Data ethics in combating COVID-19 after lockdown (Series Part 1/2)

Getting out of lockdown: risks and ethics of data-driven contact tracing

As COVID-19 spreads, governments are placing restrictions of non-essential movement with substantial human and economic costs. South Korea is a notable exception to this trend: as one of the worst-hit countries by coronavirus with its first case detected around the same time as in Italy, it curbed the growth in infections without a lockdown by rapidly scaling up its testing capabilities and effectively leveraging data to identify and isolate those infected.

The lockdown is intended to lower the number of newly confirmed cases to a manageable level while ramping up testing capacity. As the governments face mounting pressure to ease the movement restrictions, it is important to derive lessons from other countries' use of data to prevent COVID-19 from escalating again as people resume their daily activities.

This is the first post in a two-part series on the risks and ethics of data-driven methods in combating COVID-19 after the lockdown, focusing on contact tracing.

Contact tracing and transparency for targeted testing

South Korea avoided limitations on movement with a two-pronged approach to targeted testing: contact tracing and publicising movement data of infected patients.

First, the authorities aggressively track down those who may have been in contact with a confirmed COVID-19 patient using credit card activity data, surveillance camera footage, and mobile phone location history. Laws passed since the South Korea's Middle East respiratory syndrome (MERS) outbreak in 2015 specifically allow authorities this expanded access to personal information of infected people during a pandemic. Anyone found guilty of lying about details considered necessary for infection containment can be subject to a maximum of two years in prison.

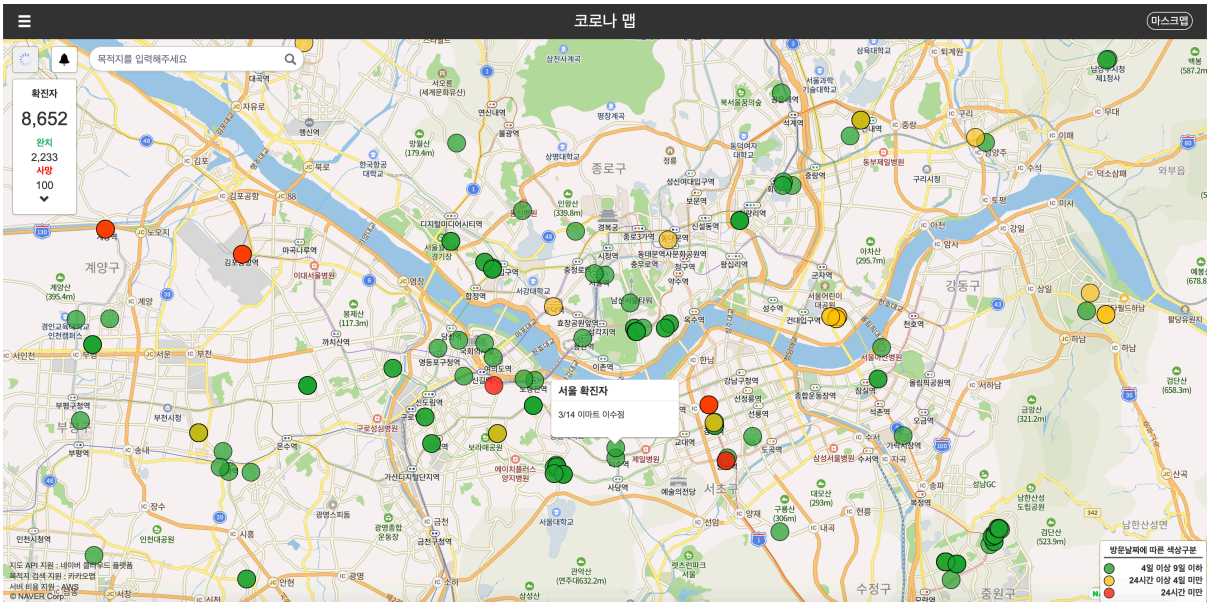
Second, the authorities publicly release the recent movement history of a confirmed COVID-19 patient. The objective is to enable people with mild symptoms to check the travel logs to see whether they may have come in contact with an infected person and get tested.

