Copyright ⓒ 2022 KSII

A Study on Personal Information Protection amid the COVID-19 Pandemic

Min Woo Kim[1], Il Hwan Kim[2], Jaehyoun Kim[3], Oh Jeong Ha[4], Jinsook Chang[5] and Sangdon Park[6*]

[1]Research Center, Korea Social Security Information Service
Health&Welfare Administration Complex B/D, 400 Neundong-ro, Gwangjin-gu, Seoul, Republic of Korea
[e-mail: mwkim@ssis.or.kr]
[2]Sungkyunkwan University Law School
25-2 Sungkyunkwan-ro, Jongno-gu, Seoul, Republic of Korea
[e-mail: ilhwan@skku.edu]
[3]Department of Computer Education, Sungkyunkwan University
25-2 Sungkyunkwan-ro, Jongno-gu, Seoul, Republic of Korea
[e-mail: jaekim@skku.edu]
[4]Sungkyunkwan University Law School
25-2 Sungkyunkwan-ro, Jongno-gu, Seoul (03063), Republic of Korea
[e-mail: odh0524@naver.com]
[5]Kyonggi University, Department of International Industrial&Information
154-42 Gwanggoysan-Ro, Yeongtong-Gu, Suwon-Si, Gyeoggi-Do(16227) Republic of Korea
[e-mail: librajinny@gmail.com]
[6]National Security Policy Research Section, National Security Research Institute
P.O. Box 1, Yuseong, Daejeon, Republic of Korea
[e-mail: sdpark@nsr.re.kr]
* Corresponding author: Sangdon Park

Received September 21, 2022; revised November 21, 2022; accepted November 30, 2022; published December 31, 2022

Abstract

COVID-19, a highly infectious disease, has affected the globe tremendously since its outbreak during late 2019 in Wuhan, China. In order to respond to the pandemic, governments around the world introduced a variety of public health measures including contact-tracing, a method to identify individuals who may have come into contact with a confirmed COVID-19 patient, which usually leads to quarantine of certain individuals. Like many other governments, the South Korean health authorities adopted public health measures using latest data technologies. Key data technology-based quarantine measures include:(1) Electronic Entry Log; (2) Self-check App; and (3) COVID-19 Wristband, and heavily relied on individual's personal information for contact-tracing and self-isolation. In fact, during the early stages of the pandemic, South Korea's strategy proved to be highly effective in containing the spread of coronavirus while other countries suffered significantly from the surge of COVID-19 patients. However, while the South Korean COVID-19 policy was hailed as a success, it must be noted that the government achieved this by collecting and processing a wide range of personal information. In collecting and processing personal information, the data minimum principle − one of the widely recognized common data principles between different data protection laws − should be applied. Public health measures

http://doi.org/10.3837/tiis.2022.12.016 **ISSN : 1976-7277**

have no exceptions, and it is even more crucial when government activities are involved. In this study, we provide an analysis of how the governments around the world reacted to the COVID-19 pandemic and evaluate whether the South Korean government's digital quarantine measures ensured the protection of its citizen's right to privacy.

Keywords: Privacy, Personal Information, COVID-19 pandemic, Data Minimization Principle

1. Introduction

Coronavirus disease ("COVID-19"), a highly infectious disease, has immensely affected the globe since its outbreak in December 2019. Although there is some disagreement about where the virus originated from, the World Health Organization (WHO) confirmed that the very first COVID-19 case was discovered in Wuhan, the capital of Hubei Province, China, which is one of the mega million Chinese cities. On January 13, 2020, the Thailand government reported the first case of COVID-19 outside of China, which clearly marked that the coronavirus (SARS-CoV-2) had begun to spread across borders. Within a week, on January 20, the South Korean government officially confirmed its first COVID-19 patient, a young female who had returned from traveling to Wuhan. In less than a month since the first confirmed case in Wuhan, a number of countries reported that the virus was spreading at unprecedented speed. In the face of a global health crisis, the WHO finally declared the COVID-19 as a pandemic on March 11, 2020. The COVID-19 mainly causes respiratory symptoms including fever, cough, and shortness of breath, but those with underlying conditions suffer from more severe symptoms as well as a risk of death. The virus has also quickly mutated, evolving through many variants. Currently, Omicron is the dominant variant, which is more readily transmittable but less lethal than prior variants. According to the data published by the Coronavirus Resource Center of Johns Hopkins University, as of March 30, 2022, the number of total casualties across the globe is over 6 million while the number of confirmed cases reached to over 480 million, Thus, it is clear that the COVID-19 will be remembered as one of the most severe tragedies of the 21st century.

As the number of COVID-19 continued to surge, more aggressive measures were introduced and carried out by the governments around the world. One was to shut down borders and to restrict free movement. This applied either within a nation between cities or between countries. Lockdown was usually the last resort against the widespread of COVID-19 because there was no specific treatment or vaccines available during the early phase of the pandemic.

While other governments adopted aggressive quarantine measures on their own, the South Korean government devised different tactics to combat the COVID-19, so called the "3T Policy" which stands for Testing, Tracing and Treating. Particularly, tracing a confirmed patient's location history became a critical component to prevent the spread of the virus within local communities. Given that the coronavirus is known to be transmitted from person to person by close contact, contact-tracing and subsequent quarantine of those contacted individuals were considered to be a reasonable and rational method to cut the chain of contagion. However, in order to do contact-tracing, a wide range of personal information

was collected and stored for the legal purpose of protecting the public health of Koreans. The types of personal information collected and processed by public health authorities include name, phone number, address, health status, CCTV footages, credit card transaction records, and history of COVID-19 vaccination once the vaccines became available. These data are types of "sensitive information" equivalent to the special categories of personal data under the EU General Data Protection Regulation (GDPR) adopted in April 2016.

