Editors: Khaled El Emam, kelemam@cheo.on.ca | Katrine Evans, k.evans@haymanlawyers.co.nz

Privacy in the Time of COVID-19: Divergent Paths for Contact Tracing and Route-Disclosure Mechanisms in South Korea

Sangchul Park | Seoul National University
Gina J. Choi | Seoul National University and University of California, Berkeley
Haksoo Ko | Seoul National University and SNU Artificial Intelligence Institute

In response to COVID-19, Korea has implemented digital contact tracing and patient route disclosure schemes. While the former has been embraced more willingly, the latter has been shunned due to privacy concerns, demonstrating that privacy is highly dynamic and is of contextual value.

Thus far, South Korea (i.e., Korea) has confronted three waves of COVID-19 since the first case was confirmed on 20 January 2020 (see Figure 1). Compared to other countries, Korea has been able to keep the number of confirmed cases at a manageable level.

In addition to the medical systems and supply chains that are in place for personal protective equipment (such as face masks or respirators) and test kits (such as RT-PCRs), various nonpharmaceutical interventions (NPIs) have played a significant role in tackling the pandemic. The main piece of legislation that regulates Korea's use of NPIs is the Contagious Disease Prevention and Control Act (CDPCA).[1]

Although NPIs are a useful tool to safeguard public health, they require citizens to sacrifice civil liberties. For instance, placing immigrants or those in close contact with confirmed patients in quarantine [(art. 42(2)(i), CDPCA)] restricts those individuals' freedom of movement. An administrative order for social distancing imposes a restriction on freedom of association [(art. 49(1)(ii), CDPCA)], albeit not as restrictive as shelter-in-home or lockdown measures.[2]

This article discusses the NPIs that have privacy implications, with a focus on digital contact tracing and patient route disclosures. There are other examples of NPIs as well, including a digital quarantine-monitoring system, implemented through a GPS tracking mobile app and the Geographic Information System [(art. 42(2)(ii), CDPCA)].[2] Focusing on contact tracing and route disclosures, this article inquires as to why, when confronting COVID-19, certain NPIs have been embraced more willingly in Korea, while other NPIs have been shunned due to privacy concerns.

Digital Object Identifier 10.1109/MSEC.2021.3066024
Date of current version: 14 May 2021

Contact Tracing

Legal Basis and Implementation

In response to the outbreak of the Middle East Respiratory Syndrome (MERS) in 2015, Korean statutory provisions regarding contact tracing have evolved to encompass the processing of data pertaining to confirmed cases as well as those data pertaining to suspected cases [(art. 76-2(1) and (2), CDPCA)].[1] These provisions stand out as a striking exception to Korea's stringent legal regime for data protection.[1] The data that can be processed under these provisions include geolocation data, personal identification data, medical and prescription records, immigration records, payment card transaction data, transit pass records, and closed-circuit television footage.[1] Korea Disease Control and Prevention Agency (KDCA) is authorized to collect those data and share them with central, municipal, or local governments; national health insurance agencies; and health-care professionals and their associations [(art. 76-2(3), CDPCA)].[1]

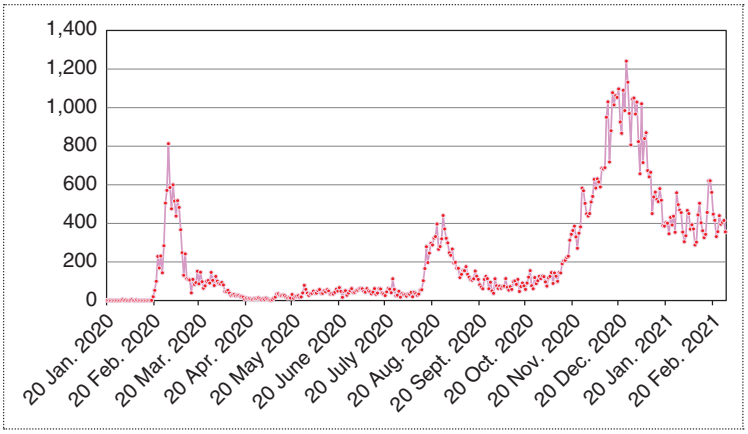

Figure 1. The daily, new confirmed cases of COVID-19 in Korea.[4]

