18

Data Governance and Trust

Lessons from South Korean Experiences Coping with COVID-19

Sangchul Park, Yong Lim, and Haksoo Ko[*]

I. INTRODUCTION

COVID-19 is reshaping history with its unprecedented contagiousness. The epidemic swept the whole world throughout 2020 and beyond. In the case of South Korea (hereafter Korea), the first confirmed case of COVID-19 was reported on 20 January 2020.[1] During the initial phase after the first reported case, the Korean government hesitated to introduce compulsory quarantine for travelers from high-risk countries.[2] It put Korea on a different trajectory compared to other countries which imposed aggressive measures including immigration quarantine from the beginning.[3] The number of confirmed infections increased significantly in a short span of time and, by the end of February 2020, the nation was witnessing an outbreak that was threatening to spiral out of control. Korea appeared to be on the way to becoming the next 'COVID-19 hotspot' after China.[4] Confronting an increasing number of cases of COVID-19, Korea had to weigh among various options for Non-Pharmaceutical Interventions (NPIs). Korea did not take extreme measures such as shelter-in-home and complete lockdowns. Instead, it employed a series of relatively mild measures, including a social distancing order that imposed restrictions on public gatherings and on operating businesses, set at different levels in accordance with the seriousness of the epidemic.[5] A differentiated measure that Korea took was an aggressive contact tracing scheme, which served a complementary role to social distancing.

[*] This chapter is a revised and expanded version from S Park and Y Lim, 'Harnessing Technology to Tackle COVID-19: Lessons from Korea' (2020) 61 *Inform. Process. [Jōhōshori]* 1025.

[1] Korea Disease Control and Prevention Agency (KDCA), 'A Foreign-Imported Case of Novel Coronavirus Was Confirmed during Immigration Quarantine: The Epidemic Crisis Alert Level Elevated to Warning' (*KDCA*, 20 January 2020) http://ncov.mohw.go.kr/tcmBoardView.do?ncvContSeq=352435&contSeq=352435.

[2] Korea started to impose a compulsory two-week quarantine for travelers from Europe on 22 March, 2020, for travelers from the US on 27 March, 2020, and for travelers from the other countries including China on 1 April, 2020. KDCA, 'COVID-19 Domestic Case Status' (*KDCA*, 27 March 2020) http://ncov.mohw.go.kr/tcmBoardView.do?ncvContSeq=353770&contSeq=353770.

[3] J Summers and others, 'Potential Lessons from the Taiwan and New Zealand Health Responses to the COVID-19 Pandemic' (2020) 4 *Lancet Reg Health West Pac* 10044.

[4] S Park, GJ Choi and H Ko, 'Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea – Privacy Controversies' (2020) 323(21) *JAMA* 2129.

[5] The central and municipal and/or local governments are authorised to 'restrict or prohibit the aggregation of multiple persons including entertainment, assembly, and rituals' in accordance with Article 49-1(ii) of the Contagious Disease Prevention and Control Act. Based on this provision, the government set the level of social distancing from Level 1 to Level 3 (with the interval being 0.5).

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

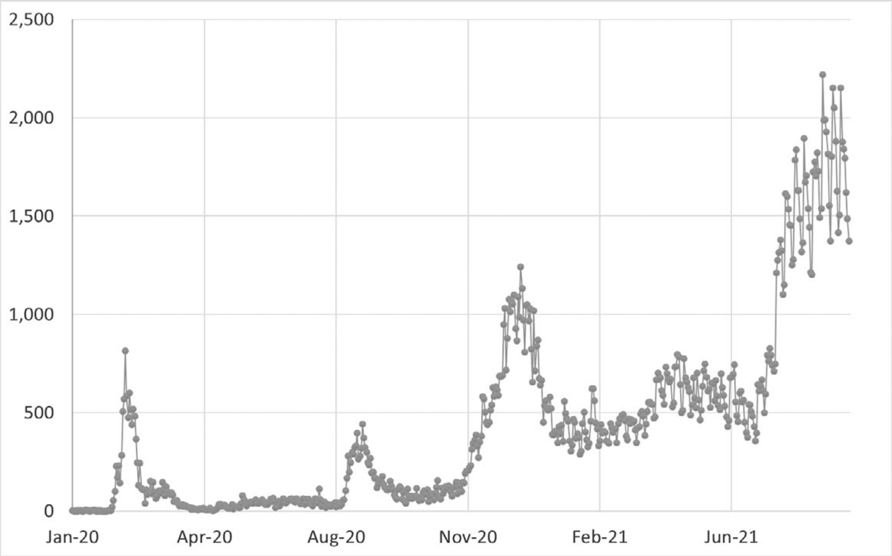

FIGURE 18.1 Daily newly confirmed COVID-19 cases
Note: KDCA, Press Releases (*MOHW*, 20 January 2020 to 1 September 2021), http://ncov.mohw.go.kr

Adopting an effective contact tracing strategy requires, as a pre-requisite, a lawful and technically feasible capability to collect and process relevant personal data including geolocation data. Doing so was possible in Korea because it had already introduced a legal framework for technology-based contact tracing after its bruising encounter with the Middle East Respiratory Syndrome (MERS) in 2015. Based on its previous experience with MERS and the legislative measures and mandates adopted in the course of the MERS outbreak, Korea was well equipped to respond to COVID-19 by swiftly mounting aggressive contact tracing and other data processing schemes when COVID-19 materialised as a significant threat to the public health of its citizens. Thus, the nation's technological infrastructure was mobilized to provide support for epidemiological investigations. The contact tracing scheme, along with a sufficient supply of test kits (such as PCR [polymerase chain reaction] kits for real-time testing) and of personal protective equipment (such as respirators), was perhaps a key contributing factor to Korea's initial success in flattening the curve of infections and deaths, when it had to confront two major outbreaks that occurred around March and August 2020, respectively. Toward the end of 2020, Korea began facing a new round of difficulties in dealing with a third outbreak, and it again actively implemented a contact tracing scheme. As of 00:00, 1 September 2021, the accumulated number of confirmed cases was recorded at 253,445 (0.49% of the total population), including 2,292 total deaths.[6] Figure 18.1 shows the trend of newly confirmed cases.

While the statutory framework introduced after the MERS outbreak provided the necessary means to launch a technology-based response to COVID-19, new challenges arose in the process. In particular, there was an obvious but challenging need to protect the privacy of those infected and of those who were deemed to have been in close contact while, at the same time, maintaining the effectiveness of the responses. This chapter provides an overview of how Korea

[6] KDCA, 'COVID-19 Domestic Case Status (1 September 00:00)' (*KDCA*, 1 September 2021) http://ncov.mohw.go.kr/tcmBoardView.do?brdId=3&brdGubun=31&dataGubun=&ncvContSeq=5878&contSeq=5878&board_id=312&gubun=BDJ.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

harnessed the power of technology to confront COVID-19 and discusses some of the issues related to the governance of data and technology that were raised during Korea's experiences.

This chapter is organized as follows: Section II provides an overview of the legal framework which enabled an extensive use of the technology-based contact tracing scheme; Section III explains the structure of the information system that Korea set up and implemented in response to COVID-19; Section IV details the actual use of data for implementing the legal scheme and relevant privacy controversies; Section V further discusses data governance and trust issues; and, finally, Section VI concludes.

