be deleted, but in some cases, a method of replacing it with other random numbers may be required. This includes the case of continuously updating information or the case of connecting information in multiple databases.

As shown in the pseudonymization example above (Fig. 1), the method of converting the “unique passenger number” to a “hashed number” constitutes pseudonymization. In order to further lower the risk of identification that the unique passenger number itself can reveal, it is replaced with information that minimizes the risk of identification through statistical processing such as the application of a hash function. Only items that distinguish individual records from other records have been replaced with other information, and the distortion of information is very low because the values of information, such as the “place of origin,” “final destination,” and “stopover,” are the same. After applying this pseudonymization method, only when the information “becomes incapable of identifying a particular individual without the use or combination of additional information for restoration to the original state” can it be determined that pseudonymization under the Personal Information Protection Act has occurred.

However, since the concept of “additional information” is not separately defined in the wording of the Act, it is difficult to interpret in detail only based on the Act. The Personal Information Protection Commission’s legal commentary presents the concept of additional information, explaining that additional information is information that can restore pseudonymized information, and is limited to the information created and used during the process of pseudonymization. In this respect, the original information itself may correspond to additional information. If the person who received the pseudonymized information can access the original information depending on the situation, the pseudonymized information can be restored to its original state, so the original constitutes additional information. In addition, information used for pseudonymization, such as encryption keys and mapping tables used in the encryption process, may be included as “additional information.” This is because, if there is such information, the original values can be restored from the pseudonymous values.

Therefore, in order for pseudonymization to meet legal standards, it is necessary to design a storage system for such additional information so that users of pseudonymous information cannot access such additional information. The Personal Information Protection Act requires that additional information is not disclosed to third parties, stipulating that additional information be divided and stored separately and that access rights are also divided [Personal Information Protection Act, art. 28-2(2), 28-4(1)].

As a criterion for pseudonymization, the Personal Information Protection Act presents the possibility of (re)identification of individuals (Personal Information Protection Act, art. 28-4). In the same context as the judgment of anonymous information through de-identification, it is inevitable that the judgment of the possibility of identification in terms of pseudonymization must be made on a case-by-case basis by comprehensively considering the purpose of pseudonymization, the information to be pseudonymized, the environment of the person using the pseudonymous data, and the risks that may arise during re-identification. When providing pseudonymous data to a third party, it is necessary to consider what other information the third party has and whether sufficient personal information protection measures are being taken. In analyzing the risk of pseudonymous data, the “Pseudonymous Data Processing Guidelines” (2020) explain that “it should be judged by considering the environment in which it is processed (provided), the size of the information (record, size of items), specificity (level of information accuracy), etc.”

Regarding pseudonymization methods for healthcare information, the Personal Information Protection Commission and the Ministry of Health and Welfare jointly announced the Guidelines for the Use of Health and Medical Information in 2020. These guidelines provide specific pseudonymization guidelines for each attribute of information for 12 types of attribute values. Among the 12 types of attribute values, measurement information, medical observation and input information,
algorithm-produced health information, the presence or absence of gene mutations or mutation types of widely known diseases, new mutation information of neoplasms from which germ cell mutation information has been removed, omics information excluding genomes, race and ethnicity information, and nationality information generally do not need separate pseudonymization procedures. The guidelines explain that, in principle, no separate action is required because the possibility of personal identification using the above attribute values is low. For example, measurement information, such as blood pressure, blood sugar, oxygen saturation, blood concentration of various substances, and heart rate, step count, and electrocardiogram values measured by wearables may have different values at each time of measurement, so personal identification is low. Therefore, when these guidelines are applied, the chances are low of biometric information, such as blood pressure and body temperature of the quarantining person, collected in this system needing separate pseudonymization. On the other hand, there is a significant need for the pseudonymization of information, such as name, mobile phone number, and address. The Personal Information Protection Act lists “statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc.” as purposes for processing pseudonymous data [Personal Information Protection Act, art. 28-2(1)]. If so, does self-quarantine tracking or health care also meet the purpose requirements of pseudonymization? While there is leeway for statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc., to satisfy the requirement for their public interest characteristics, there are some uncertain points remaining as there is no precedent specifying the requirements.