As a result of the COVID-19 pandemic, the Korean government launched a digital contact-tracing system [known as the *Epidemic Investigation Support System* (*EISS*)] in March 2020 (see Figure 2).[1] The EISS was swiftly remodeled from an existing smart city data hub system that several municipal governments had already developed for smart city projects (pursued in accordance with the Act on the Construction of Smart Cities and Industry Promotion).[2] The EISS collects data pertaining to confirmed cases and shares that data with epidemiological investigators at the KDCA and with municipal/local governments.[1] The data include 1) credit card transaction records (provided by credit card companies with clearance from the Credit Finance Association) and 2) mobile base station data (provided by mobile carriers with clearance from law enforcement agencies).[2] The latter reportedly does not include GPS or cell tower triangulation data but instead includes less-accurate cell ID positioning data (i.e., data about individuals who gave or received calls via a specific cell tower during a specified time period).

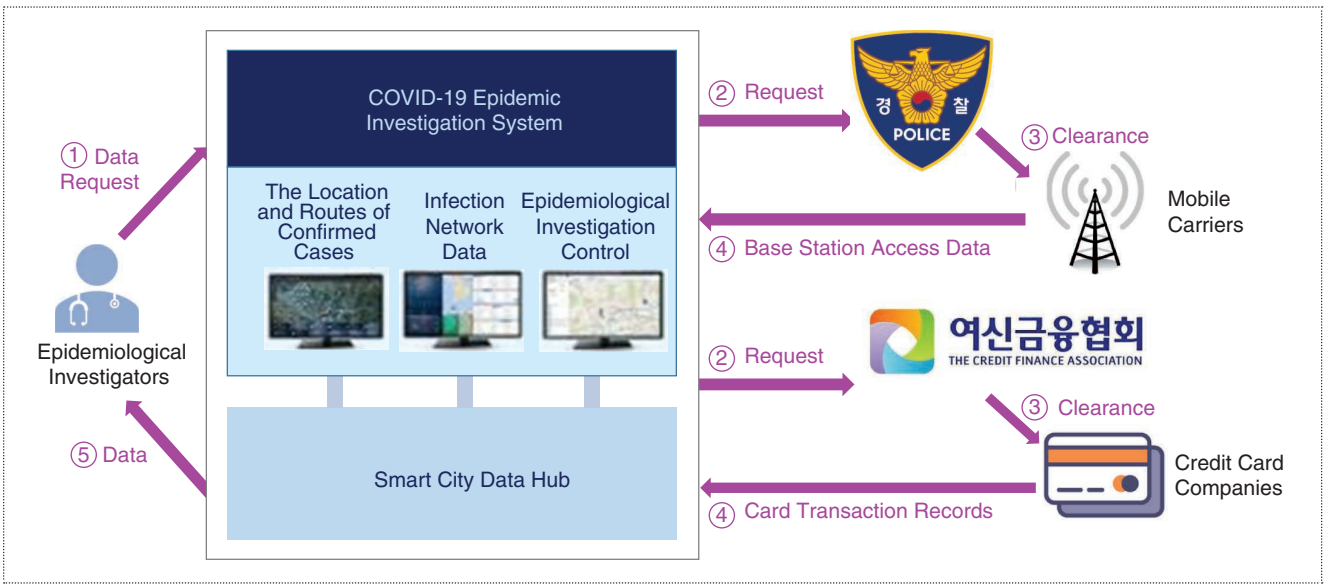

Figure 2. The COVID-19 EISS.[2,5]

In addition, health-care institutions can access the Drug Utilization Review (DUR), a separate system maintained by the Health Insurance Review and Assessment Service. Through the DUR, medical and prescription records as well as immigration records pertaining to patients can be obtained.