II. LEGAL FRAMEWORKS ENABLING EXTENSIVE USE OF TECHNOLOGY-BASED CONTACT TRACING

1. *Consent Principle under Data Protection Laws*

A major hurdle in implementing the pandemic-triggered contact tracing scheme in Korea was the country's stringent data protection regime. Major pillars of the legal regime include the Personal Information Protection Act (PIPA),[7] the Act on Protection and Use of Location Information (LIA),[8] and the Communications Secrecy Protection Act (CSPA).[9] As a means to guarantee the constitutional right to privacy and the right to self-control of personal data, these laws require prior consent from the data subject or a court warrant prior to the collection and processing of personal data, including geolocation data and communications records. Arguably, the consent principle of the Korean law is largely modeled after what can be found in the European Union's (EU's) privacy regime including the General Data Protection Regulation (GDPR). However, Korea's data protection laws tend to be more stringent than the EU's, for instance, by requiring formalities such as the notification of mandatory items when obtaining consent. Certain statutory features of the Korean data protection laws on data collection are as follows.

First, the PIPA is the primary law governing data protection. Under the PIPA, the data subject must, before giving consent to collection, be given notice including the following: (i) the purpose of collection and use, (ii) the items of data collected, (iii) retention and use period, and (iv) (unless data is collected online) the data subject's right to refuse consent and disadvantages, if any, from the refusal.[10] The data subject must, before giving consent to disclosure, be given notice of the recipient and similar items as above.[11] A recent amendment to the PIPA which took place in 2020 allows exceptions to the purpose limitation principle within the scope reasonably related to the purpose for which the personal data is initially collected.[12] The 2020 amendment of the PIPA also grants an exemption to the consent requirement when the processing of pseudonymized personal data is carried out for statistical, scientific research, or archiving purposes.[13] However, these built-in exceptions are not broad enough to cover the processing of personal data for the centralized contact tracing scheme.

[7] Personal Information Protection Act [*Gaein Jeongbo Boho Beop*], Act No 16930 (last amended on 4 February 2020, effective as of 4 February 2020).

[8] Act on Protection and Use of Location Data [*Wichi Jeongboeu Boho Mit Iyong Deung'e Gwanhan Beopryul*], Act No 17689 (last amended on 22 December 2020, effective as of 1 January 2021).

[9] Communications Secrecy Protection Act [*Tongshin Bimil Hobo Beop*], Act No 17831 (last amended and effective on 5 January 2021).

[10] PIPA, Articles 15(2), 39-3(1).

[11] PIPA, Article 17(2).

[12] PIPA, Articles 15(3) and 17(4).

[13] CSPA, Article 28-2(1).

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

Second, the LIA is a special law that governs the processing of geolocation data such as GPS (global positioning system) data and cell ID. This type of data is usually collected by mobile carriers or mobile operating system operators and is shared with mobile app developers. Under the LIA, a data subject of geolocation data must be given appropriate notice in the standard forms before giving consent to the collection, use, or disclosure of personal geolocation data.[14]

Third, the CSPA governs when and how courts or law enforcers can request communications records including base station data or IP (internet protocol) addresses from carriers or online service providers.[15] Under the CSPA, law enforcers can request data concerning a specific base station (the base station close to the location where the mobile phone user at issue made calls) from mobile carriers in order to deter crime, to detect or detain suspects, or to collect or preserve evidence.[16] Doing so is, however, permitted only when other alternatives would not work. This provision reflects the reasoning of a constitutional case of 2018. In this case, the Constitutional Court of Korea held that a prosecutor's collection of the identities of mobile subscribers that accessed a single base station infringed the constitutional right to self-control of personal data and the freedom of communications and that doing so is thus unconstitutional.[17]

However, the previous MERS outbreak had shown the need for putting in place an effective contact tracing scheme when needed. This prompted an amendment of the Contagious Disease Prevention and Control Act (CDPCA)[18] so as to override the consent requirements under Korean data protection law in the event of an outbreak. There already is a provision in the PIPA, which exempts the application of the consent and other statutory requirement for temporary processing of personal data when there is an emergency need for public safety and security including public health.[19] The amendment of the CDPCA gave more concrete legal authority for implementing a contact tracing scheme during an outbreak of a contagious disease. After the onset of COVID-19, the Korean legislature further amended the CDPCA several times in order to better cope with the situations that had not been anticipated prior to the outbreak of COVID-19.

2. *Legal Basis for Centralized Contact Tracing*

For manual contact tracing by epidemiological investigators, interviews play a crucial role. Conducting interviews obviously takes time and sometimes accuracy could become an issue. As such, manual contact tracing has limitations in terms of the timely detection and quarantine of those suspected of being infected. Efforts were made in many parts of the world in order to make up for these limitations and several automated contact tracing models have been devised. Most of the newly devised models rely on geolocation data, typically gathered through smart phones. Each of these models has its own advantages and disadvantages as discussed below.

Depending on the provenance of the relevant data, these models can be divided into centralized models and decentralized models. There can also be a hybrid model. Among different types of automated contact tracing models, a majority of developed countries appear

[14] CSPA, Articles 18 and 19.

[15] As Korea has not signed the Budapest Convention on Cybercrime, there are several differences between the CSPA and wiretapping regimes of the US and EU.

[16] CSPA, Article 13(2).

[17] Constitutional Court of Korea, Case Ref. 2012 *Heonma* 538 (28 June 2018).

[18] Contagious Disease Prevention and Control Act [*Gamyeombyeongeu Yebang Mit Gwanri'e Gwanhan Beopryul*], Act No 17893 (last amended on 12 January 2021, effective as of 13 January, 2022).

[19] PIPA, Article 58(1)(3).

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

to have chosen decentralized 'privacy-preserving' proximity tracing models. These typically relay geolocation data utilizing the Bluetooth Low Energy technology. By design, these models grant data subjects the right to avoid tracking by not downloading or activating mobile apps. Soon after early efforts were made in order to develop and deploy a contact tracing model in the EU, the European Data Protection Board (EDPB) issued guidelines dated 21 April 2020. According to the EDPB guidelines, COVID-19 tracing apps would have to be based on the use of proximity data instead of geolocation data.[20]

For the decentralized approach, there are two subtypes: a fully decentralized approach and a partially decentralized approach. A fully decentralized approach works as follows. Through the operation of a mobile app, (i) smart phones exchange ephemeral IDs of individuals nearby via Bluetooth Low Energy ('Bluetooth Handshakes'); (ii) those individuals who are subsequently confirmed positive send their ephemeral IDs to a database in the server; and (iii) each app continues to download the database from the server and alerts if its owner has been in close proximity to one of those who are tested positive.[21] Apple-Google's Exposure Notification (AGEN) scheme is a well-known case of the decentralized approach.[22] AGEN has reportedly been embedded in the majority of European COVID-19 apps, including Austria's Stopp Corona, Germany's Corona-Warn-App, Italy's Immuni, Estonia's HOIA, the UK's NHS COVID-19, Protect Scotland, and StopCOVID NI (for Northern Ireland).[23] Japan also adopted AGEN in its contact tracing scheme called COCOA.

On the other hand, a main differentiating feature of the partially decentralized approach is that, in addition to being equipped with the functions of the fully decentralized app, a partially decentralized app would send ephemeral IDs collected from other smart phones to the server database so that it becomes possible to conduct contact tracing, risk analysis, and message transmission, utilizing the data accumulated at the server database.[24] Its examples include the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) (specifically, the ROBERT protocol) and BlueTrace.[25] The PEPP-PT scheme was embedded in France's StopCovid and TousAntiCovid, and the BlueTrace approach was embedded in Singapore's TraceTogether and Australia's COVIDSafe.

Unlike these approaches, Korea has taken a centralized network-based contact tracing approach, which utilizes geolocation data collected from mobile carriers and other types of data

[20] EDPB, 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak' (*EDPB*, 21 April 2020) https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en ('In the context of a contact tracing application, careful consideration should be given to the principle of data minimisation and data protection by design and by default: contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used; as contact tracing applications can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification; the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary.') Based on these Guidelines, the Norwegian Data Protection Authority (Datatilsynet), in June 2020, banned a GPS tracking COVID-19 app (named Smittestopp) which the Norwegian Institute of Public Health developed and released. Datatilsynet, 'Vedtak om midlertidig forbud mot å behandle personopplysninger – appen Smittestopp" (*Datatilsynet*, 6 July 2020) www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2020/vedtar-midlertidig-forbud-mot-smittestopp/.