Following the above discussion, this article starts by analyzing how countries around the world, including Korea, reacted to the unprecedented crisis especially from the perspective of protecting personal information. We then investigated the public perception of invasion of data privacy during the pandemic using public surveys carried out by the Korean government, public opinion research firms and the press. Despite the wide-ranging collection of personal information for COVID-19 public health measures, the surveys showed positive reactions to what the Korean government has done during the pandemic, which raises a concern regarding not only the right to privacy but also the emergence of surveillance state.

2. COVID-19 Public Health Measures of Selected Jurisdictions

As the COVID-19 transmits person to person via close contact, tracking how the COVID-19 spreads became one of the most important tasks as a part of cutting down the chain of massive transmissions. In order to do that, many governments attempted to deliver various measures for contact-tracing.

Some countries adopted to use one's personal information to do contact-tracing. For instance, the South Korean government took so called 3T policy which stands for Testing, Tracing and Treating. Following the 3T policy against the COVID-19, the government developed different digital measures, (1) Contact-tracing (2) the Self-check App, (3) the COVID-19 Electronic Wristband, and (4) Electronic Entry Log. All these highly advanced digital public health measures stood on the firm legal basis, (i) the Personal Information Act (ii) the Act on the Protection, Use, ETC. of Location Information, and (iii) the Infectious Disease Control and Prevention Act. Based on the legal basis, the public authority widely collected personal information. It includes name, mobile number, credit card transaction records, location information et cetera.

The Chinese government also counted on using personal information and developed an app called the Health Code. The app was designed to interplay with WeChat or Alipay, which are the most widely used apps among Chinese citizens. Those apps supported to monitor individuals' health status and the history of movement via scanning functions. In addition to that, surveillance camera footage and facial recognition technologies interplayed with the contact tracing app.

On the other hand, unlike South Korea or China's approach, the governments like the United States, Germany and Japan, developed and released apps, but they took a different pathway to fight the coronavirus with the bluetooth technology. For instance, two big tech companies, Google and Apple, jointly developed a privacy-friendly contact-tracing measure, the Privacy-Preserving Contract Tracing ("PPCT"), The PPCT, with bluetooth technology, does not collect one's personal information that can identify a specific natural person. It works with encryptions that when one came into proximity to another person who had the app, those random number codes would be exchanged. The Massachusetts Institute of

Technology along with private companies and academic institutions also developed a contact-tracing measure, the Private Automated Contact Tracing ("PACT"). The PACT works similar with the PPCT functions using the bluetooth technology. The Japanese government released an app called COCOA, which is designed for doing contact tracing. If an individual activated Bluetooth, the app would record those who were in one meter proximity for over 15 minutes. Once a person is confirmed as COVID-19-positive, the app notifies the app users and recommends taking the COVID-19 test to prevent transmission. It does not rely on GPS location services or collects one's name, gender, address, phone number. What it was processing information is only whether a person is infected or not. Germany decided to release an app for COVID-19 tracing, the Corona-Warn-App, developed jointly by SAP, a large German software company, and Deutsche Telekom, a major mobile carrier in Germany. While the federal government attempted to mandate the tracing app, the German government tried to amend the relevant laws to collect location information. However, after experiencing criticisms, it changed eventually to the bluetooth technology rather than using one's location information or mobile records. It works that when a person came into contact with another individual who had also installed the app, random codes would be exchanged. With the exchange of the random codes, the German public authority can find out the chain of infections albeit without being able to identify the actual individuals

Table 1. Public Health Measures of Selected Jurisdiction Summary

Country	Used Technologies	Use of Personal Information
South Korea	GPS, QR Code	Yes
China	GPS, Scanning	Yes
United States	Bluetooth	No
Japan	Bluetooth	No
Germany	Bluetooth	No

During the pandemic, contact tracing was a widely adopted measure to control the disease. The main goal is to identify individuals exposed to the coronavirus and trace the individuals who are in danger of developing or have developed a disease. Some countries like South Korea or China developed more sophisticated contact tracing with the latest data technologies and the use of personal information, i.e., name, phone number, address, location information, while western countries relied on bluetooth technologies to do contact tracing.

3. Korean Digital Public Health Measures and their Legal Basis

The South Korean public health authorities designed diverse measures specially based on the latest data technology in order to cope with the wide speared of COVID-19. Public health measures, (1) Contact-tracing (2) the Self-check App (3) the COVID-19 Electronic Wristband and (4) Electronic Entry Log (KI-Pass), were widely enforced for quarantine. Those digital public health measures extensively collected and used one's personal information under the legal basis, the Personal Information Protection Act, the Infectious Disease Control and Prevention Act, and the Infectious Disease Control and Prevention Act.