Progress

Considering what has transpired in many countries during the COVID-19 pandemic, the implementation of a centralized contact-tracing scheme appears to be uncommon. Many Western countries have opted for decentralized or privacy-preserving proximity-tracing schemes based on Bluetooth Low Energy.[2] One such well-known scheme is Apple/Google's Exposure Notification application programming interface (AGEN), which is reported to have been embedded in the COVID-19 apps of several European countries, several U.S. states, and Japan.[2] AGEN is designed to push alerts to users who were in proximity to confirmed patients, while maintaining user anonymity. A decentralized system such as AGEN has limitations in terms of its utility for making contributions to epidemiological investigations.

To further aid epidemiological-investigative processes, other countries have adopted a partially centralized approach, with France utilizing the Pan-European Privacy-Preserving Proximity Tracing (i.e., PEPP-PT) and Singapore and Australia employing BlueTrace protocols.[2] Under this approach, the smart device held by a confirmed case sends, to a server database, not only his or her ephemeral ID but also the IDs of those in close proximity.[2] However, both fully decentralized and partially centralized approaches allow users to avoid tracking by erasing, deactivating, or simply refusing to download proximity-tracing apps. This makes it challenging for the apps to acquire the requisite penetration rate to work effectively.[2]

The centralized approach, reportedly adopted in a relatively small number of countries including Korea, Israel, and Vietnam, has a different role from a decentralized Bluetooth scheme. As its full name suggests, Korea's EISS is designed mainly to provide support to interview-based epidemiological investigations by assisting investigators in their work to verify interviewees' responses about their whereabouts.

The EISS collects data pertaining to confirmed cases and shares that data with epidemiological investigators at the KDCA and with municipal/local governments.

Regarding the centralized contact-tracing scheme adopted in Korea, it appears that the public has generally embraced—or at least acquiesced to—the need for such a system. Kim et al.'s (2021) survey of 188 Koreans between 25 June and 10 July 2020

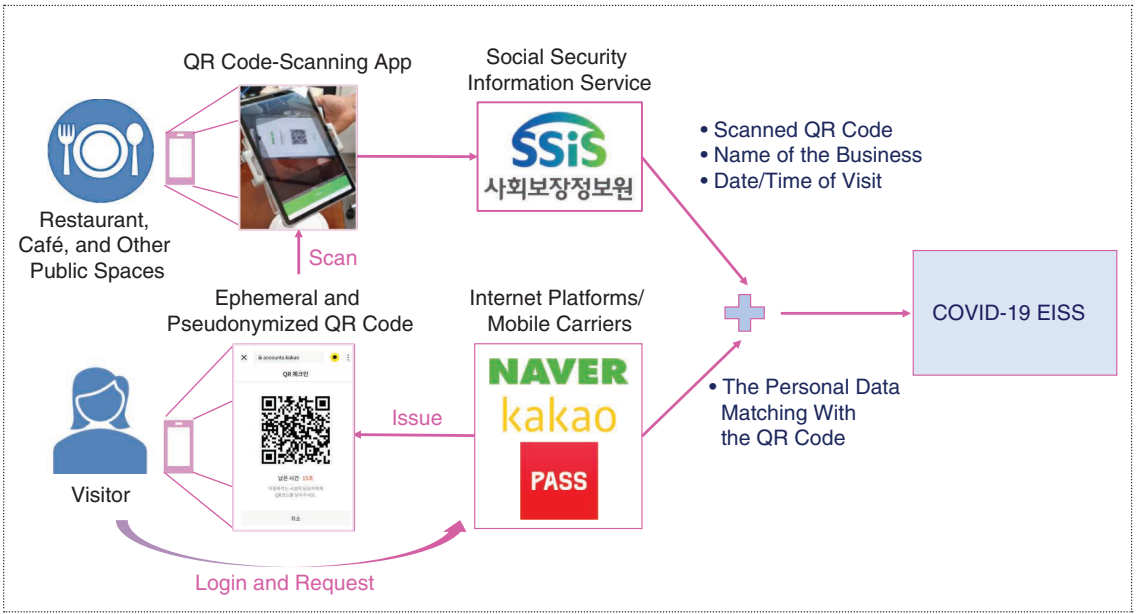

Figure 3. The KI-Pass, a QR code-based electronic visitor booking system.[6]

found the disapproval and approval rates for the systems to be 9 and 81%, respectively, for compiling credit card transaction records and 10 and 78%, respectively, for compiling mobile phone data.[3] A high level of public support in Korea for contact tracing may have arisen from the perception that, in facing the pandemic, deploying timely measures for quarantining, testing, and isolation is crucial. In addition, the fact that the EISS is derived from a smart city project could have afforded the system a heightened sense of public trust because the EISS uses a separate network that is different and disjointed from the network that government agencies utilize for routine administrative matters.