[21] N Ahmed and others, 'A Survey of Covid-19 Contact Tracing Apps' (2020) 8 *IEEE Access* 134577 (hereafter Ahmed and others, 'A Survey of Covid-19').

[22] Apple and Google, 'Privacy Preserving Contact Tracing' (*Apple*, 2020). https://covid19.apple.com/contacttracing.

[23] PH O'Neill, T Ryan-Mosley, and B Johnson, 'A Flood of Coronavirus Apps are Tracking Us. Now It's Time to Keep Track of Them' (*MIT Tech Rev*, 7 May 2020) www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

[24] N Ahmed and others, 'A Survey of Covid-19' (n 21).

[25] Ibid.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

that facilitate tracking of individuals. This approach does not allow its citizens to opt out of the contact tracing scheme. Only a few other jurisdictions, including Israel[26,27] and China,[28] appear to have taken this approach. In Korea, government agencies are granted a broad authority to process personal data during a pandemic for epidemiological purposes. Under the current provisions of the CDPCA, the Korea Disease Control and Prevention Agency (KDCA)[29] and municipal or/and local governments can, at the outbreak of an infectious disease, collect, profile, and share several categories of data that pertain to individuals who test positive or individuals who are suspected of being infected.[30] The data that can be collected include geolocation data; personal identification information; medical and prescription records (including the Drug Utilization Review [DUR]); immigration records; card transaction data for credit, debit, and prepaid cards; transit pass records for public transportation; and closed-circuit television (CCTV) footage.[31] In this context, 'individuals who are suspected to be infected' mean those who have been in close proximity to confirmed individuals, those who entered the country from a high risk region, or those who have been exposed to pathogens and other risk elements.[32] These individuals can be required to quarantine.[33] The CDPCA explicitly stipulates that the request of geolocation data under this law overrides the otherwise-applicable consent requirements under the LIA and CSPA.[34]

The KDCA can share the foregoing data with (i) central, municipal, or local governments, (ii) national health insurance agencies, and (iii) healthcare professionals and their associations.[35] The KDCA must also transfer a part of the data, including immigration records, card transaction data, transit pass records, and CCTV footage, to national health insurance information systems and other designated systems.[36]

Despite this legal mandate and authority, however, in practice, the scope and breadth of the data processed for contact tracing purposes and the recipients of the shared data have been much narrower, as explained in Subsections 3 and 4.

[26] Israel reportedly resorted to its emergency powers to redirect the counterterrorism monitoring program of the Israel Security Service (Shin Bet) into conducting contact tracing, which its Supreme Court later held to be unlawful unless the practice is permitted through legislation (Israeli Supreme Court, HCJ 2109/20, HCJ/2135/20, HCJ 2141/20 *Ben Meir v Prime Minister* (2020) (English translation) (*VERSA*, 26 April 2020) https://versa.cardozo.yu.edu/opinions/ben-meir-v-prime-minister-0).

[27] In July 2020, Israel's legislation, Knesset, passed a law authorizing the Security Service to continue to engage in contact tracing until 20 January 2021, and approved an extension of this period in January 2021(Knesset News, 'Foreign Affairs and Defense Committee approves continued use of the Shin Bet in the efforts to contain the spread of the coronavirus' (*The Knesset*, 13 January 2021), https://main.knesset.gov.il/EN/News/PressReleases/Pages/press13121q.aspx).

[28] China is also understood to have adopted a centralized approach utilizing QR codes, mobile apps, and other means, but its technical details have not been disclosed clearly (Paul Mozur et al., 'In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags' (*New York Times*, 7 August 2020), www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html).

[29] On 12 September 2020, the Korea Centers for Disease Control and Prevention (KCDC) was reorganized as a formal government agency to better combat the pandemic under the name of the Korea Disease Control and Prevention Agency (KDCA). References to the KDCA in this chapter include the agency's activities prior to the reorganization.

[30] CDPCA, Article 76-2.

[31] CDPCA, Article 76-2(1)(2).

[32] CDPCA, Article 2(xv-2).

[33] CDPCA, Article 42(1).

[34] CDPCA, Article 76-2(2).

[35] CDPCA, Article 76-2(3).

[36] CDPCA, Article 76-2(4).

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

3. *Legal Basis for QR Code Tracking*

The amendment to the CDPCA of 4 March 2020[37] authorized the KDCA, the Ministry of Health and Welfare, and municipal and/or local governments to issue decrees to citizens 'to keep the list of administrators, managers, and visitors at the venues or facilities having the risk of spreading infectious diseases'.[38] This new provision enabled the KDCA to deploy an electronic visitor list system by utilizing QR (quick response) codes.

4. *Legal Basis for the Disclosure of the Routes of Confirmed Cases*

Under the CDPCA, at the outbreak of a serious infectious disease, the KDCA and municipal and/or local governments must promptly make the following information publicly available on the Internet or through a press release: the path and means of transportation of confirmed cases; the medical institutions that treated the cases; and the status of relevant close contacts.[39] Anybody can appeal if the disclosed information is incorrect or if there is any opinion. From this appeal, if deemed needed, the KDCA or municipal and/or local governments should immediately take necessary remedial measures such as making a correction.[40]

This provision allowing for public disclosure of information is an important exception to the principles set forth under Korea's data protection laws. This provision was introduced in the CDPCA in 2015 following the MERS outbreak. At the time, epidemiologists first requested the government to disclose the information about the hospitals that treated confirmed cases and also about the close contacts in order to protect healthcare professionals from the risk of infection.[41] The public opinion also urged the government to ensure transparency by disclosing whereabouts of confirmed cases.[42] In response, the government disclosed the list of the hospitals that treated confirmed cases on 5 June 2015, breaking the non-disclosure principle for the first time. A bill for the foregoing provision was submitted on the same day and was passed by the legislature on 6 July 2015.[43] The bill was passed within a very short period of time and, as such, there was insufficient time to consider and debate privacy concerns and other important implications that would arise from the amendment. Following the outbreak of COVID-19 in 2020, this provision was immediately triggered, raising considerable privacy concerns as explained below in Sub-section V 2.

5. *Legal Basis for Quarantine Monitoring*

The amendment to the CDPCA of 4 March 2020[44] authorized the KDCA and municipal and/or local governments to check the citizens for symptoms of infectious diseases and to collect geolocation data through wired or mobile communication devices.[45] This new provision enabled the KDCA to track GPS data to monitor those quarantined at home.

[37] Effective as of 5 June 2020.

[38] CDPCA, Article 49(1)(ii-ii).

[39] CDPCA, Article 34-2(1).

[40] CDPCA, Article 34-2(3)(4).

[41] The Korean Society of Infectious Diseases, 'White Paper on Chronicles of MERS' (*KSID*, 2015) www.ksid.or.kr/file/mers_170607.pdf.

[42] Ibid.

[43] Effective as of 7 January 2016.

[44] Effective as of 5 June 2020.

[45] CDPCA, Article 42(2)(ii).

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

Prior to this amendment, the quarantine monitoring app had already been in use. During this period, in order to comply with the consent requirements for the collection and use of personal geolocation data under the LIA, the app to be used for monitoring purposes made a request to an installer to click on the consent button before installation process starts. Because installing the monitoring app and providing the requisite consent allowed one to avoid the inconvenience of being manually monitored by the quarantine authorities or of facing the possibility of being denied entry into the country, most individuals who were subject to quarantine appear to have chosen to use the app. It was not entirely clear whether such involuntary agreement to download and activate the app constitutes valid consent under the LIA, and the foregoing amendment to the CDPCA clarified the ambiguity by explicitly allowing the collection of geolocation data for quarantine monitoring purposes.

