Tracing Apps to Fight Covid-19

Are surveillance technologies effective?

By Mohammad Javed Alam and Marine Al Dahdah

Tracing apps to prevent the spread of Covid-19 have been implemented in various Asian countries, and Europe is also considering their use. But is the data privacy risk worth taking? This essay proposes an overview of such technologies and questions their efficiency.

From drones barking social distancing orders to tracing people's movements through smartphones, many governments are rushing to embrace new surveillance tools that would have been unthinkable just a few months ago. All over the world, a diverse and growing tech-based chorus, relayed by the media and many governments is calling for the use of smartphone proximity technology to fight Covid-19. Whether already implemented or only envisaged, the logic is common: since the coronavirus spreads with the movement of populations, using the mass of digital personal data generated by our smartphones can help to understand how the virus is progressing, and even guide quarantine or lockdown decisions. In particular, public health experts and tech giants argue that smartphones could provide a solution to an urgent need for rapid, widespread contact tracing applications; to track and trace infected people and who they came in contact with as they move through the world. Proponents of this approach point out that many people already own smartphones, which are frequently used to track users' movements and interactions in the physical world. Many different technical solutions are offered to put in place such tracing apps; all relying on the faith

that there is a digital solution to fight the spread of the pandemic. This essay proposes an overview of such technologies and examples of their national deployments in different countries. It also questions the efficiency of such technologies for epidemiological purposes and their impact on privacy and individual liberties.

From cell sites to Bluetooth: on different technologies and tracing strategies

Data on individuals' movements and locations can be collected through various technologies, cell sites, GPS and Bluetooth being the major ones. Cell phones work by continuously connecting to a set of radio antennas called "cell sites". The records generated by cell sites is often only able to place a phone within a zone of 800 meters to three kilometers. GPS sensors built directly into phones can do much better. GPS-enabled smartphones are typically accurate within a 4.9 m (16 ft.) radius under open sky. However, GPS radio signals are relatively weak; the technology does not work indoors and works poorly near large buildings, in large cities, and during bad weather. Tracing solutions for Covid19 needed more precise technologies to identify close contacts. That's why developers rapidly worked around applications which measured Bluetooth signal strength to determine whether two smartphones were close enough together for their users to transmit the virus.

With the Bluetooth technology, when two users of the app come near each other, both apps estimate the distance between each other using Bluetooth signal strength. If the apps estimate that they are less than two meters apart for a sufficient period of time, the apps exchange identifiers. Each app logs an encounter with the other's identifier. The users' location is not necessary, as the application only needs to know if the users are sufficiently close together to create a risk of infection. But none of these technologies, even by being combined for better accuracy, can guarantee that a given phone can be located with less than 2 meters precision at a given time, which is one of the central promise of these technical solutions. Nevertheless, Apple and Google announced a joint application using these principles that will be rolled out in iOS and Android in May and a growing number of similarly designed applications are now available and adopted nationwide in many countries. At least 19 countries are

using phone apps to identify people who are corona positive and work out who they might have been in contact with. The case of China is analyzed in another article (Governing by Technology in China), so we decided to detail other examples from Asia, but also Europe and the USA.

From Korea to India, Asian mixed success stories

At the beginning of the pandemic South Korea and Singapore were presented by media[1] as success stories of digital strategies to help containing the spread of the virus. Korea's traumatic experience with a 2015 outbreak of Middle East Respiratory Syndrome (MERS) paved the way with a law allowing the government to collect personal data and security camera footage during any outbreak. The authorities used it to trace Covid patients' movements using all of the cellphone technologies presented in the previous section combined with other digital media. As the number of corona cases increased, South Korean authorities adopted the 'COVID-19 Smart Management System'. The system was adapted from an existing "City Data Hub" platform originally developed for smart cities to analyze their traffic, energy use, environment and safety. The system crosses geolocalized data with existing public and private databases to automate contact tracing by combining data from the National Police Agency, three telecommunications firms, and twenty-two credit card companies. The system needs 10 minutes to figure out where people have recently been. If a confirmed positive covid case is found the authorities send a message on smartphone to the people in proximity to inform them that an infected person has gone to certain shops, hospitals, pharmacies or other places nearby them. That way, people can figure out rapidly if they have come in contact with an infected person.[2] This very intrusive surveillance system has no equivalent elsewhere and has been described as a great contribution to the success of South Korea's strategy against the pandemic.