perhaps served as an impetus for the Korean government to develop and introduce the QR code-based, electronic visitor booking system KI-Pass on 10 June 2020 [(art. 49(1)(ii-ii), CDPCA) (see Figure 3)]. The managers at restaurants, cafés, fitness centers, karaoke bars, nightclubs, and other high-risk premises now must ask visitors to produce an ephemeral QR code (using mobile apps developed by Internet platform companies such as Kakao and Naver or the Pass app, which was jointly developed by mobile carriers) and have the QR code scanned by either an infrared dongle or smart device (with a QR scanner app) installed at these business premises.[6]

The KI-Pass system separates ephemeral and pseudonymized QR codes from personally identifiable data.

This does not mean, however, that there have been no privacy controversies. For instance, several nongovernmental organizations have filed constitutional petitions with the Korea Constitutional Court to challenge the constitutionality of contact-tracing schemes. In particular, they assert that 1) the CDPCA provisions that have enabled contact tracing (arts. 2(15-2) and 76-2) are, in themselves, unconstitutional and that 2) the government's collection of mobile base station data based on these statutory provisions is also unconstitutional. This petition is based on the Korean Constitutional Court's 2018 decision in which the Court held that a provision enabling the investigation of the identity of mobile subscribers that accessed a single base station is unconstitutional.

Despite this controversy, public support for contact tracing has

To alleviate privacy concerns, the Korean government has designed a bifurcated system. The KI-Pass system separates ephemeral and pseudonymized QR codes from personally identifiable data.[6] Thus, a manager at a business premise collects only a visitor's time of entry and pseudonymized QR codes (without collecting any further data pertaining to the visitor) and forwards that data (along with the name of the business premise) to the Social Security Information Service.[6] Internet platform companies or mobile carriers maintain the personal identification data that matches the QR code.[6] The relevant parts of these data sets are only combined and transmitted to the EISS once a visitor is confirmed positive for COVID-19.[6] The transmitted data are then used by the KDCA and by municipal/local governments for epidemiological investigations. After four weeks, the data are erased.[6]

Route Disclosures

Legal Basis and Implementation

At the outbreak of a serious epidemic, the KDCA and municipal/local governments have statutory obligations to make the following information available on the Internet or through a press release: 1) the travel paths and means of transportation for confirmed patients, 2) the medical institutions which treated these patients, and 3) the status of those in close contact with the patients [(art. 34-2(1), CDPCA)].[1] An appeal can be made if the disclosed information is incorrect.[1]

This route-disclosure provision was hurriedly added to the CDPCA amid the 2015 MERS crisis. On 5 June 2015, only two weeks after the first MERS case was confirmed, a legislative bill was submitted to Korea's legislature. The bill passed the legislature on 25 June 2015, only 20 days after its filing.

Immediately following the outbreak of COVID-19 in Korea in 2020, the route-disclosure program was reactivated. During the disclosure process, names and other personally identifiable information are removed. Occasionally, however, the age, gender, home address, and workplace of certain individuals were disclosed. Furthermore, the uneven scope and granularity of disclosures among different layers of central, municipal, and local authorities caused confusion.[1] Municipal and local governments started to dispatch text messages to the public to alert them to the occurrence of confirmed cases within their localities. Doxing (more formally, reidentification attacks including linkage or inference attacks) often took place. Concerns were raised about an invasion of privacy. Further, private

businesses, such as restaurants and shops, whose names were identified and included in the disclosed route data, often experienced abrupt losses of business.[1]