III. ROLE OF TECHNOLOGY IN KOREA'S RESPONSE TO COVID-19

A variety of technological means were employed in the process of coping with the pandemic in Korea. Among these, the most important means would include the tools to gather and utilize geolocation data for the purposes of engaging in contact tracing and other tracking activities. The following describes how technological tools were deployed.

1. *Use of Smart City Technology for Contact Tracing*

Based on the mandate and authority under the CDPCA, the Korean government launched the COVID-19 Epidemic Investigation Support System (EISS) on 26 March 2020.[46] By swiftly remodeling the EISS from the existing smart city data hub system developed by several municipal governments, Korea could save time during early days of the pandemic. Prior to the outbreak of COVID-19, in accordance with the Smart City Act,[47] the Korean central and municipal and/or local governments had been developing and implementing smart city hubs; several 'smart cities' have been designated as test beds for innovation in an effort to foster the research and development in areas related to sharing-economy platforms, AI services, Internet-of-Things technologies, renewable energy, and other innovative businesses. In relative terms, compared to a situation in which systems developed for security service agencies are redeveloped and used for contact tracing purposes, the use of a smart city system might have the advantage of heightened transparency and auditability.

The EISS collects requisite data pertaining to confirmed cases and those who are suspected to have been in contact. Data that can be collected includes base station data from mobile carriers and credit card transaction data from credit card companies. In order to obtain data, clearances should be obtained from the police and from the Credit Finance Association (CREFIA), respectively, for base station data and for credit card transaction data. After clearances are obtained, transfer of the data to epidemiological investigators takes place on a near real-time basis.[48] Equipped with base station data and credit card transaction data, epidemiological investigators can effectively track many of the confirmed cases and their close contacts, as

[46] A pilot operation started on 16 March 2020.

[47] The Act on Construction of Smart Cities and Industry Promotion [*Smart Doshi Joseong Mit San'eop Jinheung Deung'e Gwanhan Beopryul*], Act No 17799 (last amended on 29 December 2020, to be effective as of 30 December 2021).

[48] The Ministry of Land, Infrastructure and Transport (MOLIT), 'Online Q&A for the Support System for the COVID-19 Epidemiological Investigation' (*MOLIT*, 10 April 2020), www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?id=95083773.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

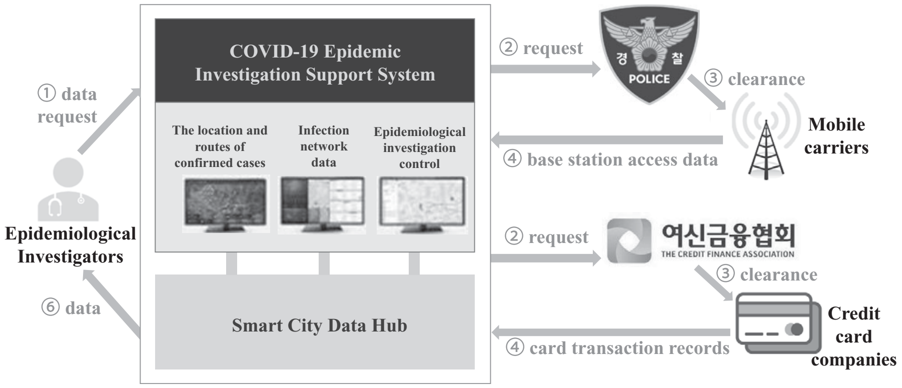
① data request
Epidemiological Investigators
⑥ data
COVID-19 Epidemic Investigation Support System
The location and routes of confirmed cases
Infection network data
Epidemiological investigation control
Smart City Data Hub
② request
경 찰 POLICE
③ clearance
Mobile carriers
④ base station access data
② request
여신금융협회 THE CREDIT FINANCE ASSOCIATION
③ clearance
Credit card companies
④ card transaction records

FIGURE 18.2 The COVID-19 Epidemic Investigation Support System
Note: MOLIT, 'COVID-19 Smart Management System (SMS), formally named 'COVID-19 Epidemic Investigation Support System (EISS)' (*MOLIT*, 6 December 2020), https://smartcity.go.kr/ (hereafter MOLIT, 'COVID-19 Smart Management System').

Korea is reported to have the highest penetration rate in the world for mobile phones and for smart phones, respectively at 100% and 95% as of 2019 (Figure 18.2).[49]

In addition to the EISS, epidemiological investigators at municipal or local governments can, upon request, be given access to the DUR by the KDCA. Under 'normal' circumstances, a main use of the DUR would be to give useful information about various drugs to the general public and to those engaged in the pharmaceutical supply chain. In the context of COVID-19, the DUR could further be used for obtaining requisite tracing data.

2. *Use of QR Codes for Tracking Visitors to High-Risk Premises*

On 10 June 2020, shortly after the 2020 amendment to the CDPCA came into force, Korea further launched a QR code-based electronic visitors' log system to track visitors to certain designated types of high-risk premises such as restaurants, fitness centers, karaoke bars, and nightclubs. This system was deployed with the help of two large Internet platform companies, Naver and Kakao, and of mobile carriers through an app called Pass (Figure 18.3).

With this system in place, for instance, a visitor to a restaurant must get an ephemeral QR code pattern from a website or mobile app provided by the Internet platform companies or mobile carriers, and have the pattern scanned using an infrared dongle device maintained by the restaurant, typically at the entrance.[50] That way, QR code-based electronic visitor lists are generated and maintained for these premises (KI-Pass). Maintaining this tracking system could, however, raise concerns over privacy or surveillance. In order to address these concerns, identifying information about the visitors is kept separately from the information about individual business premises. More details about this bifurcated system are provided in Sub-section IV 2.

[49] Pew Research Center, 'Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally' (*Pew research*, 5 February 2019), www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/.

[50] MOHW, 'Guidance on the Use of Electronic Entry Lists (for Visitors and Managers)' (NCOV, 10 June 2020), http://ncov.mohw.go.kr/shBoardView.do?brdId=2&brdGubun=25&ncvContSeq=2603 (hereafter MOHW, Guidance on the Use of Electronic Entry Lists).

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

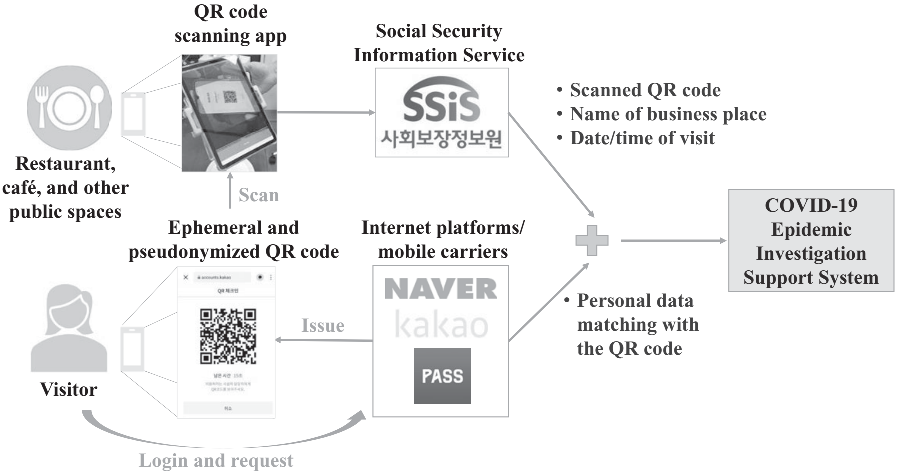
QR code scanning app
Social Security Information Service
SSiS 사회보장정보원
• Scanned QR code
• Name of business place
• Date/time of visit
Restaurant, café, and other public spaces
Scan
Ephemeral and pseudonymized QR code
Internet platforms/ mobile carriers
NAVER
kakao
PASS
COVID-19 Epidemic Investigation Support System
• Personal data matching with the QR code
Issue
Visitor
Login and request

FIGURE 18.3 The KI-Pass, a QR code-based electronic visitor booking system
Note: Naver Corporation, 'QR Check-In' (*NAVER*, 2020) https://m.help.naver.com/support/contents.

