Corona-Tracking and Privacy: The Opposite Approaches of South Korea and Japan

Maiko Ichihara

Associate Professor, Graduate School of Law, Hitotsubashi University

This article was originally published in the Asia Democracy Research Network on July 27, 2020.
Original site:
http://adrnresearch.org/publications/list.php?cid=1&sp=%26sp%5B%5D%3D1%26sp%5B%5D%3D2%26sp%5B%5D%3D3&pn=1&st=&code=&at=view&idx=89

COVID-19 emerged as an invisible enemy for the human being. It is not easy to fight this enemy when we do not know who is infected or what surfaces the virus may be on. Governments have begun using IT to track infected people in order to make this invisible enemy as visible and manageable as possible.

IT-based tracking methods were in use even before the COVID-19 outbreak, triggered by the September 11 terrorist attacks in 2001. As a countermeasure against terrorism, technologies such as biometric identification and facial recognition were developed and widely used, especially for immigration control. Advances in AI have further increased the speed and accuracy of personal identification, and combined with the widespread use of GPS, the Internet, smartphones, closed-circuit TVs, and IC cards, the foundations have been laid for individual surveillance. Various countries and regions, including China, Singapore, and Penang in Malaysia, have built smart cities using these technologies. However, to date there has not been large-scale surveillance of individuals in democratic countries.

COVID-19 Tracking by South Korea

In this context, the South Korean government's early initiation of coronavirus tracking has attracted attention. The government's swift deployment of tracking measures was made possible by its experience with the MERS epidemic in 2015. The Infectious Disease Prevention and Control Act was amended in response to MERS to make it possible for the government to request telecommunication and other relevant companies to provide personal information on those who are infected or suspected of infection. Based on this Act, the Korea Centers for Disease Control and Prevention (KCDC) has used credit card history, closed-circuit TV records, GPS functions on phones, and smart cards for public transportation to track the moves of confirmed cases, and has alerted those who may have come into contact with them. Although the names of the infected are not disclosed, their behavioral histories, along with personal information such as gender, age, and nationality, have been made public on the KCDC website.

Those who enter the country from abroad are required to install a self-examination app at the immigration office and register information about their passport number, country of residence, and health status. They must enter their health information for 14 days, and if they forget to do so for four days, they will be reported to the police.

In late March, the Korea Electronic Technology Institute, KCDC, and the Ministry of Land, Infrastructure and Transport developed the Epidemic Investigation Support System (EISS) based on a Smart City data platform, which collects information related to urban planning. The Smart City was originally scheduled to be tested in February 2020 but has been converted to a COVID-19 countermeasure system. Once KCDC enters the information on confirmed cases, authorized agents request personal information needed to track these cases from the telecommunication and credit card companies through EISS. In response, the companies upload the information to EISS either automatically or manually.

The tracking and analysis of hotspots using the EISS reduced the time required to collect and analyze data on infected persons from 2–3 days to less than one hour. As a result, South Korea has quickly examined and isolated infection suspects. Messages are also shared with people who might have come into contact with the infected persons to raise awareness of their own potential for infection. Despite the early outbreak in Daegue, the tracking system has contributed to controlling the spread of infection to this day, allowing people to continue their daily lives without lockdown. The country even managed to hold its legislative election in April.

The EISS has paid attention to minimizing privacy breaches and to preventing the hacking of personal information. Personal information of infected people can be browsed on EISS only up to 14 days according to the virus's incubation period. The number of investigators authorized to access the information is limited as well. The only data accessible is related to the infection route, and information from closed-circuit TV or face recognition systems are not linked to it. To prevent hacking, investigators log in via VPN and two-factor authentication. The database is encrypted.

However, this approach still does not eliminate privacy violation completely. The fact that the authority obtains personal information without the consent of either the individuals themselves or the courts is problematic and raises concerns of abuse. In particular, there is no clear timeframe set for the use of this system and the storage of individual data. The pandemic itself is expected to be prolonged, and the possibility of the use of the system for different purposes after the pandemic cannot be completely ruled out.

This concern was compounded by the revelation that the South Korean government is still holding personal data on those who were infected with MERS in 2015. Kwon Jun-wook, director of the National Institute of Health, told a press conference in early June that they have decided to store data on MERS-infected individuals permanently. This is a move that violates the Personal Information Protection Act, which requires data on infected individuals to be deleted without delay. Although the government says that it will delete information on the confirmed cases of COVID-19 after the pandemic, based on the MERS precedent, the government's statement is not considered credible.