Issues with the current regulatory system and legislative proposals
Under the current legal system, the collection and use of personal information through self-quarantine apps are applied in a dual manner, with the Infectious Disease Prevention Act and the Location Information Act and Personal Information Protection Act. In the case of location information, it may be collected without the consent of the self-quarantining person who is the data subject based on the provisions of Article 42(2) of the Infectious Disease Prevention Act and used within the purpose of collection without separate consent. For personal information other than location information, it must be collected in accordance with Article 42(2) of the Infectious Disease Prevention Act, or the other information must meet the requirements of Article 15(1) of the Personal Information Protection Act. For information collected in this way, it may be used within the scope of purpose without the consent of the self-quarantining person, but otherwise, the consent of the self-quarantining person must be acquired. However, since the scope of application of the requirement “within the scope of the purpose of collection” is not clear, the possibility of use falling outside the purpose of collection should also be kept in mind. If personal information is to be used other than for the purpose of collection without separate consent regarding the use of the personal information itself, the use may be based on the provisions of compatibility or pseudonymization prescribed by the Personal Information Protection Act. Ultimately, it becomes a dual legal structure as shown in Table 8.

It is true that, if not stipulated by the Infectious Disease Prevention Act, there is a legal basis for the use of all forms of information because the Personal Information Protection Act is applied supplementarily as a general law (Personal Information Protection Act, art. 6). However, it is necessary to make legislative preparations to effectively respond to cases where there is a possibility that infectious diseases continue to bear unpredictable social costs for members of society, such as the COVID-19 pandemic. In particular, if the scale of the spread of infectious diseases is difficult to handle only with traditional management methods, there is an urgent need to establish a regulatory environment where methods utilizing IT devices, such as self-quarantine apps, can be actively used. Ultimately, through legislative preparations for the use of self-quarantine apps, the social and economic costs associated with infectious diseases can be reduced by using data collected through self-quarantine apps safely and effectively. With the current legal system in which the Personal Information Protection Act and the Infectious Disease Prevention Act are dualized, there is a problem of increasing institutional risks regarding the use of self-quarantine apps. First, because the boundary between use within the purpose of collection and use outside of the purpose of collection is uncertain, those who want to develop and apply self-quarantine apps face legal uncertainty about whether to use the Infectious Disease Prevention Act or the Personal Information Protection Act as a basis.

In the context of privacy regulations, the relationship between the Personal Information Protection Act as a general law and the Infectious Disease Prevention Act as an individual law in their application follows the principle of supplementarity, in which the general law applies supplementarily to the individual law and provides its own standards for the application of multiple regulations. However, high institutional risks under these un-
certainties are likely to eventually eliminate willingness to use self-quarantine apps, as there are additional legal interpretation issues, such as determining whether the provisions of the Infectious Disease Prevention Act, the individual law, are in the Personal Information Protection Act, the general law, and determining whether, if the two laws overlap, how to specifically organize the application of the two laws.

Therefore, regarding Korean privacy regulations, it is necessary to consider a legislative solution that includes a direct basis for the use of personal information collected in the provisions of the Infectious Disease Prevention Act. This is the method of referring to the requirements for the collection and utilization of personal information in the Personal Information Protection Act and, to the extent that it does not conflict with the Personal Information Protection Act, reflecting the provisions in the Infectious Disease Prevention Act. For example, by directly reflecting expressions such as “use” or “provision” in addition to the expression “collection” in Article 42(2) of the Infectious Disease Prevention Act, thereby giving it concrete content, the institutional risk of collecting and using personal information through self-quarantine apps can be lowered to some extent. Alternatively, there is the option of establishing a provision that does not require separate consent when using pseudonymized data for effective management of self-quarantine by reflecting the special provisions of pseudonymization stipulated in the Personal Information Protection Act analogically. By having the Infectious Disease Prevention Act directly introduce management methods that safely protect privacy, such as pseudonymization, the concerns of privacy infringement of data subjects being managed by self-quarantine apps can be lowered.

CONCLUSION

Because the basis of non-face-to-face self-quarantine management is personal information that is automatically collected from individuals through devices, there are concerns for a high risk of privacy infringement. There is also criticism that the current Infectious Disease Prevention Act violates individual rights to self-determination of personal information because personal information of the data subject can be collected without the consent of the data subject. However, in addition to cost perspectives, it cannot be concluded that methods of using a device for privacy protection are insufficient compared to traditional face-to-face management methods. With face-to-face methods, there is still a privacy risk that the epidemiological investigator will leak information intentionally or by negligence, as the methods ultimately involve an infectious disease-related entity, such as an epidemiological investigator directly collecting the individual’s personal information face-to-face. Whether the privacy risks of the face-to-face method and the privacy infringement risks of the non-face-to-face method are high or low are not uniformly determined.

In the end, the key is to find a legal and institutional solution that can effectively operate the self-quarantine app in terms of privacy protection no matter which method is established, that is, even if an ICT-based system is established. In terms of the collection and utilization of information through self-quarantine apps, the Personal Information Protection Act and the Infectious Disease Prevention Act are applied through a dual structure in Korea. The Personal Information Protection Act has the advantage of presenting consistent and predictable legal standards for privacy protection through the application of general law. However, in order to effectively respond to urgent situations, such as the management of health care, especially in the management of infectious diseases, there is a significant need to regulate institutional mechanisms for self-quarantine in a one-stop manner under the Infectious Disease Control Act, which better reflects the value of health care. Therefore, it is time to consider moving the current system, which separately applies the Personal Information Protection Act or the Infectious Disease Control Act depending on whether the use falls within or outside the purpose of collection, towards the direction of reflecting a direct basis for the use of personal information in the Infectious Disease Prevention Act.