3. *Public Disclosure of the Routes of Confirmed Cases*

Routes of confirmed cases are disclosed on the websites of the relevant municipal and/or local governments, in a text or tabular form. No enhanced technology is used for the disclosure. The disclosed information is also sent to mobile phones held by nearby residents as an emergency alert message in order to alert them of the possible exposure and risks.

4. *Use of GPS Tracking Technology and Geographic Information System (GIS) for Quarantine Monitoring*

The CDPCA also grants authorization for quarantine measures to government agencies. Thus, a 14-day quarantine requirement was introduced for (1) individuals who are deemed to have been in close proximity to confirmed cases[51] and (2) individuals who arrive from certain high-risk foreign countries.[52] To monitor compliance, those who are under quarantine are required to install and run a mobile app called the 'Self-Quarantine Safety Protection App' developed by the Ministry of the Interior and Safety. The app enables officials at competent local governments to track GPS data from smart devices held by those quarantined on a real-time basis, through the GIS, in order to check and confirm whether they have remained in their places of quarantine. Also, quarantined individuals are expected to use the app to report symptoms, if any, twice a day (Figure 18.4).

IV. FLOW OF DATA

In a nutshell, developing and deploying a tracing system is about gathering and analyzing data. While using the collected data for epidemiological purposes could be justified on the basis of public policy reasons, legitimate concerns over surveillance and privacy could be raised at the

[51] Implemented from 23 February 2020.
[52] Expanded to all countries as of 1 April 2020.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

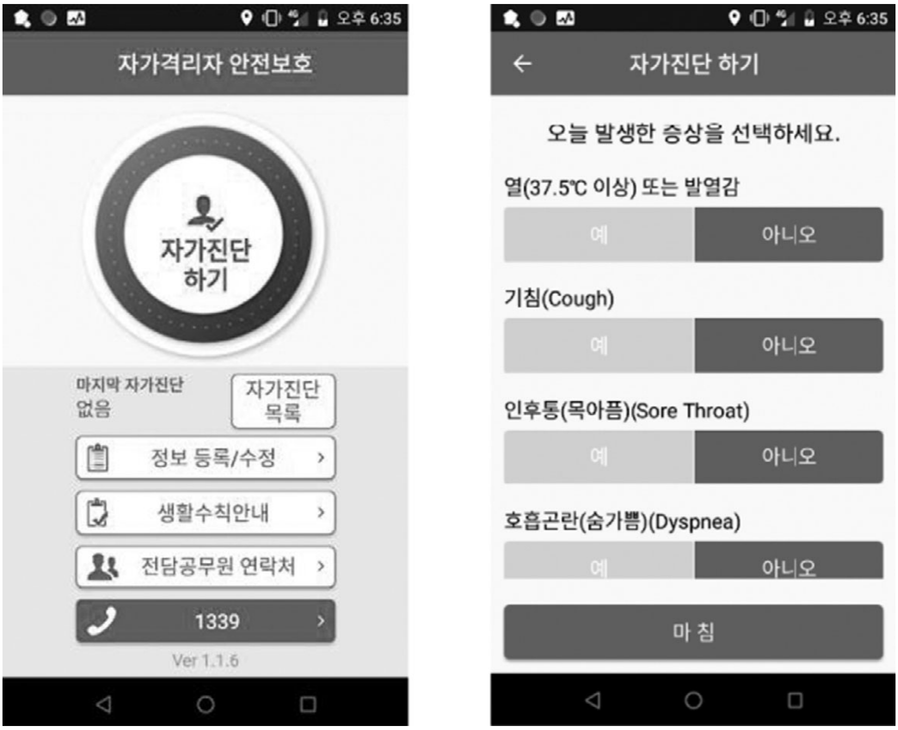

FIGURE 18.4 User interface of the Self-Quarantine App
Note: Google Play Store and Ministry of the Interior and Safety, Self-Quarantine Safety Protection App, https://play.google.com/store/apps/

same time. As such, it is imperative to consider provenance and governance of various types of data. A starting point for doing this would be to analyze the flow of data, to which we now turn.

1. *Centralized Contact Tracing*

Personal data including geolocation data of an individual flows within the EISS in the following steps: (i) the KDCA or municipal and/or local governments make a request; (ii) the police and/or the CREFIA give clearances to the transfer of mobile base station data and/or credit card transaction data, respectively; (iii) mobile carriers and/or credit card companies provide data as requested; (iv) epidemiological investigators review and analyze data pertaining to confirmed cases; (v) the investigators verify and obtain further information through interviews with confirmed cases; (vi) the investigators further conduct epidemiological network analysis and identify epidemiological links regarding the spread of COVID-19; and (vii) the KDCA and municipal and/or local governments receive relevant data and implement necessary measures such as quarantine or the disinfection or shutdown of premises where confirmed individuals visited.[53]

[53] MOLIT, 'COVID-19 Smart Management System (SMS) <Formally Named 'Epidemic Investigation Support System (EISS)'>' (*MOLIT*, 6 December 2020) https://smartcity.go.kr/2020/06/12/%ec%bd%94%eb%a1%9c%eb%82%9819-%ec%97%ad%ed%95%99%ec%a1%b0%ec%82%ac-%ec%a7%80%ec%9b%90%ec%8b%9c%ec%8a%a4%ed%85%9c-%ec%84%a4%eb%aa%85%ec%9e%90%eb%a3%8c-%eb%b0%8f-qa/ (hereafter MOLIT, 'COVID-19 Smart Management System').

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

In the whole process, mobile base station data plays a crucial role for tracing purposes. Mobile base station data contains the names and phone numbers of the individuals who were near a specific base station. Exact location data were not collected, although collecting such data would have been technically feasible through triangulation using latitude or longitude data. However, as mobile base stations are installed at an interval of 50 to 100 meters in a downtown of a densely populated city such as Seoul, base station data can be considered precise enough for the purpose of identifying those who stayed near a confirmed case. At the same time, because the geographic coverage of a base station could be rather broad, there could be an issue of over-inclusion, with implications on privacy.

2. *QR Code Tracking*

An outbreak in May 2020 was investigated and found to have an epidemiological relationship to a night club located in the Itaewon district, in Seoul. When this outbreak became serious, efforts were made to locate the individuals affected and to conduct interviews so that further preventative measures could be deployed. However, only 41.0% of individuals, (i.e., 2,032 out of 4,961 individuals), could be contacted by epidemiological investigators over the phone.[54] This was mainly due to the fact that the visitor list was hand-written by the visitors themselves and that sexual minorities who visited the club wrote down false identifies and/or phone numbers for fear of being forced to reveal their sexual orientations. This inability to contact a larger number of visitors to a particular premise reinforced the view that paper visitor lists should be substituted, where possible, with electronic visitor lists, so that the accuracy of the information contained in the visitor lists can be all but guaranteed.