Experts agree that contact tracing and early testing is crucial. A group of scientists based at the Big Data Institute at Oxford University proclaim, "It is possible to stop the epidemic," demonstrating that sufficiently fast, sufficiently efficient, and at-scale contact tracing can reduce the spread of the epidemic below the transmission threshold.

The government's transparency in releasing accurate, timely, and detailed information about each new infection has been met with wide support from Koreans. In 1,000-person survey published in February, a researcher in health journalism found that most respondents supported the government sharing travel details of people with COVID-19.

These regular updates have prevented public panic and fostered confidence to move freely knowing that the risks are being managed. The public data sets drive further innovation in

tackling coronavirus. The government sends regular alerts of new confirmed infections, and a mobile app called Corona 100m provides push notifications when a user is near an affected location and has been installed 20,000 times per hour.



CoronaMap: https://coronamap.site/

Transparency has been also a useful weapon against the spread of misinformation. The widely reported news that a confirmed patient had visited hourly “love motels” and foot massage parlours turned out to be false. The city released a statement that patient 32 is, in fact, an 11-year-old female student, warning that spreading such misinformation is a punishable offense in violation of the Information and Communication Network Act.

Other countries have enabled access to personal data to inform contact tracing efforts. Israel’s internal security agency is using a cache of mobile phone location data originally intended for counterterrorism operations. However, the use of personal data of an infected patient for contact tracing raises issues of privacy and sparks fears of government surveillance.

Privacy-preserving contact tracing

In other countries, including the UK, the authorities do not have access to data required for such contact tracing, instead relying on conversations with the patient to identify those who have had close contact. This precludes the authorities from identifying those unknown to the patient (e.g. who dined next to the patient in a restaurant) and relies on the patient’s memory and faithful disclosure of all movements during the incubation period. The public release of confirmed patients’ movement data is also understandably controversial. The UK does not release data on the whereabouts of confirmed cases due to their “overarching duty and obligation to maintain patient confidentiality.”

To address these limitations, the NHS announced plans to work with Apple and Google to build a mobile app that tracks other nearby phones via Bluetooth, and when a user self-reports having coronavirus symptoms, it would automatically notify all recent close

contacts. This protects user privacy because the authorities do not require access to personal information, and the contact-matching process takes place locally on the phones rather than centrally through the government.

Unlike the South Korean approach that temporarily allows authorities to use all available data to effectively trace contacts, the proposed app is decentralized with limited human oversight. There are several limitations to this approach, as detailed by a cybersecurity expert in his blog. These include:

1. **Testing dependency:** The technology would only be effective if it is coupled with widespread testing, as contact tracing should be followed by a diagnosis and quarantine;
2. **Incentivising take-up:** Because downloading the app and consenting to its terms is voluntary, unlike the South Korean contact tracing, there is limited incentive to use it;
3. **Risk of false positive alerts:** Bluetooth app could flag up those in separate rooms, and in crowded urban environments, having a flood of low-risk alerts could entice a user to ignore the warnings; and
4. **Gaming:** In addition to unintentional errors, there is a risk of potential misuse and false reporting of diagnosis and symptoms, leading to greater panic.

Even with the automated contact tracing alert apps, public health authorities will still need to ask a patient with a confirmed diagnosis for close contacts. This is most effective when driven by data including public transportation usage and credit card records, which is how South Korean contact tracing has been effective in tracking down all potential infections.

There are alternative proposals to leverage such data while remaining vigilant in protecting patient privacy. In an open letter, academics have proposed data intermediaries with fiduciary responsibilities through the mechanism of trust law and the remit to monitor the terms and safeguards constraining data sharing. This would - in theory - empower people to pool together their rights over their data to a trusted third party without concerns over entrenching surveillance in our states. As in South Korea, there should be pre-defined terms to limit the usage of data and its access time period, purpose, and sharing and essential cybersecurity protection.