1 See for instance : South Korea apps trace contacts and enforce quarantine, Singapore's coronavirus response contained outbreak—but is hard to replicate

2 From February 2020 all foreigners entering South Korea were required to download the Self-diagnosis mobile app and report their health condition twice a day for two weeks ; those who fail to report for two days on arrival receive direct calls or visits from health authorities. An American citizen documented on twitter that on arrival his wife had her location checked 37 times in three days.

Singapore began with voluntary use of TraceTogether app to find the close contacts of Covid infected people. It requires : a/ users' consent to store their mobile numbers in the registry and b/ Bluetooth switched on. The app first attaches a random ID to a mobile number and then uses Bluetooth to detect other users who come within two to five meters and records their random ID internally. If a person tests positive for Covid, the Ministry of Health contacts the person with a dedicated code to send through the app and trigger the alert. The Ministry of Health then decrypts the random IDs to determine the mobile numbers of the people who came in contact with the infected person. Singapore authorities claim to have inserted multiple measures to protect users' privacy and personal data: the use of the app is voluntary and collects only mobile numbers; all the data collected is stored locally on the user's phone, encrypted and data are automatically deleted after 21 days. The Singaporian system has been replicated in several countries, and is the model of the actual protocols being discussed in Europe. The success of Singapore is albeit mixed, as the country had to face a massive second wave of the epidemic in April, questioning its tracing strategy.

Brought as a voluntary based app, the Indian government Covid tracing app Aarogya Setu has now become almost mandatory, as institutions—public and private—and individuals must install it to avoid penalties, fines and even jail sentences. The App requires you to give personal information and the number of countries visited in the last thirty days. It is also designed to take a self-assessment survey of symptoms and to sign a self-declaration if you were tested Covid positive. The application also needs to use GPS and Bluetooth of the mobile phone continuously to keep track of the user's status and location. If two individuals with the app come in contact a digital handshake between apps will alert if one of them is Covid positive. The Government of India says that data is anonymized but doesn't explain how and is not transparent about the source code of the application, contrary to Singapore. The terms of the app explain that the government "will not be liable for any claims in relation to use of the app". Knowing that India doesn't have a privacy law to oversee such violations, there are many questions of privacy and surveillance around the AarogyaSetu app, that some digital activists presented as The story of a failure.

From USA to Europe, tech giants vs old-fashioned means

Neither the US nor the European Union have adopted a digitally-based tracing policy so far. In the United States, there is no contact tracing system at federal level, the US government adopting a liberal and market based approach, the development of such digital contact-tracing systems was mostly taken up by tech companies. Apple and Google are collaborating for an application programming interface (APIs) using Bluetooth Low Energy (BLE) principles that will be rolled out for iOS and Android in May. Apple and Google say that proximity tracking will be built-in feature for upcoming operating systems to help ensure broad adoption. A minority of States in the USA have released concurrent digital contact-tracing apps as a supplement to in-person contact tracing. North Dakota, South Dakota and Utah have rolled out two voluntary digital contact-tracing systems which are not linked to the Apple-Google plan. Care19 and HealthyTogether apps are using a combination of GPS, WiFi, IP address, cellular location data and Bluetooth to trace people who may have come in contact with an infected person. A majority of States in the US are in fact focusing on more traditional ways of handling the pandemic. For instance, the worst hit states are relying on health workers and manual contact tracing; New York, New Jersey and Connecticut partnered to hire 1,000 health workers in May to track cases. California, home of many tech giants, chose a human based tracing system and is building a coalition of 10,000 state-employees trained in epidemiology and infectious disease containment strategies to do contact tracing based on a system already put in place in 22 counties.

In the European Union, home to the world's strictest privacy regimen, the use of digital tracing methods is controversial as many governments face much wider scrutiny when personal data is involved. Technical controversies and distrust towards market-based solutions have pushed governments to first opt for a decentralized system against tech giants Apple-Google. The Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) uncloaked on April 1, called for developers of contact tracing apps to get behind a standardized approach to processing smartphone users' data, to coordinate digital interventions across borders and to shrink the risk of overly intrusive location-tracking tools. But the PEPP-PT project was split in late April when Germany and Switzerland pulled out, citing privacy worries. France was also part of the PEPP-PT in the beginning but is now working on a homegrown decentralized app.