This hastened the development of a QR code-based electronic visitor list system, which was deployed on 10 June 2020.[55] When a visitor has his or her QR code scanned by an infrared dongle device installed at a business premise, the manager of the business premise does not collect any personal data, other than the code itself. Under the system deployed in Korea, visitor identification information is held by the issuers of QR codes only, unless a need arises to confirm the identity for epidemiological purposes. Specifically, one of the three private entities which issue QR codes holds visitor identification information: Internet platform companies Kakao and Naver and mobile carriers who jointly developed the app named Pass. Data directly related to business premises are held by the Social Security Information Service (SSIS). That is, the SSIS collects the following data: the name of the business premise, time of entry, and encrypted QR codes. The SSIS does not hold any personally identifiable data in this context.[56] That way, relevant data are kept separately, and a bifurcated system is maintained. When a report is made that a visitor to a business premise is confirmed positive, the bifurcated datasets are then combined on a need basis in order to retrieve the relevant contact information, which is transmitted to the EISS. The transmitted information is then used by the KDCA and municipal and/or local governments for epidemiological investigations. The data generated by QR-code scanning is automatically erased after four weeks.[57]

[54] MOHW, Guidance on the Use of Electronic Entry Lists (n 50).

[55] Ibid.

[56] Ibid.

[57] Ibid.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

TABLE 18.1. *11 January 2021 Disclosure of the local government of Gwanak-gu, Seoul*[58] *(case numbers redacted)*

□ Status of Case No. ****
- Source of Infection: Presumably infected from a family member
- Confirmed positive on 11 January.

□ Status of Case No. ****
- Source of Infection: Presumably infected from a family member
- Confirmed positive on 11 January.

□ Status of Case No. ****
- Source of Infection: Presumably infected from a confirmed case at the same company in a different region
- Confirmed positive on 11 January.

□ Status of Case No. ****
- Source of Infection: Under investigation
- Confirmed positive on 11 January.

□ Status of Case No. ****
- Source of Infection: Under investigation
- Confirmed positive on 11 January.

□ Status of Case No. ****
- Source of Infection: Under investigation
- Confirmed positive on 11 January.

※ Measures
- Will transfer confirmed cases to the government-designated hospitals
- Will disinfect the residence and neighboring areas of confirmed cases
- Investigating visited places and close contacts

3. *Public Disclosure of the Routes of Confirmed Cases*

As explained above, municipal and/or local governments receive geolocation data and card transaction data from the EISS and disclose a part of the data to the general public. At an earlier stage of the COVID-19 outbreak, very detailed routes of confirmed cases were disclosed to the public. These disclosures did not include the names or other personally identifiable information of the confirmed individuals. What was revealed typically included a pseudonym or part of the full name of the infected individual as well as sex and age. In addition, vocation and/or area of residence was often disclosed. Although directly identifiable personal information was not disclosed, sometimes simple investigation and profiling would enable re-identification or reveal personal details. Certain individuals indeed became subject to public ridicule, after their identities were revealed. Debates on privacy followed, and the KDCA revised its guidelines about public disclosure of information on contact tracing. As a result, municipal and/or local governments are now disclosing much more concise information focusing on locations and premises rather than on an individuals' itinerary. Also, disclosure information is deleted after fourteen days following disclosure. One of the examples is as shown in *Table 18.1*.

4. *Quarantine Monitoring*

The self-quarantine app collects GPS data from mobile devices and shares it with the GIS, so that an official at the local government can monitor the location of a quarantined individual on a real-time basis.

[58] Gwanak-gu Local Government, 'The Statuses and Routes of COVID-19 Confirmed Cases' (*Gwanak*, 11 January 2021) www.gwanak.go.kr/site/health/ex/bbs/View.do?cbIdx=587&bcIdx=117494&parentSeq=117494.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

V. DATA FLOW AND DATA GOVERNANCE

Collecting relevant data on a near real-time basis is crucial in order to contain the spread of COVID-19. At the same time, data collection immediately raises privacy concerns. As such, a delicate balance must be struck between conducting effective epidemiological investigations and protecting the privacy of individuals. Delineating the precise flow and provenance of collected data will give implications as to how the delicate balance can be struck and maintained. The following section gives some explanations as to what transpired in Korea in this respect.

1. *Centralized Contact Tracing (including QR Code Tracking)*

An early response is critical to contain the spread of highly infectious diseases such as COVID-19. In turn, the effectiveness of such a response relies on the prompt collection and sharing of accurate data about confirmed cases and close contacts. Manual epidemiological tracing has serious limitations. It takes time for human investigators to conduct manual tracing, causing delays. Also, manual tracing is vulnerable to faulty memory or deception on the part of interviewees, resulting in inaccurate epidemiological reports.

In response to the rapid spread of COVID-19, Korea chose to integrate such human efforts with a technology-driven system of data processing. For example, a prompt compilation of geolocation data has been a crucial enabling factor in Korea's contact tracing strategy. The EISS, which makes use of the smart city technology, allowed public health authorities to efficiently allocate valuable resources. With the assistance of technology, for instance, epidemiological investigators were able to conduct tracing in a more effective and efficient manner.

At the same time, questions were raised whether the centralized contact tracing model adopted in Korea was overly intrusive, even harmful to fundamental freedoms constituting the very cornerstones of a democratic society. The collection of data has sometimes been equated to mass surveillance, raising privacy concerns as well. This line of criticism would have a clear merit, if certain other alternative tracing systems show the same or even higher level of efficacy, while collecting less granular and less detailed personal data.

The problem, however, is that, while a decentralized system such as the Bluetooth-based approach is in general better in protecting privacy, it has its own shortcomings that are yet to be solved. First, a tracing app needs to attain a certain penetration rate, in other words, the proportion of active users of the mobile app among the whole population should be sufficiently high for a tracing system to function properly. In order to achieve the so-called digital herd immunity this penetration rate should be fairly high – sometimes set at 60 to 75%.[59] To date, most countries have failed to achieve this level of penetration rate, due to, among other things, low levels of smartphone penetration rates. Second, Bluetooth-based proximity tracing may not work effectively in crowded areas that are in fact prone to experience explosive outbreaks of infectious diseases such as COVID-19. Third, decentralized models generally do not allow for human-in-the-loop based verification and tend to show excessively high false positives.[60] Fourth, iOS does not allow third-party apps running in the background to function properly in order to

[59] V B Bulchandani and others, 'Digital Herd Immunity and COVID-19' (2020) https://arxiv.org/pdf/2004.07237.pdf.

[60] J Bay and others, 'BlueTrace: A Privacy-Preserving Protocol for Community-Driven Contact Tracing across Borders' (*Government Technology Agency*, 9 April 2020) https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

broadcast Bluetooth signals, unless the AGEN system is deployed.[61] Fifth, for a fully decentralized approach, there would be no informational benefits to public health authorities because relevant information simply does not flow to public health authorities. While this could be beneficial in maintaining the privacy interests of citizens, at the same time, precious opportunities for gaining epidemiological data would be lost. Lastly and perhaps most fundamentally, the decentralized approach has to rely on good-faith cooperation by confirmed individuals. That is, the approach would not work unless confirmed individuals make voluntary reports and, as such, this approach exhibits a similar problem as in a manual tracing method.

This is not to say that a centralized model would always be preferable. While a decentralized approach may not lead to a herd immunity, it could nonetheless play a complementary role in containing the spread of COVID-19, particularly in densely populated areas such as city centers and on university campuses. Thus, as a general matter, a centralized approach and a decentralized approach each have their own strengths and limitations. For a centralized approach, its main strengths would include: immediate availability undeterred by the penetration levels; effective response to mass infection; no compatibility concerns; and most importantly, impactful contribution to epidemiological investigations.

In the case of Korea, there is no denying that contact tracing and other tracking mechanisms were a crucial component in the whole apparatus dealing with daunting challenges caused by COVID-19. Also, overall, Korean society at large complied with the requirements imposed by these tracking mechanisms, without raising serious privacy concerns. If we go one step further, there could be various viewpoints and reactions as to why Korean citizens in general complied with the measures adopted by the government.