According to the World Health Organization, contact tracing is the process of identifying, assessing, and managing people who have been exposed to someone who has been infected with the COVID-19 virus, enabling to prevent the further transmission, to control the virus and to find out potentially infected persons before they gets into a serious medication.[1] While contact tracing can be done either manually, or speaking to individuals directly, or digitally, the South Korean government took digital tools to carry out contact tracing under the 76-2 of the Infectious Disease Control and Prevention Act. With the legal basis, the public authorities, i.e., the head of local government and cities, may request to have a concerning patient's personal information or, if necessary, to prevent infectious diseases and block the spread of infection. The types of collectable personal information are as follows. (***See Table 2***)

Table 2. Types of Collected Personal Information for Contact Tracing

Types of Collected Personal Information	Legal Basis
· Names · Resident Registration Numbers · Addresses · Telephone numbers (including cell phone numbers) · Prescriptions · Medical record · Records of immigration control · Location information	§ 76-2 of the Infectious Disease Control and Prevention Act
· Credit card, debit card, and pre-paid card statements · Transportation card statements · Image data compiled through image data processing equipment	§ 32-2 of the Enforcement Decree of The Infectious Disease Control and Prevention Act

In addition to that, to prevent the spread of COVID-19 into the local community, the South Korean government developed a mobile app called the Self-quarantine Safety Protection App. The app was released both Android and iPhone version with multiple language supports. The purpose of the app is to monitor health status of the targeted individuals entered into the Korean territory. Thus, Koreans and foreigners arriving from foreign countries were required to install the app. If a person leaves the original quarantine area without permission, or fails to report his or her health status, the app automatically notifies the violation of self-quarantine rules. Therefore, that person could face up to one year imprisonment or be fined up to 10 million won (approximately 8,200 USD).

Like the contact-tracing, the app was designed to collect one's personal information with the data technologies under the relevant laws. The laws, the Infectious Disease Control and Prevention Act, the Quarantine Act, the Personal Information Protection Act and the Act on

The Protection and Use of Location Information, allowed the central and the local governments to collect personal information as follows. (***See Table 3***)

Table 3. Types of Collected Personal Information for Contact Tracing App

Types of Collected Personal Information	Legal Basis
· Names, Date of Birth · Gender, Nationality · Cell phone numbers · Telephone numbers (including cell phone numbers) · Health Status such as fever, cough, Sore throat, Dyspnea · Geo-location information	§ 76-2 of the Infectious Disease Control and Prevention Act

Besides the Self-quarantine Safety Protection App, another digital tool, enforcing an electronic wristband for quarantine regulation violators, was adopted. As the violators defied the quarantine regulations, by disabling location services or by leaving the quarantine area without their mobile phone, the public health authority decided to implement a new measure.

The wristband was designed to track the violator's movement with connecting to the app via bluetooth technology. When a quarantined person tries to take off the wristband or to leave the specific quarantined area, it sends an alarm to local government officials. As its purpose is to monitor quarantined individuals, the wristband comes with a health monitoring functions. Thus, sensors equipped with the wristband check COVID-19 symptoms – fever, cough or throat soar – twice a day. Not to mention it tracks a patient's location. Once the patient denies answering properly and timely, the police may visit the place where the patient is.

Unlike other public health measures adopted by the South Korean government, enforcing a wristband to violators lacked firm legal basis. The public health authority expanded to apply the existing law, the Infectious Disease Control and Prevention Act. After the announcement to adopt the wristband, the National Human Rights Commission of Korea eventually delivered a public statement pointing out that it should be enforced to the minimum extent permitted by the law after reviewing the balance between restriction of basic rights and public interests as well as intrusiveness of such measures.[2]

The South Korean government adopted a more innovative measure to do contact-tracing, the QR electronic entry log, KI-PASS. It is similar to a recording system that tracks one's visitation history. The electronic entry log applied to high-risk facilities with poor ventilations such as gyms, restaurants or bars. Before the digitalized recoding system, the handwritten entry log was enforced, but the effectiveness for the handwritten entry was compromised due to inaccuracy issues and privacy matters.

The electronic entry log was originally collected when and where you have visited with legal basis. It collected relevant information via QR code. The collected information was encrypted and stored separately with Korean big techs, i.e., NAVER Corp. or Kakao Corp., and Korean Social Security Information Service, one of the public institutions under the Ministry of Health and Welfare of Korea. After the COVID-19 vaccines were released to the

public, the public health authority was enabled to monitor whether visitors are fully vaccinated. Thus, based on the regulations, unvaccinated persons were prohibited to visit high-risk facilities via the electronic entry log. The types of collectable personal information as follows (***See Table 4***)

Table 4. Types of Collected Personal Information for Contact Tracing QR Code

Types of Collected Personal Information	Legal Basis
· The day and the time of visitation · Residence information · Cell phone numbers · Telephone numbers (including cell phone numbers · Record of vaccination history · Geo-location information	§ 76-2 of the Infectious Disease Control and Prevention Act

3.1 The Meaning of Personal Information in Intelligent-information Society

In the modern society, the degree of digitalization is advancing rapidly. The pace of acceleration advanced exponentially after the advent of personal computers and internet services including the world wide web. These inventions played a key role in revolutionizing how we live and work. Due to their immense impacts, workplaces and homes without computer or internet are now hard to imagine. Moreover, the release of smartphones and other digital devices are further reshaping the way that we live and function.

Currently, global scholars and business leaders are in agreement that we are at the entry point of the Fourth Industrial Revolution. In this era, combination of artificial intelligence and data technology, the so called "Intelligent-information technology," is becoming the core driving force. Artificial intelligence enables machines to carry out human-like intellectual activities while data technology facilitates real-time collection, linkage, storage, and analysis of personal information.[3] Intelligent-information technology is a term integrating those technologies. Therefore, in an Intelligent-information Society, it is possible for machines to reach to the highest level of human intellectual activities, even those that are now considered to be only possible by a human being.[4] Therefore, considering the latest digital technologies (e.g., Artificial Intelligence, Big Data, Internet of Things, Clouds and Mobile), the use of massive amount of personal information is undeniable and inevitable.