The new decentralized system would require storing the data locally on smartphones. The app is most likely to use short range Bluetooth to establish a voluntary contact-tracing network, while keeping extracted data on the user's phone. Germany and France are expecting to have an app based contact tracing system in place by June, with the help of Google-Apple for Germans, without it for French. Nevertheless, because of the data protection issues behind such systems, both countries focused their efforts on providing dedicated health teams to more traditional epidemiological tracing methods.

Efficiency of tracing Apps for epidemiologic purposes

The value of such applications lies in its effective ability to detect at-risk contacts and to use this information in ways that are relevant to epidemic control measures, such as access to screening tests, treatment or quarantine. In the first place, these applications only make sense if they actually detect such risky contacts.

The lowest approximations estimate that more than 60%, but rather 80% to 100% of the population would need to use the application for it to be effective, provided it produces reliable data. For instance, South Korea's smartphone penetration rate is of 70.4% while India's is only of 25.3%. [3] Even in countries where smartphone penetration rate is high, like the US, Germany or France, there are great inequalities in smartphone penetration. If 77% of the French population has a smartphone, this proportion drops to 44% for people over 70 years old, although they are among the most vulnerable. Moreover, many people do not necessarily know how to activate Bluetooth and some refuse to keep it permanently activated for practical reasons (battery) or to protect themselves from malicious use. So aiming at 80 to 100% of the population using such an app is technically impossible. Then it assumes that tracking applications can accurately evaluate the distance of a person (more or less than a meter?) whatever the environment and the positioning of the phone. In practice, there will probably be both undetected contacts (such as surface transmissions) and false alarms (such as detection through a wall). Indeed, the detection range of Bluetooth seems to vary too much from one device to another and its accuracy in less

3 Source: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

than two meters is not sufficient to provide reliable results. Finally, there appears to be no consensus on the length of time and distance of proximity that would justify alerting a person who has come into "contact" with another infected person; in certain densely populated areas (certain neighborhoods, supermarkets, large companies) there would be an explosion of false positives (indicating Covid infected people, when they are not), making the application useless.

The existing "classical" epidemiologic tracing procedures are based on disease reporting mechanisms and on the public authorities' taking charge of an investigation to trace a contaminated person and its at-risk contacts. The public authorities then contact the latter, and advise them on what action to take. With tracing apps, when Patient X gets sick, he has to trigger the application so that the people with whom he has been in contact can be notified. But who certifies that Patient X is sick and that the information should be passed on? Two possibilities : 1/ Patient X will trigger the report himself; 2/ It is necessary for Patient X's illness to be confirmed by a test or a health professional, for the information to be disseminated (for example, by giving Patient X a disposable code which will trigger the report). Option one is the one chosen by India, option 2 is the one chosen by Singapore. Indeed, if people can declare themselves sick without the control of a medical authority, any malicious or "hypochondriac" user can make false declarations of illness. The multiplication of such misrepresentations will quickly render the system inoperative. In any case, there is a concern that the population will not have access to tests regularly enough to report themselves reliably enough (and relying solely on self-diagnosis could lead to a surge in false positives). Indeed, contrary to the existing procedure, these digital technologies systematically and indiscriminately alert people who have been in contact with a patient, which implies that both the patient and the competent professionals are deprived of the ability to determine who it is really desirable to alert. One could question, for example, the need to advise all contacts to go for a test, whereas for elderly people or people with pre-existing pathologies, this would in fact represent an additional risk. These aspects are not addressed in the public documentation of the proposed applications, which forgets that the implementation of existing procedure of detection of clusters by epidemiologists always gives the possibility of multiple arrangements. Moreover, a recent research shows contact tracing is only efficient at the beginning of the outbreak. Finally, by creating a false sense of health security, the application could provide an incentive to reduce social distancing and other protective measures, while failing to issue sufficiently reliable alerts.