In terms of data protection, the PIPA was enacted in 2011 and earlier statutes also contained various elements of data protection. Separately, the Constitutional Court of Korea, in 2005, declared that the right to data protection is a constitutional right. As such, Korean citizens are in general well aware of the value of data protection in modern society. In adopting technology-based contact tracing mechanisms and complying with the requirements associated with such contact tracing mechanisms, it can be said that the Korean society as a whole made a wide-ranging value judgement about privacy, public health, and other social and legal values. Among other things, citizens exhibited a striking willingness to cooperate with authorities in their efforts to collect epidemiological data including geolocation data, which can be traced back to their previous experience with the MERS outbreak. Utilizing new technologies for epidemiological purposes was perhaps not much of an additional concern as, in relative terms, many Koreans are at ease with adapting to new technological environments.

This does not mean, however, that the data collection was without controversy. On the contrary, several activist groups joined forces and filed a constitutional petition seeking the Constitutional Court of Korea's decision regarding the constitutionality of contact tracing mechanisms.[62] More specifically, the petition challenges the constitutionality of the CDPCA provisions which enabled contact tracing in the first place.[63] It also views the government's collection of mobile base station data based on these provisions unconstitutional, in particular pointing to the collection of data about the visitors at a night club in the Itaewon area during an outbreak, as doing so violates, among other things, the constitutional right to self-determination of personal

[61] J Taylor, 'Covidsafe App Is Not Working Properly on iPhones, Authorities Admit' (*The Guardian*, 6 May 2020), www.theguardian.com/world/2020/may/06/covidsafe-app-is-not-working-properly-on-iphones-authorities-admit.

[62] Constitutional Court of Korea, Case Ref. 2020 *Heonma* 1028 (filed on 29 July 2020, pending).

[63] CDPCA, Articles 2-15, 76-2.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

data.[64] This petition grounds itself on the Court's 2018 decision that held the collection of the identities of mobile subscribers that accessed a particular base station in the course of criminal investigation unconstitutional.[65] Regardless of the outcome of this case, the scope of geolocation data might need to be adjusted to balance epidemiological benefits with privacy.

In the case of QR codes, the bifurcated approach perhaps helps mitigate security risks and privacy concerns, by separating personally identifiable data from visitor logs and by combining them only when necessary for epidemiological investigation. Also, while both a paper form for visitor logs and a QR-code based electronic log system are usually available at business premises, the general public appears to prefer the QR code-based electronic visitor log system. Part of the reason would be the trustworthiness of the QR-code system. That is, while there is virtually no concern over possibilities of data breach for a QR code-based electronic visitor log system, a paper visitor list could be vulnerable to illegal leakage by employees of business premises or by subsequent visitors.[66]

About the contact tracing mechanism in general, there could be a concern over possibilities of 'function creep.' The concern is that, while conducting contact tracing under the current extraordinary circumstances of COVID-19 could be justified, after the pandemic is over, the government may be tempted to use this mechanism for surveillance purposes. In the case of Korea, there are two built-in safeguards against this from happening. First, data collection for epidemiological purposes is under the sole purview of the KDCA and the relevant databases are maintained by the KDCA as well. This means that, even if the government is tempted to divert the system for different purposes, doing so would be a cumbersome procedure simply because the system is maintained and held by a single public health agency with a narrow public health mandate. Second, the KDCA's authority for the current data collection is, for the most part, derived from statutory provisions contained in the CDPCA and not from the PIPA, a general data protection statute. After the pandemic is over, the KDCA or any other government agencies would require a separate statutory rationale in order to collect data.

Compared to the Korean government's active role in utilizing technology to cope with the COVID-19 pandemic, public-private collaboration based on the sharing of public data and the use of open APIs (application programming interfaces) in Korea has somewhat lagged. There have been recent cases of meaningful contributions from the private sector, however. An example would be a collaborative dataset sourced from public disclosures, which has been actively used for visualization purposes and also for machine learning training purposes.[67]

2. *Public Disclosure of the Routes of Confirmed Cases*

Unlike contact tracing itself, which was generally accepted as a necessary trade-off between privacy and public health in facing the pandemic, the public disclosure of the routes of

[64] Joint Representatives for the Petition for the Decision that Holds COVID-19 Mobile Base Station Data Processing Unconstitutional, 'Petition' (*Opennet*, 29 July 2020) https://opennet.or.kr/18515.

[65] Constitutional Court of Korea, Case Ref. 2012 *Heonma* 538 (28 June 2018).

[66] MOHW, 'Guidance on the Use of Electronic Entry Lists' (n 50).

[67] J Kim and others, 'Data Science for COVID-19 (DS4C)' (*Kaggle*, 2020), www.kaggle.com/kimjihoo/coronavirusdataset/data. Another example is SK Telecom's support of an AI-based teleconference system for quarantine monitoring: ZDNET, 'SKT Reducing COVID-19 Monitoring Workloads up to 85% Using AI' (*ZDNET*, 25 June 2020), https://zdnet.co.kr/view/?no=20200625092228. Refer to CHOSUNBIZ, 'Taking up to 30,000 Calls a Day When 2,000 was a Challenge Due to the Coronavirus … "Thank you AI"' (*ChosunBiz*, 24 May 2020), https://biz.chosun.com/site/data/html_dir/2020/05/23/2020052301886.html for other Korean examples of private initiatives utilizing AI related to the COVID-19 pandemic.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

confirmed cases quickly became controversial due to privacy concerns. Such public disclosures were, in fact, another policy response from the experiences of the MERS outbreak. That is, during the MERS outbreak, there was great demand for transparency and some argued that the lack of transparency impeded an effective response. However, with the onset of the COVID-19 outbreak, the pendulum swung in the other direction. Not just the detailed nature but also the uneven scope and granularity of disclosures among the KCDA and the numerous municipal and local authorities caused confusion, in particular during the initial phase. Concerns were not limited to the invasion of privacy. Private businesses, such as restaurants and shops, that were identified as part of the routes often experienced abrupt loss of business.

These concerns were encapsulated in the recommendation issued by the National Human Rights Commission (NHRC) on 9 March 2020.[68] The NHRC expressed concerns about unwanted and excessive privacy invasion as well as secondary damages such as public disdain or stigma, citing a recent survey showing that the public was even more fearful of the privacy invasion and stigma stemming from an infection than the associated health risk itself.[69] The NHRC noted that excessive public disclosure could also undermine public health efforts by dissuading those suspected of infection from voluntarily reporting their circumstances and/or getting tested for fear of privacy intrusions.[70] The NHRC further recommended that route disclosures be made in an aggregate manner focusing on locales at issue, rather than disclosing the times and places of visits at an individual level and possibly revealing personal itineraries.[71]

In response to the NHRC's recommendations, the KDCA issued its first guidelines regarding public disclosures to municipal and local governments on 14 March 2020, which limited the scope and detail of the information to be made publicly available. Specifically, the KDCA (i) limited the period of route disclosure from one day prior to the first occurrence of symptoms to the date of isolation, (ii) limited the scope of visited places and means of transportation to those spatially and temporally proximate enough to raise concerns of contagion, considering symptoms, duration of a visit, status of contacts, timing, and whether facial masks were worn, and (iii) banned the disclosure of home addresses and names of workplaces. On 12 April 2020, the KDCA further revised the guidelines. Under the revised guidelines, (i) information on routes should be taken down 14 days after the confirmed case's last contact with another individual, (ii) information on 'completion of disinfection' should be disclosed for relevant places along the disclosed routes, and (iii) the period of route disclosure should start from two days prior to the first occurrence of symptoms.[72] One complication from public disclosures of information is that, once a disclosure is made, the disclosed information is rapidly further disseminated via various social media outlets by individual users. Thus, data protection agencies have been actively sending out takedown notices to online service providers to ensure that such content is taken down following the 14-day period.