The Personal Information Protection Act, one of the three main data protection laws in Korea, is a general law subject to the principle of the special law and it defines personal information.[5][1] Following the definition, phone numbers or computer IP addresses, which

[1] "A personal information controller shall not process any information prescribed by Presidential Decree (hereinafter referred to as "sensitive information"), including ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, and other personal information that is likely to markedly threaten the privacy of any data subject: Provided that this shall not apply to any of the following circumstances; (1) the individual's consent or (2) where other statutes require or permit the processing of sensitive information."

are not directly identifiable personal information by themselves, could fall under the scope of personal information. Thus, the scope of personal information is expanding and evolving.

One's personal information is an asset not only for private businesses but also for the government and public sectors, because it can be used for personalized services regarding social welfare, taxation, education, etc. Also, following the rapid development of digital technology, new industries such as mobile healthcare or telemedicine are also using and generating personal information. While the benefits of using personal information are clear, it is crucial to protect the right to privacy and other fundamental rights under the Constitutional Law in the process. We now turn to discuss the conflicting issues regarding personal information, as a subject matter of the protection and its use in the Intelligent-information Society.

3.2 The Right to Control Personal Information and its Meaning

Information such as name, phone number, address, passport number, and IP address, in general, would easily fall under the scope of personal information. Education history, occupation and or salary could also be considered as personal information, even though it does not precisely identify an individual. By combining fragmented information from multiple sources, an individual can be readily identified. Therefore, in highly digitalized society, one's identity is easily discernable regardless of the type and amount of information provided to individual sources.

In one of its landmark cases, in 2005, the Constitutional Court of Korea recognized a constitutional right to privacy in the form of the right to control personal information, or the right of Informational Self-determination, a case where collecting and digitalizing fingerprint information and using it for public investigation purposes were at issue.[6] The Court provided that it is a right of the data subject to personally decide when, to whom or by whom, and to what extent his or her information will be disclosed or used. The Court further stated that it is a basic right, although not specified in the Constitution, existing to protect the personal freedom of decision from the risk of infringement by state power and info-communication technology. Thus, the Court concluded that the subject matter of the case, the fingerprints of individuals, which are unique to an individual, shall be considered as personal information that identifies an individual from another. The scope of the right to control personal information is broad. Protected personal information includes physical information, personal beliefs, and social status – that is, information that allows characterization or identification of a specific individual.

According to the rationale of the Constitutional Court, one's COVID-19 infection status, location history, credit cards transaction data, and body temperatures recorded for the Entry Log all fall into the scope of personal information. Some of this information also fall under the definition of "sensitive information" which should receive absolute protection under the relevant laws. As the case pointed out, use of personal information without consent or beyond the scope of consent including collection, use, storage, and transfer of personal information by the government constitutes a violation of the right to control personal information. Therefore, collecting and processing the COVID-19 patient's history of

movement and health status such as body temperatures would constitute a violation of the right to control personal information, following the rationale of the Constitutional Court. Article 37(2) of the Korean Constitution prescribes that an individual's rights can be refrained for the purpose of national security, public order or public welfare. It also states, however, that the government cannot infringe the core value of the rights given to individuals. The COVID-19 crisis is no exception to this protection provided by the Constitution. Even in the face of a global pandemic, constitutional privacy rights should be respected.

4. Public Survey on the Korean Government's COVID-19 Policy and Critical Evaluations

4.1 COVID-19 and the Public Perceptions on Digital Public Health Measures

While trying to achieve the public health goal of preventing the spread of COVID-19, the Korean COVID-19 policy relied on heavy use of personal information. Based on public survey results, however, it appears that the general public did not perceive digital contact-tracing measures as excessive invasion of privacy. Meanwhile, concerns over erosion of privacy rights in Korea were raised from abroad.

First, regarding contact-tracing, the public showed an overwhelmingly positive view regarding the measure to mandate the QR-code based Electronic Entry Log, or KI-Pass, according to a survey conducted by TBS, a Korean press, with REALMETER, a Korean public opinion research company. ***(See Table 5)*** The results show that 70.3% of the public approved the government's enforcement of digital contact-tracing while only 16.5% of the respondents expressed negative views. Individuals who had favorable response to the QR-code-based Electronic Entry Log regarded it as an easy and effective method for contact-tracing. On the other hand, the respondents who were skeptical voiced concerns about the possibility of privacy infringement.

Table 5. Enforcing Electronic Entry Log
(Targeted Respondent: General public)

Q. What do you think about enforcing the Electronic Entry Log?	
Positive	70.3%
Negative	16.5%
Do not know	13.2%
Total	**100.0%**

Another public survey revealed similar results. (***See Table 6)*** According to the Hankook Research, one of largest public opinion research firms, 66 % of the entire respondents answered that the QR code Electronic Entry Log (KI-Pass) should be maintained considering the COVID-19 situation in Korea. While only 28% of the respondents answered that the

regulation enforcing QR code Electronic Entry Log should be relived or abolished as it restricts one's right to vaccinations. The survey was conducted in late December of 2021, and the targeted respondents were 1,000 adults.

Table 6. Enforcing Electronic Entry Log
(Targeted Respondent: General public)

Q. What do you think about enforcing the Electronic Entry Log?	
Should be maintained	66.0%
Should be relived or abolished	28.0%
Do not know	6.0%
Total	**100.0%**

Second, regarding mandating a wristband to the persons under COVID-19 quarantine, a public opinion survey was carried out by a private research company, Korean Research, on behalf of the Ministry of Culture, Sport and Tourism. The total number of respondents was 1,000, who were individuals over 18 years old. Approximately 80% of the respondents expressed positive opinions regarding the wristband, and only 13.2% of the respondents disapproved mandating the wristband, (***See Table 7***)

Among the respondents approving the wristband, preventing the wide spread of COVID-19 was the most popular reason for approval, accounting for almost half (47.1%) of the group. On the other hand, among those who were against enforcing the wristband, 42.4% expressed concern over human rights violation. Human rights include the right to privacy, given that a wide range of personal information is being stored and processed by the government.