No such thing as an anonymous tracing app

The Covid-19 emergency allows governments all over the world to use digital technology in a way that would be considered too intrusive under normal circumstances. The debate on data protection and privacy seems secondary and agreeing to governments' digital conditions now in some countries is seen as part of the citizens' responsibility. The developers of these tracing applications assure that they are privacy friendly. However, this notion remains vague. Since the beginning of the epidemic, researchers in computer security have invested in the design of such systems, others such as R. Anderson, S. Landau or B. Schneier, have denounced their dangers and expressed themselves firmly against their implementation, in view of the potential risks to private life, and freedoms needlessly sacrificed, the use of such applications imply. Indeed, the objective of such application (to alert targeted persons) is in essence incompatible with the legal notion of anonymity—it is at best a pseudonymity, which does not protect against any type of individual surveillance. Decentralized tracing protocols require the establishment of a Covid-19 patient file. Centralized models, on the other hand, have a file of people who are likely to contract the disease because they have been in contact with a patient. In all cases, these files are pseudonymized, which means that the patients are not identified by name or national identification number but by a code or number that is independent of their actual identity. In the proposed systems, the identity of Covid-19 patients is pseudonymized with cryptographic mechanisms. However, this number could be de-pseudonymized by combining it with other information in the database (the identifiers of people who have been in contact), or outside the database (for example, collected with a Bluetooth antenna), or by IP address. It is therefore not an anonymous database such as defined for example by the European law (GDPR)[4].

To the extent that tracing apps would act as a large-scale whistleblowing system for patients affected by the disease, the information it provides would provoke

[4] « The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person » Article 4, recital 26 of EU-GDPR.

suspicion, transform possible contamination into a moral error and exacerbate the stigmatization of those at risk in an already sensitive context. Such effects have already been reported causing real "witch hunts." For example in South Korea, residents can receive alerts indicating that a person living in the same neighborhood tested positive for the virus. These alerts give sex, age and list of recent travels of the individual. Although a priori anonymous, this information may have led to identifications by the public, followed by online smear campaigns (an infected person is blamed for potentially spreading the virus). Cell phone alerts disclosing personal data (gender, age, location, and workplace) of a young man who went out to several gay bars and unknowingly spread the virus have caused uproar among LGBT community in South Korea. The Solidarity for LGBT Human Rights believes this kind of sensitive information is private, and irrelevant to public health and called it a serious human rights violation. This risk of stigmatization was already considered worrying twenty years ago, when the file of HIV-positive people was being compiled, and this concern seems even more legitimate in the age of social networks.

Whether by making it compulsory, or by too much social pressure, people not using the application would risk not being able to work or to access certain public places freely, making their consent not-free and therefore lacking. For instance, the Singapore government has made it mandatory for government offices and enterprises to use SafeEntry, an app which collects personal data of workers and visitors, by scanning personalized QR codes at the entrance and exit of each site. The Singapore Government says that 40,000 sites are using SafeEntry and that businesses are required to abide by the Singaporean personal data protection act in handling the data they collect. In Italy, certain employees won't be able to access their workplaces freely, making the use of such app compulsory and against the European legislation (GDPR). In India's national capital region district Noida, not having ArogyaSetu app in your phone is a punishable offence. If you are a resident of the district, then not having the application may lead to 6 months imprisonment and a $13 fine.

Even if the application is adopted by a part of the population on a voluntary basis, it is to be feared that the government could impose it more easily on the rest of the population or made compulsory, against its will (see already the examples of Singapore and India). Knowing that all security and liberticidal measures taken in times of "emergency" have never been questioned and no one is able to tell in advance

how long the application will be deployed, once the application is deployed, it will be easier for the government to add enforcement functions (individual containment control) to it. Moreover, the application provides an incentive to subject one's body to constant surveillance, which will increase the social acceptability of other technologies, such as facial recognition or automated video surveillance, which are currently widely rejected. For instance, Singapore is experimenting with a dog-like robot to maintain social distancing in the parks. It is equipped with all surveillance gears and has in-built algorithms to detect objects and persons within one meter of its proximity.

To conclude, these applications reinforce the blind belief in technology and surveillance as the main responses to health, ecological or economic crises, while on the contrary they divert attention away from solutions: scientific research, public service funding, etc. The use of an application whose objectives, techniques and conditions of use carry significant risks for societies and individual liberties, for probably poor (or even counter-productive) results, cannot be considered as an acceptable solution. The media, political time and budgets allocated for this purpose would be better used to inform and protect the population (and healthcare workers) by methods with proven effectiveness, such as the provision of masks, tests, medical care and equipment.

Further reading

- Ross Anderson "Contact tracing in the real world". Published and consulted on April 12th 2020.
- Susan Landau "Looking beyond contact tracing to stop the spread". Published and consulted on April 10th 2020
- Bruce Schneier. "Contact tracing COVID-19 infections via smartphone apps". Published and consulted on April 13th 2020.

Published in booksandideas.net, 18 May 2020.