In May 2020, a spate of confirmed cases arose at a nightlife district in Itaewon, Seoul, that is frequented by persons with a specific sexual orientation. While public health authorities mounted a campaign urging prompt testing for those who could be at risk, it was ostensible

[68] NHRC, 'Statement Concerning the Excessive Disclosure of Private Information Pertaining to Confirmed COVID-19 Cases' (*NHRC*, 9 March 2020), www.humanrights.go.kr/site/program/board/basicboard/view?currentpage=2&menuid=001004002001&pagesize=10&boardtypeid=24&boardid=7605121.

[69] Ibid.

[70] Ibid.

[71] Ibid.

[72] KDCA, 'Guidance to Information Disclosure of Transit Routes of Confirmed Patients, etc.' (*KDCA*,12 April 2020), www.cdc.go.kr/board.es?mid=a20507020000&bid=0019&act=view&list_no=367087.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

that the fear of being forced to reveal sexual orientations or being socially ostracized was a significant deterring factor. In response, the Seoul Metropolitan government initiated anonymous testing from 11 May 2020, under which individuals were only asked for their phone numbers. The anonymous testing scheme expanded and began to be applied to the whole country on 13 May 2020.

After witnessing these debates, the KDCA issued further revised guidelines dated 30 June 2020. The latest guidelines provided that municipal and/or local governments should disclose the area, the type of premises visited, the trade names and addresses of these premises, the date and time of exposure, and disinfection status and that disclosures should not be made for each individual and his or her timeline but instead in the format of 'lists of locations visited.' The guidelines further stipulated not to disclose information regarding the visited places if all close contacts have been identified.[73]

Subsequently, an amendment to the CDPCA was made dated 29 September 2020 and this amendment, among others, included a provision that excludes from the scope of public disclosure the 'sex, age, and other information unrelated to the prevention of contagious disease as stipulated in the Presidential Decree.'[74] The current Presidential Decree for the CDPCA lists the name and detailed address as examples of such 'other information unrelated to the prevention of contagious disease.'[75]

The above shows the ongoing process of trial and error in search of a more refined approach which would better balance the imperatives emanating from public health concerns during a pandemic with privacy and other social values. Urgency of the situation perhaps made it imperative to implement swift measures for gathering information. While implementing swift measures is inevitable, it is also important to review the legitimacy and efficacy of these measures on an ongoing basis and to revise if needed. For instance, compared to the disclosure of precise routes profiled for each confirmed case, the disclosure of aggregated route information has proven sufficient to achieve the intended public health policy goals. As demonstrated in the *Itaewon Case*, a less privacy-intrusive alternative can also assist infection control efforts by encouraging voluntary reporting and testing.

Regarding the disclosure of the names and addresses of business premises, assuming that disinfection can effectively address contagion risks, the only benefit would be to alert other visitors and to encourage them to self-report and get tested. Therefore, if all visitors are in fact identifiable through contact tracing, the public disclosure of the type of business and the broader area of the location, rather than identifying the name of the specific business premise, would be sufficient for purposes of public health. In fact, revisions to the KDCA guidelines were made reflecting practical lessons learned throughout 2020 and provide for deletion of data that is unnecessary or no longer necessary.

3. *Quarantine Monitoring*

Human surveillance of quarantined persons is often costly, ineffective, and in many cases inevitably intrusive. The quarantine monitoring through GPS tracking has generally been

[73] KDCA, 'Guidance to Information Disclosure of Transit Routes of Confirmed Patients, etc.' (3rd ed) (30 June 2020), www.gidcc.or.kr/wp-content/uploads/2020/02/%ED%99%95%EC%A7%84%EC%9E%90_%EB%8F%99%EC%84%A0_%EB%93%B1_%EC%A0%95%EB%B3%B4%EA%B3%B5%EA%B0%9C_%EC%95%88%EB%82%B43%ED%8C%90.hwp.

[74] CDPCA, Article 34-2 (1).

[75] Presidential Decree for CDPCA, Article 22-2 (1).

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

regarded as a more effective but less intrusive substitute for the human surveillance. As such, there have not been serious privacy concerns raised about quarantine monitoring.

4. *Data Governance*

On a regulatory front, the outbreak of COVID-19 has highlighted the need for Korea's privacy and data protection authorities to be ever more vigilant during public emergencies. In February 2020, Korea undertook a major reform to its privacy and data protection laws which came into effect as of 5 August 2020. As a result of the amendments, Korea's data protection authority will be consolidated and vested in the Personal Information Protection Commission (PIPC). This reform is expected to allow the PIPC to engage in a more proactive role in balancing the rights of data subjects with public health goals and to provide clearer guidance as to what to disclose and how to de-identify when making public disclosure.

On a broader level, in terms of the flow and provenance of data, two general directions can be distinguished. One direction is from the general population to public health authorities. Data gathered and shared in this direction is mainly done in order to carry out contact tracing, to conduct epidemiological analyses, and to devise and implement public health measures. At the same time, data flows toward the other direction as well, from the government and public health authorities to the general public. What is carried out in this context is mostly public disclosures of data about confirmed cases. Doing this would presumably be helpful for purposes of enhancing transparency and giving alerts so that citizens can prepare.

Regarding both directions of data flows, there are tensions between public health purposes and privacy interests: gathering and disseminating detailed information would in general be helpful in containing the spread of COVID-19, while, at the same time, doing so could be detrimental to the protection of the privacy of citizens. Details of the tensions, however, are different between the two directions of data flows. When data flows from the general public to public health authorities, a major concern would be the possibility of surveillance. Seen from a public policy perspective, attention would thus need to be paid as to whether and how a possible concern over surveillance could be assuaged. Putting in place systematic and procedural safeguards could be helpful. On the other hand, when data flows from public health authorities to the general public, mostly in the form of public disclosures of data about confirmed cases, concerns could be raised about the privacy of citizens. A privacy concern in this context could arise due to the possibility of the revelation of unwanted or embarrassing personal details. The risk could be elevated, if there is an added motivation for a public officer to gain attention through media, by leaking a 'headline grabbing' news item. In that regard, attention may need to be paid as to what data is made available to public sector officers.

VI. LOOKING AHEAD

As the COVID-19 outbreak continues its course, new societal challenges or existing ones that are being exacerbated by the pandemic such as the digital divide, are gathering more attention in Korea and elsewhere. Heightened concerns of ostracization or stigma directed to minority groups, the vulnerability of health and other essential workers that face constant exposure to infections, and children from underprivileged families that are ill equipped for remote learning are but a few examples. The *Itaewon case*, discussed earlier, has demonstrated the need for authorities to be prepared to promptly address concerns of prejudice against minority groups in the Korean society. The same should be said regarding the acute health and economic

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press

disadvantages faced by the underprivileged during a pandemic. Yet, the societal challenges in the post-COVID-19 era, with its trend towards remote work, education, and economic activity will likely call for more long-term and fundamental solutions.

In this regard, the active use and application of AI and data analytics, as well as a robust ethical review concerning its governance, is expected to be critical in achieving the social reforms required to cope with the challenges of the present and coming future. In doing so, a prerequisite would be to compile and draw a 'data map' so that data's flow and provenance can systematically be understood. With such understanding, further discussions could perhaps be made regarding appropriate levels of granularity for data disclosures and different levels of access control and other safeguards, depending on specific needs or policy goals. Korea's experience dealing with COVID-19 can provide a valuable lesson in this context.

https://doi.org/10.1017/9781009207898.024 Published online by Cambridge University Press