Table 7. Mandating a Wristband during Quarantine
(Targeted Respondent: General public)

Q. What do you think about enforcing self-quarantined persons to wear a wristband?	
Agree	80.2%
Disagree	13.9%
No answer / Do not know	5.9%
Total	**100.0%**
Q. Why do you agree on enforcing self-quarantined persons to wear the wristband?	
Importanceof preventing the wide-spread of COVID-19	47.1%
Enables effective monitoring of the self-quarantined	19.3%
Need a more aggressive measure than the Self-check App	18.5%
Inevitable measure following self-quarantine violation	14.6%
Seems to be fine as other countries adopted similar measures	0.4%
For reasons other than the above	0.1%
Total	**100.0%**

Q. Why do you disagree on enforcing self-quarantined persons to wear the wristband?	
Violation of human rights	42.4%
Putting more efforts on administrative workforce is better than developing the device	22.3%
Those who comply have to suffer discomfort because of potential violators	18.7%
Not effective in preventing those who try to escape from the device	11.5%
Only limited cases of quarantine violation occurred, and the current system seems to be enough	2.9%
For reasons other than the above	2.2%
Total	**100.0%**

It is notable that Korean citizens are favorable to digital health public measures regardless of the amount of personal information collections, if we see the **Table 5 and Table 6**. Moreover, it seems that enforcing a wristband to quarantined individuals is a favorable method for Koreans to control the coronavirus, if we look at the **Table 7**. One of the compelling reasons for that could be ensuring the public health outweighs the right to privacy which may serve as a ground for the surveillance state.

4.3 Evaluating the Korean Government's Digital Public Health Measure

As discussed above, the Korean government used latest data technologies in order to cope with COVID-19 pandemic. It is hard to say that those digital public health measures were unsuccessful given that the confirmed cases were relatively lower than any other countries across the globe during the early state of COVID-19 pandemic. However, four different digital public health measures, (1) Contact-tracing (2) the Self-check App, (3) the COVID-19 Electronic Wristband, and (4) Electronic Entry Log, raised privacy invasion issues as they heavily relied on the use of personal information.

Koreans were subject to the administrative order since the beginning of the COVID-19 pandemic. During the two years from the outbreak of the pandemic, digital public health measures widely penetrated Koreans' daily lives. The Electronic Entry Log, the Self-check App, and the Electronic Wristband were enforced, and the relevant laws provided the legal basis to collect personal information for the purpose of protecting public health. An individual's name, phone number, location history, body temperature, credit or debit card transactions, mobile data, CCTV footage, and COVID-19 vaccination history were all subject to collection by the government.

While some of the aforementioned information is classified as general personal information, one's body temperature or vaccination history is different. They are information related to personal health, which is protected as sensitive personal information because the intrinsic value of sensitive information is deeply relevant to one's human rights. If medical information is revealed to a third party with no legal basis, the data subject could be at risk of unjustifiable prejudices. For that reason, the Personal Information Protection Act clearly prescribes the definition of sensitive information. In addition, the Infectious Disease Control and Prevention Act provides the legal basis to process an individual's sensitive information.

The article 34-2 and the article 76-2 of the Act clearly states that.[7][2]

4.4 Reviewing the COVID-19 Digital Measures and the Data Minimum Principle

In 1980, the Organization for Economic Co-operation and Development (OECD) adopted and released a privacy guideline, the Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereinafter "OECD Privacy Guideline"). The OECD privacy Guideline, though lacking legal binding power, has been regarded as a cornerstone with regard to the privacy rights and the free flow of personal data across the globe, as implemented into the laws, i.e., EU GDPR, the Personal Information Protection Act of South Korea.

The OECD Privacy Guideline clearly provides the eight core data privacy principles; (1) Collection Limitation Principle; (2) Data Quality Principle; (3) Purpose Specification Principle; (4) Use Limitation Principle (5) Security Safeguard Principle; (6) Openness Principle; (7) Individual Participation Principle; (8) Accountability Principle. Moreover, in 2013, the guideline faced a change due to the fast-changing environments driven by latest data technologies. Newly developed mobile IT devices with high-speed network technology enabled the flow of massive amount of personal data online, raised a concern over one's right to privacy, and required more strengthened data protection levels.

Back to the South Korean COVID-19 pandemic public measures, a number of personal information was widely collected for contact-tracing. The Infectious Disease Control and Prevention Act provided legal basis for use of various types of personal information. As discussed above, public health measures such as contact-tracing focusing on detailed information of confirmed patients, the Self-check app, the COVID-19 Electronic Wristband and the Electronic Entry Log, a.k.a. KI-Pass, were enforced. The governments collected a wide range of personal information just as seen on the above tables (from 2 to 4).