Progress

Unlike contact tracing, public disclosures of the travel paths and contacts of confirmed cases have often resulted in controversies, mainly due to privacy concerns.[1] The National Human Rights Commission (NHRC) issued a recommendation dated 9 March 2020, expressing concerns about privacy invasions, public disdain, or social stigma.[1] The NHRC cited a survey showing that the public was more fearful of the disclosure than of the associated health risk.[2] The NHRC warned that excessive public disclosures could also undermine public health by dissuading those suspected of infection from voluntarily reporting their circumstances and/or getting tested.[2] The NHRC further recommended that route disclosures be made in an aggregate manner focusing on the locales at issue, rather than by revealing personal itineraries.[2]

Following the NHRC's recommendations, the Korea Centers for Disease Control and Prevention (KCDC) (renamed the KDCA in September 2020) issued a guideline on disclosures on 14 March 2020. The guideline suggested limiting the period of time for route disclosure from one day prior to the first occurrence of symptoms to the date of isolation (later revised to two days); limiting the scope of disclosures about the places the person visited and his or her means of transportation to those spatially and temporally proximate enough to raise concerns of contagion; taking into account the symptoms, duration of a visit, status of contacts, timing, and whether face masks were worn; and banning the disclosure of home addresses and names of workplaces.[2]

On 12 April 2020, the KCDC further revised the guideline. Under the guideline, the information on routes should be removed from public disclosure 14 days after a confirmed patient's last contact with another individual, and information on the "completion of disinfection" should be disclosed for relevant places along the disclosed routes.[2]

Around May 2020, the rates of COVID-19 infection surged in Seoul's Itaewon nightlife district, which is popular among the gay community.[2] Although public health authorities mounted a campaign urging prompt testing, it was obvious that individuals' fear of being forced to reveal their sexual orientations was a significant deterring factor against obtaining testing.[2] In response to this, the Seoul Metropolitan Government changed course and initiated anonymous testing beginning on 11 May 2020, under which examinees were asked for only their phone numbers.[2] The authorities began applying the anonymous testing scheme nationwide on 13 May 2020.[2]

Meanwhile, the KCDC prepared and issued a further-revised guideline dated 30 June 2020. The guideline limited the scope of public disclosure to the area, type, trade name, and addresses of premises visited; the date and time of exposure; and the disinfection status. The guideline further provided that disclosures should not be made at an individual level based on an individual's timeline and itineraries and that disclosures should instead be made in the format of "lists of locations visited." Moreover, the guideline stipulated not to disclose information regarding the places an individual visited if all of his or her close contacts have been reported.

Subsequently, certain statutory provisions of the CDPCA were amended on 29 September 2020 to exclude a confirmed patient's name, gender, age, and detailed home address from the scope of public disclosure [art. 34-2(1), CDPCA; art. 22-2(1), Presidential Decree for CDPCA].

As a result of these lengthy debates and controversies, the information contained in route disclosures has become nearly anonymized, which is in sharp contrast with what was disclosed at the outset of the pandemic. Kim et al.'s (2021) aforementioned survey found that the disapproval and approval rates for route disclosures in Korea were 28 and 59%, respectively, regarding the inclusion of age and gender in disclosures and 9 and 79%, respectively, regarding the exclusion of age and gender in disclosures.[3] The survey, despite its limitations, reveals clues about people's attitudes, which have instigated changes in the public-disclosure regime thus far.

The intricate relationship between contact tracing and route-disclosure schemes appears to demonstrate that privacy is highly dynamic and is of contextual value, irreducible to all-or-nothing inquiries.

The intricate relationship between contact tracing and route-disclosure schemes appears to demonstrate that privacy is highly dynamic and is of contextual value, irreducible to all-or-nothing inquiries.

There have been three crucial differences in the risks, benefits, and public trust associated with these schemes.

First, contact tracing involves the sharing of data within the public sector only among authorized officers, and thus, mostly poses data security risks, not a lot of privacy risks. However, route disclosures entail a more direct possibility of invasions of privacy (including the stigma effect), which discourages those suspected of infection from making voluntary reports and getting tested. There was room for reducing the associated social costs. Doing so was feasible because there would be no significant difference in epidemiological benefits (addressing information asymmetry, heightening public awareness, and inducing those in close contact to make voluntary reports) between a pseudonymized disclosure (which is vulnerable to doxing or reidentification) and a fully anonymized disclosure. In other words, the conversion of pseudonymized disclosures into anonymized disclosures could possibly result in a Pareto-efficient outcome.