ACKNOWLEDGEMENTS

This research was supported by a government-wide R&D fund project for infectious disease research (GFID), Republic of Korea (grant number: HG20CO003000021).

AUTHOR CONTRIBUTIONS

Conceptualization: Sun Goo Lee and Eunsoo Kim. Data curation: Sun Goo Lee. Formal analysis: Sun Goo Lee and Eunsoo Kim. Funding acquisition: Sun Goo Lee. Investigation: Sun Goo Lee and Eunsoo Kim. Methodology: Sun Goo Lee and Eunsoo Kim. Project administration: Sun Goo Lee. Resources: Sun Goo Lee and Eunsoo Kim. Supervision: Sun Goo Lee. Validation: Sun Goo Lee and Eunsoo Kim. Visualization: Sun Goo Lee and Eunsoo Kim. Writing—original draft: Sun Goo Lee and Eunsoo Kim. Writing—review & editing: Sun Goo Lee and Eunsoo Kim. Approval of final manuscript: all authors.

ORCID iDs

Sun Goo Lee https://orcid.org/0000-0003-3894-6224
Eunsoo Kim https://orcid.org/0000-0002-3523-4355

REFERENCES

1. KDCA. Press release: a large increase of awareness and practice of proper handwashing compared to the previous year [Internet] [accessed on 2022 March 28]. Available at: https://kdca.go.kr/board/board.es?mid=a20501010006&bId=0015&list_no=171240&cg_code=&act=view&nPage=81.
2. Our World in Data. Coronavirus (COVID-19) vaccinations [Internet] [accessed on 2022 March 28]. Available at: https://ourworldindata.org/covid-vaccinations.
3. WHO. Vaccine efficacy, effectiveness and protection [Internet] [accessed on 2022 March 28]. Available at: https://www.who.int/news-room/feature-stories/detail/vaccine-efficacy-effectiveness-and-protection.

4. Kim MS. MIT technology review. South Korea is watching quarantined citizens with a smartphone app [Internet] [accessed on 2022 March 28]. Available at: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/.

5. Ministry of the Interior and Safety. Card news: application on secured self-quarantine Q&A 7 [Internet] [accessed on 2022 March 28]. Available at: https://www.mois.go.kr/frt/bbs/type002/commonSelectBoardArticle.do?bbsId=BBMSTR_000000000205&nttId=76155.

6. European Commission. Guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection. [Internet] [accessed on 2022 March 28]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29.

7. Korean Law Information Center. Reasons for enactment or amendment, infectious disease prevention and control act. 2022. Available at: https://www.law.go.kr/LSW/lsRvsRsnListP.do?lsId=001792&chrClsCd=010202&lsRvsGubun=all.

8. Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. 2007. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp140_en.pdf.

9. Garfinkel SL. De-identification of personal information. Gaithersburg (MD): National Institute of Standard and Technology (NIST); 2015.

10. Personal Information Protection Commission (S. Kor.). Guidance on Personal Information Protection Act and Relevant Regulations. 2020. Available at: http://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=7023.

11. OECD. The OECD privacy framework. Paris: OECD Publishing; 2013.

12. Hintze M. Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency. Int Data Priv Law 2018;8:86-101.

13. Hintze M, El Emam K. Comparing the benefits of pseudonymisation and anonymisation under the GDPR. Journal of Data Protection & Privacy 2018;2:145-58.

14. Personal Information Protection Commission (S. Kor.). Pseudonymous Data Processing Guideline. 2020. Available at: https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=8900.

15. U.K. Information Commissioners’ Office (ICO). Anonymisation: managing data protection risk code of practice. Wilmslow: Information Commissioner’s Office; 2012.

16. Elliot M, Mackey E, O’Hara K. The anonymisation decision-making framework 2nd edition: European practitioners’ guide. Manchester: UK Anonymisation Network; 2020.

17. Arbuckle L, El Emam K. Building an anonymization pipeline: creating safe data. Sebastopol (CA): O’Reilly Media; 2020.

18. Li TC. Privacy in pandemic: law, technology, and public health in the COVID-19 crisis. Loy U Chi L J 2021;52:767-865.

19. Park S, Choi GJ, Ko H. Information technology–based tracing strategy in response to COVID-19 in South Korea—privacy controversies. JAMA 2020;323:2129-30.