For instance, during the early stage of COVID-19 in 2020, the collected COVID-19 patient's location information raised a concern over the privacy rights because of unwanted exposures by the government. Across the Korean territory, disclosing a confirmed patient's recent visitation histories - where he or she has been before being tested positive - was regarded as

[2] When an infectious disease harmful to citizens' health is spreading, the Minister of Health and Welfare shall promptly disclose information with which citizens are required to be acquainted for preventing the infectious disease, such as the movement paths, transportation means, medical (The article 34-2 of the Infectious Disease Control And Prevention Act), and Public health authority can request information from third party such as (1) personal information including names, resident registration numbers prescribed in Article 7-2 (1) of the Resident Registration Act, addresses, and telephone numbers (including cell phone numbers); (2) prescriptions prescribed in Article 17 of the Medical Service Act, records of medical treatment prescribed in Article 22 of the same Act, etc.; (3) Records of immigration control during the period determined by the Minister of Health and Welfare; and (4) Other information prescribed by Presidential Decree for monitoring the movement paths of patients with infectious diseases (The article 76-2 of the Infectious Disease Control And Prevention Act)

a mean to ensure the right to know. Openness could make a huge contribution to the prevention of the coronavirus. However, the disclosed information by the government via online was unreasonably specific, enabling anybody to find out who he or she was by googling. Specially, social media activities searchable through online without hinderance contributed to re-identify a specific individual. One of the well-recognized cases, in 2020, took place in Itaewon, a popular spot for nightlife in Seoul, during the enforcement of COVID-19 quarantine. There was a confirmed patient who visited a dance club eventually was tested to positive to COVID-19. Not to mention that relevant information regarding him was publicly opened via online. Given that coronavirus transmits easily at highly populated and poorly ventilated places, the visitors of that dance club had no chance to avoid the massive contagions. A huge criticism was raised against them because they violated not only the quarantine rule but also provided a trigger of COVID-19 mass-contagion. However, after releasing the visited place, it suddenly raised a contempt on sexual minorities, the LGBTs.[8] As revealed that the dance club was well-known for LGBTs, the outcry pointed to the confirmed patient, and malicious comments behind the internet anonymity surged against the entire sexual minorities. Another case raised a criticism on a woman belonging to one of the Korean churches, “the Shincheonji” which is a religious sect. She, in first place, hided crucial information to the public health authorities, which eventually made a contribution to spread the epidemic. Like the Itaewon case, due to the disclosed information via online, where she visited turned out to be an issue. The “Shincheonji” church, was criticized for their mysterious activity and alleged financial accusations before. With the combination of the perception, the public outcried to the entire member of the Shincheonji.[9]

It would no exaggeration to say that those privacy-related cases could not happen without a wide range of personal information collected by the government. The patient was tracked by additional personal-information-related tools such as CCTV, credit card information, transportation card statements pursuant to the 32-2 of the Enforcement Decree of the Infectious Disease Control and Prevention Act.

One’s privacy rights have been threatened amid the COVID-19 pandemic on the basis of digital technologies. The collected information and the disclosed information played each other. It is hard to deny that the digital public health measures can be a great instrument to curve the freedom of the number of patients, and personal information is a key source to achieve the goal.

However, if we look the cases, where the patient visited had little relevance to COVID-19 quarantine measures. Moreover, religious information falls into the scope of sensitive information, i.e., an individual's ideology, faith, trade union or political party membership, political views, health, sexual orientation, across the global data protection laws. That sensitive information generally is not allowed to process unless a consent form of data subjects was provided. Of course, the article 23 of the PIPA allows to process sensitive information, provided that where other statutes require or permit the processing of sensitive information. What religion you have should be protected as it is one of specific types of sensitive information.

In this regard, the collection limitation principle under the OECD Privacy Guideline can be a useful basis for controlling the excessive COVID-19 digital measures. The collection

limitation principle, one of the privacy principles presented by OECD, is that the collection of personal information should have specified, explicit and legitimate purposes and should not be further processed over what it needs to be. This principle is clearly articulated in the article 3 of the PIPA. In other words, once personal information is required to be processed, it should be retained only as long as necessary. Thus, under the collection limitation principle, collecting and storing personal information more than necessary in relation to the purposes is not allowed.

As a part of protecting privacy rights, data processors seeking irrelevant or excessive amount of personal information are illegitimate. Moreover, after the official release of COVID-19 vaccination, the public health authority enforced the Electronic Entry Log (KI-Pass). All South Korean citizens who seek to enter the highly populated facilities such as restaurants or gyms are forced to present the KI-Pass operated by smartphone QR code. The QR code contained various types of personal information including name, phone number to the number of vaccinations. If an individual was not vaccinated or did not provide the relevant information, the individual could not enter the designated public space. And, if a business mandated to keep the entry log violated the administrative order, it was fined up to three million KRW (approximately 2,700 USD). The government maintained that all public health measures were operating under voluntary consent provided by individuals. However, the QR code Electronic Entry Log were designed and enforced to individuals and businesses outside of the scope of free consent. It was evident that the consent was hardly provided to the government voluntarily.[10]

With the above view, the collection of location information, CCTV footage, credit card transaction record, COVID-19 vaccination history is considered to be excessive. To be specific, one's face on the CCTV footage and the COVID-19 vaccination history fall into the scope of sensitive information. The PIPA, pursuant to the article 23, regulates the legitimacy of processing sensitive information. To be legitimate, data processors have to earn the consent from the data subject or, in case of other statutes specifically required, a permit for the processing of sensitive information. In fact, the PIPA pursuant to the article 58 provides that it does not apply when personal information processed temporarily where it is urgently necessary for the public safety and security, public health, et cetera. No exception to the provision on sensitive information is applied. However, there is no clear definition as to what the "processed temporarily where it is urgently necessary for the public safety and security, public health, et cetera" means so that there is a probability of arbitrary applications. Also, due to the unclear legal definition, nothing can tell the exact duration of collecting and storing personal information. Furthermore, most of data protection laws in the global world including the PIPA are clearly explicit that one's sensitive information is required to have strong protection for the reasons that it is highly relevant to a person's human rights. But, following the article 58 of the PIPA that excludes the application of the PIPA, the core rule that requires consent from data subjects to process one's sensitive information turns out to be useless.