In addition, the fact that an excessive amount of personal information on infected individuals is made public has been a problem, both domestically and internationally. Social media is used to search for the infected persons and to pry into their private lives, violating their individual dignity and discriminating against them. Oh Byoung-il of the Korean Progressive Network says that the personal information of infected people such as gender, nationality, and age are not necessary in warning about the possibility of contact. In addition, people with symptoms may be hesitant to take a COVID-19 test if they fear the breach of privacy, the National Human Rights Commission of Korea warns. Nevertheless, individual tracking is used in South Korea because the public generally supports the government's approach of controlling the virus while tolerating privacy violations to some extent.

Japan Hesitant to Obtain Personal Information

In Japan, on the other hand, there has always been a strong sense of aversion to the invasion of privacy, and the government has not allowed health officials to access personal information. While Japan has traced the moves of confirmed cases to prevent the formation of clusters just as in South Korea, information on their moves has been obtained through interviews.

The introduction of an app to track contact with infected people was examined carefully, and COCOA was introduced on June 19, five months after the first case of infection was discovered in Japan. While the South Korean system allows the authority to access personal information, COCOA is a system developed by Google and Apple which uses Bluetooth to reveal information on contact. It notes within the individual's own phone the presence of devices that have been within one meter of each other for more than 15 minutes, with a random IDs issued every 10 minutes. The ID information stored on the individual's phone is not sent to the central server, but if a person tests positive for COVID-19 and enters the number issued by the Ministry of Health, Labour and Welfare into the app himself/herself, the ID-related information is sent to the central server. Notifications are then sent to the devices that may have been in the vicinity of the device of the confirmed case. The system is not tied to personal information, such as location, and the government cannot access personal information through COCOA.

Nevertheless, due to the fear of personal information leaks, the number of downloads within a month of the announcement was only 7.69 million. The download is limited especially among the younger generation. There is also a probability that people will not register the fact of infection, and indeed, the number of registrations of infection in one month was only 27. Without an increase in the number of users, the effectiveness of this system will not increase.

Some commentators point out that the weak level of trust in government might be a stumbling block for downloads. In addition, there is also a widespread concern in the society about the misuse of information by the app companies.

As such, concerns about privacy violations have prevented the government from an effective use of IT-based tracking in Japan. However, the government's approach unfortunately did not guarantee the protection of human rights; the absence of coercive government control led to voluntary mutual monitoring of people in the society. The emergence of a number of so-called "Jishuku Keisatsu" (self-restraint police), who voluntarily protest, report to the police, and threaten people for going out, not wearing masks, or continuing to operate their businesses has become a social problem. Despite the government's choice of measures to respect privacy and civil liberties, people are acting to suppress each other's civil liberties.

Conclusion

While there is no protection of human rights without life, we need to move with one eye on the post-COVID society. Allowing excessive privacy violations by governments is dangerous because it could be the basis for an authoritarian surveillance society; the encapsulation of various restrictive measures in the EISS is sensible. In addition, it would be desirable for the Korean government to set deadlines for access to personal information and commit to deleting personal information after the pandemic, and to do so in a manner that allows for public scrutiny. In Japan, there is a need for continued advocacy on how mutual surveillance suppresses civil liberties. It is advisable to educate people about the issue of self-restraint police, as has occurred during the COVID-19 pandemic, as a part of civic education.

The COVID-19 pandemic has led to increased interaction on the Internet and will make it even easier to monitor individuals in the future. We need to begin tackling this issue and take steps to preserve privacy and freedom both online and offline.

Maiko Ichihara is Associate Professor in the Graduate School of Law at Hitotsubashi University, Japan, and a Visiting Scholar at the Center on Democracy, Development and the Rule of Law at Stanford University. She is also a co-chair of the Democracy for the Future project at the Japan Center for International Exchange. Throughout her career, she has undertaken research on international relations, democracy support, and Japanese foreign policy. Her recent publications include: "Universality to Plurality? Values in Japanese Foreign Policy," in Yoichi Funabashi and G. John Ikenberry, eds., *The Crisis of Liberalism: Japan and the International Order* (Washington DC: Brookings Institution Press, 2020); and *Japan's International Democracy Assistance as Soft Power: Neoclassical Realist Analysis* (New York and London: Routledge, 2017).