Second, identifying a specific individual through a contact-tracing scheme has clear epidemiological benefits as doing so would help isolate the individual if he or she is confirmed positive for a contagious disease. Further, this capability would help avoid extreme measures, such as lockdowns. A fully anonymized public disclosure can confer, as noted, additional epidemiological benefits such as transparency or awareness. Disclosing identifiers or quasi-identifiers, however, does not confer significant incremental benefits.

Third, the differences in risks and benefits among the measures could result in different levels of public trust. This could, in turn, lead to different reactions from policy makers and legislators. In particular, different stakeholders (such as elected officers, career government officers, and health experts) could have different incentives and motivations. These differences in public trust placed each scheme on a different trajectory, when Korea strived to strike a balance between public health efforts and privacy or a broader range of civil liberties. ■

Acknowledgments

Dr. Ko received grants from the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF- 2019S1 A5A2A03036673). Dr. Park was supported by the 2021 Research Fund of the Seoul National University Asia-Pacific Law Institute, donated by the Seoul National University Foundation. Dr. Ko is the corresponding author. All authors contributed equally to this article.

References

1. S. Park, G. J. Choi, and H. Ko, "Information technology-based tracing strategy in response to COVID-19 in South Korea–Privacy controversies," *JAMA*, vol. 323, no. 21, p. 2129, 2020. doi: 10.1001/jama.2020.6602.
2. S. Park and Y. Lim, "Harnessing technology to tackle COVID-19: Lessons from Korea," *Inform. Process. [Jōhōshori]*, vol. 61, no. 10, p. 1025, 2020.
3. J. Kim and M. P. Kwan, "An examination of people's privacy concerns, perceptions of social benefits, and acceptance of COVID-19 mitigation measures that harness location information: A comparative study of the U.S. and South Korea," *ISPRS Int. J. Geo-Inform.*, vol. 10, no. 1, p. 25, 2021. doi: 10.3390/ijgi10010025.
4. "Press Releases" (Jan 20, 2020 to Feb 27, 2021). KDCA. https://www.cdc.go.kr/board/board.es?mid=a20501000000&bid=0015 (accessed Mar. 29, 2021).
5. "MOLIT, MSIT, and KCDC launch the COVID-19 Data Platform." MOLIT, Mar. 26, 2020. http://www.molit.go.kr/english/USR/BORD0201/m_28286/DTL.jsp?id=eng_mltm_new&mode=view&idx=2931 (accessed Mar. 29, 2021).
6. "Guidance on the use of electronic entry lists (for Visitors and Managers)." MOHW, June 10, 2020. http://ncov.mohw.go.kr/shBoardView.do?brdId=2&brdGubun=25&ncvContSeq=2603 (accessed Mar. 29, 2021).

Sangchul Park is an assistant professor in the School of Law, Seoul National University, Gwanak-ro 1, Seoul, 08826, Korea. His research interests center around information technology law, including artificial intelligence and law. Park received a J.S.D. from the University of Chicago. Contact him at parks@snu.ac.kr.

Gina J. Choi is a visiting professor in the School of Law, Seoul National University, Gwanak-ro 1, Seoul, 08826, Korea, and a visiting fellow (nonresident) at the University of California, Berkeley, School of Law, Berkeley, California, 94720, USA. Her research interests include law and regulatory policy for risk, security, and disaster management. Choi received a J.S.D. from the University of California, Berkeley. Contact her at jeehyun.choi@snu.ac.kr.

Haksoo Ko is a professor in the School of Law, Seoul National University, Gwanak-ro 1, Seoul, 08826, Korea. He is also the president of the Asian Law and Economics Association, the president of the Korea Association for Artificial Intelligence and Law, and the associate director of the Artificial Intelligence Institute of Seoul National University. His research interests include data privacy, artificial intelligence law, and law and economics. Ko received a J.D. and a Ph.D. in economics from Columbia University. Contact him at hsk@snu.ac.kr.