While such Korean laws provided a clear legal basis to use sensitive information in adopting digital public health measures to combat COVID-19, there are globally recognized principles with respect to the use of personal information without the individual's consent. Given that

public health authorities collected a wide range of personal information from individuals during COVID-19, such measures are subject to criticism based on the Collection Limitation Principle, a.k.a. the Data minimum principle. The principle points out that the processing of personal information must be legitimate and must not be done beyond the essential reasons for processing. In other words, the government should minimize the processing of personal information. Protection of public health is the government's core priority and, for that purpose, the use of personal information to carry out contact-tracing is necessary. Regardless of the end goal, however, collection of personal information should be limited under the Collection Limitation Principle under the OECD Privacy Guideline. Particularly, if sensitive information is involved, it is required that strengthened safeguards are ensured. Especially, the Purpose Specification Principal mandates to specify the purpose of processing sensitive information.[11]

Despite that the effectiveness of digital contact tracing using one's personal information is outweighed, it should be considered that how the digital contact tracing may affect on privacy. For instance, like what South Korean government did, tracking on a person's location information by cell phone records is an invasion to one's privacy.[12] Digital quarantines collecting wide range of personal information for public health could raise an issue to digital censorship and suppressing the freedom of speech rather than the original purpose, controlling the coronavirus.[13]

The unprecedented health crisis raised the possibility that governments relied on the use of latest data technologies. The Korean government especially collected one's location information under the legal basis for diverse purposes such as contact-tracing or social distancing. Unlike other governments like EU countries, the Korean health authorities did not use bluetooth technology to locate the patient or anonymized location information. Depending on where you were, location information cannot pinpoint specific individuals due to building structures, i.e., underground. The location information can tell you where you have visited but it is not able to tell whom you have met with. Given the weakness of tracking location information, the Korean government collected one's credit card transaction records and Closed-Circuit Television (CCTV). In other words, the government processed unnecessarily excessive amounts of personal information. Collection of location information is likely to be ineffective, but it was carried out. Individuals have right to enjoy the right to privacy. However, once location information is collected from smartphone or mobile IT device by the governments, the state of digital surveillance will weaken the confidence against the government, and violate the freedom of speech, and privacy. To minimize a threat to individual's rights, the data minimum principle should be strengthened. Nothing can go beyond the OECD's fundamental privacy rights, mostly reflected in global data protection laws.

Once personal information is collected by the government, a concern over digital big brother is likely to be raised. The COVID-19 pandemic posed a threat to privacy with the use of excessive personal information. Once the personal information was collected, there should be a limit to use for the original purposes. No exceptions to the government shall be applied. If the original purpose is attained, data processors should destroy them. This is basic rules with regard to the data protection regimes. In addition to the over-collections and

destructions, the national government relied on wrongly established openness principle. Disclosing irrelevant information and the prevention of highly infectious disease has no relevancy each other. Rather, the disclosing of irrelevant information produced unwanted outcomes. Some of the patients suffered from malicious online comments.

All of the privacy-related cases took place from the COVID-19 contact-tracing. The meaning of digital big brother is not limited to a giant public existence watching citizens. It should be expanded to the extent that a hidden existence in private sectors could replace the public digital monster.[14] One's privacy is now under the surveillance from both governments and the general public, once information is disclosed without a consent. Even on the legal basis, data processors are necessary to rethink the OECD privacy guideline and apply its principles to their practices.

Moreover, if the digital quarantines are enforced, without the voluntariness, decentralization, simplicity, transparency, and the lack of reliance on a persistent identifier, there would be no public trust on the public health measures.[15] Therefore, as the privacy rights could be in danger under the name of public health for the digital quarantines, it should be carefully considered that one of the widely accepted principles, the data minimum principle, is applied during the pandemic.[16]

5. Conclusion

COVID-19 has posed a huge threat to our health and life. As the coronavirus continues evolving, the number of casualties has reached to over millions and the number of infected persons is close to half of the entire global population. In order to prevent the spread of the virus, governments around the world introduced a myriad of public health policies. Among different strategies, the Korean government relied heavily on data technology against the coronavirus and adopted: (1) digital contact-tracing (2) the Self-check App and (3) the COVID-19 Electronic Wristband. These methods were designed to collect, store and use one's personal information. Under relevant laws, public health authorities legally gathered a wide range of personal information including name, phone number, address, health status, CCTV footages, credit card transaction records. Later, when COVID-19 vaccines were introduced, vaccination history including the type of vaccine and numbers were also collected by the QR code Electronic Entry Log.

While the Korean government was successful in containing the wide spread of COVID-19 during the early stages of the pandemic, the cost of digital public health measures should not be dismissed. Based on the Collection Limitation Principle, collection of personal information should be minimized. This principle is widely accepted in global data protection laws since the OECD introduced Guidelines on the Protection of Privacy and Trans border Flows of Personal Data in 1980. Even the Korean data protection law, the Personal Information Protection Act, clearly incorporates the principle in Article 3 of the Act, which prescribes the Collection Limitation Principle and the Purpose Specification Principle together.

Given the extent of collection and processing of personal information by public health authorities, the Korea's public health measures did not comply with the globally recognized data principles. Of course, in the face of a global pandemic, it was necessary to use individual's personal information. However, the Korean government did not attempt to harmonize the data minimum principles and public health goals; rather it even expanded to collect one's vaccination history that falls under sensitive information, equivalent to the special categories of persona information under the EU GDPR.

We cannot predict the future thus do not know what type of new infectious disease might affect our life. Considering rapid development of data technology, it is foreseeable that the government will continue heavily relying on technology to fight future public health crises. The Korean government's COVID-19 policies provide an important lesson for the future and should alarm us regarding the possible emergence of the surveillance states. A public health goal cannot justify invasion of individual privacy, and the data minimum principle must be respected as the highly digitalized society continues evolving.