Disclosure of recently affected locations for the purpose of contact tracing should also be mindful of privacy concerns, which may lead to those with symptoms avoiding testing. Korea's Centers for Disease Control and Prevention said on 14 March that such detailed location information should be released only when epidemiological investigations could not otherwise identify all the people with whom an infected person had been in contact before their diagnosis.

Data released should be minimised to be fit for the purpose of alerting those who may have been in contact with a confirmed patient. For example, South Korea's release of detailed individual-level movement data risks identification despite its pseudonymisation. Instead of publishing the movement history, the government may consider de-linking the locations from the patient ID and list only the locations and timestamps.

While privacy concerns may deter the UK from publicising infected patients' movement history, a combination of a privacy-preserving contact alerting application, effective contact tracing by public health authorities, and transparent, frequent government communications can enable widespread and early testing and quarantine for the post-lockdown pandemic management.

Sample record excerpt released by Seoul government (translated by author)
Would you want your movement history publicised? South Korea's release of patient movement data is detailed and potentially invasive of privacy, risking identification by friends and family.

Patient ID (Seoul)	230
Patient ID (South Korea)	7923
Foreign travel	Spain, Czech Republic
Identified	12-Mar
Home location	Gwan-ak-gu
Hospital	Seobuk Hospital
Movement history	March 5 10: 50 ~ 11:50 Walk from home to Wesley Gym (Bongcheon-ro 516), exercise for about 50 minutes * 5 contacts ※ Disinfection and sterilization completed → 11: 50 ~ 12:30 Walk to office, work for a while → 12: 30 ~ 13:30 Walk home, delivery food → 13: 30 ~ 16:00 Walk to work → 16: 00 ~ 17:05 Walk to Starbucks Seoul University Station (Southern Ring Road 1817) * One contact person ※ Safe after disinfection and sterilization. → 17: 05 ~ 23:01 Walk to work (mask worn). Ate delivery food with six colleagues. * Six contact colleagues → 23: 01 ~ 23:05 Walk home (mask worn). March 6 10: 30 ~ 10:35 Walk to work (mask worn) → 10: 35 ~ 11:40 Work → 11: 40 ~ 13:10 Lunch at Outback Steakhouse Seoul National University with 4 colleagues at Nambu Beltway 1840 (mask worn) * 4 colleagues in contact ※ Safe after disinfection and sterilization. → 13: 10 ~ 19:27 Return to work after lunch, snack with colleagues at work * 19 contact colleagues → 19: 27 ~ 19:35 Walk home (mask worn) → 19: 35 ~ 22:10 Home, delivery food → 22: 19 ~ 24:30 Walk to Sugar karaoke room (173 Gwanak-ro 173) with 4 colleagues * 4 colleagues in contact ※ Safe after disinfection and sterilization. March 7th 00: 30 ~ 03:59 Tomoizakaya Restaurant (24 Gwanak-ro 15-gil), mask worn with 5 colleagues and 1 friend * Contact person: 8 (5 colleagues, 1 friend, 2 employees) ※ Disinfection and sterilization completed → 03: 59 ~ 04:11 7-Eleven Seoul National University Station (Bongcheon-ro 471), mask worn * No contact person ※ Disinfected, safe to visit. → 04: 11 ~ 04:12 Walk home (mask worn) → Home after 04:12

Beyond the lockdown

As governments are pressured to lift the restrictions on the freedom of movement, they will need to more effectively use available data for contact tracing. South Korea has successfully curbed the spread of COVID-19 without a lockdown, but this was achieved through targeted testing enabled by existing legislations giving authorities temporary access to enormous amount of personal data and the rights to publicize them. The measures had its shortcomings in protecting individual privacy, with excessive disclosure of movement data. However, it should be possible to implement similar measures in other countries while being more mindful of the risks, such as through decentralised and privacy-preserving data management, terms and safeguards limiting data access and usage, and minimisation of data to be fit-for-purpose.