Acknowledgement

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2022-0-00688, AI Platform to Fully Adapt and Reflect Privacy-Policy Changes)

References

[1] WHO, "Coronavirus disease (COVID-19): Contact tracing," 5, 2021. Article(CrossRef Link)
[2] National Human Rights Commission of Korea, "COVID-19 Is a Test of Our Society's Ability to Protect Human Rights," 4, 2020. Article(CrossRef Link)
[3] Joint Ministries, "The mid-and-long Term Comprehensive Measures to the Intelligent-information Society responding to the Fourth Industrial Revolution," 2016. Article(CrossRef Link)
[4] Kim Il Hwan, "The Role and Function of the Constitutional Law in the Intelligent-information Society," *Sungkyunkwan Law Review*, vol. 37 no. 2, 2020. Article(CrossRef Link)
[5] Korea Legislation Research Institute, Personal Information Protection Act, Article 23 (Limitation to Processing of Sensitive Information), (1) 1, 2020. Article(CrossRef Link)
[6] 99Hun-Ma513 and 2004Hun-Ma190 (consolidated), May 26, 2005. Article(CrossRef Link)
[7] Korea Legislation Research Institute, Infectious Disease Control And Prevention Act, Article 76-2 (Request for Provision of Information and Verification of Information), (1) 3, 2021. Article(CrossRef Link)
[8] Min Joo Kim, Tracing South Korea's latest virus outbreak shoves LGBTQ community into unwelcome spotlight, May 11, 2020. Article(CrossRef Link)
[9] Raphael Rashid, Being Called a Cult Is One Thing, Being Blamed for an Epidemic Is Quite Another, March 9, 2020. Article(CrossRef Link)
[10] Kim Il Hwan, "Die Untersuchung über die Zweckbindung in Datenschutzgesetz," *Study on the American Constitution*, 25(3), pp. 109-134, 2014. Article(CrossRef Link)
[11] Kwon Guen-Bo, "Preventive measures against Infectious Disease and Information Human Rights," *Public Law Journal*, 21(3), pp. 3-31, 2020. Article(CrossRef Link)

[12] Koustubh "K.J." Bagchi, Christine Bannan, Sharon Bradford Franklin, Heather Hurlburt, Lauren Sarkesian, Ross Schulman, and Joshua Stager, “Digital Tools for COVID-19 Contact Tracing: Identifying and Mitigating the Equity, Privacy, and Civil Liberties Concerns,” *COVID-19 White Paper 22, Edmond J. Safra Center for Ethics*, 2020. Article(CrossRef Link)
[13] Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, “Censored Contagion: How Information on the Coronavirus is Managed on Chinese Social Media,” *Research Report*, 125, 2020. Article(CrossRef Link)
[14] Lee Joonbok, “Legal study for Reasonable response to Coronavirus(COVID-19) Pandemic: Suggestions on the Scope of Information Use by Infectious Disease Patient,” *KANGWON LAW REVIEW*, 61, 2020. Article(CrossRef Link)
[15] Jay Stanley and Jennifer Stisa Granick, “The Limits of Location Tracking in an Epidemic,” *ACLU*, 2020. Article(CrossRef Link)
[16] EDPB, “Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak,” 2020. Article(CrossRef Link)

Dr. Min Woo Kim is the researcher of the Korea Social Security Information Service, a public institution under the Ministry of Health and Welfare of South Korea. He received his bachelor of laws from Hongik University, LL.M. from Georgetown University Law Center in Washington DC, USA, and Ph.D. in law degree from Sungkyunkwan University. His academic interest area includes data protection law and privacy.

Professor Ilhwan Kim is the Dean of Sungkyunkwan University (SKKU) Law School and heads the SKKU Science& Technology Law Institute. He served as the Chairperson of the Personal Information Dispute Mediation Committee. He received his bachelor of laws and master of laws from Sungkyunkwan University and earned his Ph.D. in law degree from the University of Mannheim in Germany. His academic interest area includes constitutional law and data protection law.

Professor Jaehyoun Kim received his B.S. degree in mathematics from Sungkyunkwan University (SKKU), Seoul, Korea, M.S. degree in computer science from Western Illinois University and Ph.D. degrees in computer science from Illinois Institute of Technology in USA. He served as a Chief Technology Officer at Kookmin Bank in Korea before he joined the Department of Computer Education at Sungkyunkwan University in March 2002. Currently he is a professor at Sungkyunkwan University. Also, he is a dean of College of Education and a chairman of Data Science (DS) Education Center at SKKU. His research interest areas include software engineering & architecture, e-Learning, SW/AI education and computer-based learning.

Dr. Oh Jung Ha is the researcher at Sungkyunkwan University (SKKU) Science& Technology Law Institute. She received her master of laws degree and Ph.D. in law degree from Sungkyunkwan University. Her academic interest area includes artificial intelligence, algorithm, personal data and constitutional law.

Professor Chang Jinsook is the assistant professor at Department of International Industrial Information of Kyonggi University and teaches International Economic Law. She received her bachelor of laws, master of laws and Ph.D. degree from Sungkyunkwan University. She also earned LL.M. with specialization certificate in International Law at American University Washington College of Law in Washington DC, USA.

Dr. Park Sang Don is the senior researcher at the National Security Research Institute. He researches about the law and policy. He received his LL.B., LL.M. and Ph.D. in law degree from Sungkyunkwan University. His research interest areas include constitutional law theory, administrative law theory and public laws on ICT and security.