CSIS Commentaries DMRU-083-EN

17 June 2020

COVID-19 Apps: Fear of Tyranny by Data

Fitriani

Researcher, Department of International Relations, CSIS Indonesia
fitri.bintang@csis.or.id

In everyday life, the modern people use various software programs, often called applications or "apps" for short, from online shopping to ride-hailing, but why privacy concerns recently raised due to the introduction of COVID-19 apps? The reason behind this is the increasing number of governments around the world endorsed and, even, in specific condition, enforced people to install COVID-19 tracking app. There are at least twenty countries/territories rolling out electronic tracking to curb the spread of Coronavirus, including Australia, China, Norway, Singapore, Vietnam and Indonesia.

The concerns toward COVID-19 apps are two-folds, in the short run, there is a concern of mass surveillance and data storage security. Whilst, in the long run, there are concerns of the misused the information collected, especially if government subcontract the creation of the app and data storage to third party without sufficient legislation in place, as regulation is often set aside to get the app in public as soon as possible to manage the impact of COVID-19.

Applying Existing Technology

The effort to restrain the spread of Coronavirus of course can be done manually by tracking the interaction of people tested positive having the virus, asking who they have interact for the past 14 days or more, but the result will be greatly depend on the extend of people's memory. Moreover, getting the phone numbers of people interacting with COVID-19 positive patients and calling them one by one to suggest self-quarantine would be tedious and time-consuming work, despite arguably it would create employment.

For efficiency, therefore, tracking technology is used to collect data and prompt alert. Using mobile technology to track COVID-19 is cheaper and scalable, provided most of the population already has access to internet and smart phone. It is also notable to mention that good data collection and utilisation can help health scientists to seek solution to lower the disease transmission level and support officials to create better policies as well as allocation of resources, such as ventilator and test kits.

Technology used in contract tracing app for COVID-19 commonly utilises Bluetooth and Global Position System (GPS) that is not new. Both tools have existed over a decade and being used daily, relatively without concern when cyber hygiene steps followed. Bluetooth and GPS are used in, amongst all, headphones, smartwatches, digital maps, or food ordering apps. Again, these digital tools support people lives' daily, especially those of digital natives born post-1990 after the internet invented—this covers 360 million people of world population and 40 million Indonesians.

It is good to understand how the tracking apps work. They usually record identity of device and/or phone number to detect its movement and interaction with other devices. It is also important to provide clear information what technology does to overcome myth. Bluetooth, for example, does not measure distance but assesses the strength of signal interaction (usually known as digital handshake) that can be used to estimate distance. However, the Bluetooth tracking will record phone model and therefore this identity needs to be randomised if possible. Understanding that COVID-19 tracking apps require to record users' identity, be it phone number of headset model, it is important to be mindful of the privacy risk posed. Most people do not mind having their data tracked as their information are already in the cloud, but for some, especially for certain government officials, military personnel or minority groups, it could be life threatening. Conversely, COVID-19 tracking apps can also be life-saving to contain the virus spread.

There are two actions that can be taken by governments in designing COVID-19 tracking to respect users' privacy and data. Firstly, identity collected by the app can be anonymised or randomised, and there should be a choice to opt out anytime even after the information keyed in by user. Secondly, the data storage location should be carefully considered, whether it is centralised in a server or distributed in users' phone, what ministries or agencies can have the rights to access the data, and old tracing data recorded (usually more than 14 days) can be autodeleted.

Comparison of COVID-19 Apps

Until late May 2020, COVID-19 tracking apps have been issued in more than twenty countries,[1] tailored to national language, situation and culture. This article will compare several tracking apps from Asia, namely those issued by China, Singapore, South Korea, India and Indonesia as mainly the Asian

1 Per 26 May 2020, Australia, Austria, Czech Republic, Georgia, Greece, Guatemala, Hungary, Iceland, India, Indonesia, Israel, Italy, Jordan, Kazakhstan, Malaysia, New Zealand, North Macedonia, Norway, Saudi Arabia, Singapore, South Korea, South Africa, South Africa, Sri Lanka, Thailand and Vietnam have issued COVID-19 tracking apps. Other countries, such as Switzerland, Egypt, Russia and the US are said to follow. See Privacy International, "Apps and COVID-19", https://privacyinternational.org/examples/apps-and-COVID-19 and Norton Rose Fulbright, "Contact Tracing Apps", https://www.nortonrosefulbright.com/en-mh/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy accessed 26 May 2020.

nations react faster to the spread of the virus as it is closer to the first epicentre of the outbreak, as well as having experience from previous disease outbreak, such as SARS and avian flu. Arguably also, often times the democratic structure in Asian countries are more pliable to issued government policy, in this case tech apps, first and deal with the legislation requirement later, compared to Western rigid democratic law-based democracy.[2] However, author will touch upon several Western countries that are formulating COVID-19 tracking app policies.

China is the first country that introduce COVID-19 tracking app, namely the Alipay Health Code that requires entry of personal details (name, national ID number, contact information, and details of recent travel) stored in centralised server and shares data with law enforcements. Users will be issued coloured QR code that indicates their health status, which impacted their movement. If they are suspected positive or having interact with positive persons, they may be refused entry as they scan their QR code to enter a building or take public transport. Some argue whether such stringent measure is needed and label even it as digital surveillance[3] but the app did support China to excel in containing the spread of COVID-19.

In Taiwan, conversely, people are not required to download mobile apps but passengers arriving need to hand their mobile phone for the authorities to record their phone details. Taiwan uses slightly different technique through big data analytics through collection of phone number, headset, travel, insurance and GPS data. Its tracking systems triangulate phone signal locations and for persons subject of quarantine, the authorities will be alerted if the phone is turned off more than 15 minutes followed with the search by police forces.[4] Interestingly, Taiwan does not implement a lockdown, thus enable its 11 million labour force to stay working, but conduct stringent enforcement of COVID-19 protocol. It is so strict that even the cars used to transport people suspected with Coronavirus to be park in specific area and tracked by GPS. Similar action of tracking mobile SIM card of arriving travellers is also done by Thailand but the data collection coverage is not as vast as Taiwan.

Singapore's TraceTogether is another success case of COVID-19 app. The app relies on low energy Bluetooth and designed with "privacy and cyber security" in mind.[5] The Bluetooth connection detect other phones in range and log the digital handshakes. If a phone user that tests positive for COVID-19 give consent through the app, people they come to close contact with can be alerted. The data is encrypted and data storage is decentralised, which stored in the users' phone for 21 days. This means that users need to consent sending the stored data to the health authorities, who can decrypt the data and notify the contacts concerned. What makes it interesting is that Singapore's GovTech has made their app code open and can be used by other countries and/or tech experts trying to create contract tracing app.[6] By end of May 2020, several countries, including Australia and Germany, have admit that they use the Singapore's open-source code in developing their COVID-19 apps.

The tracking done in Republic of Korea (South Korea) is utilising several methods. The people that are asked to install COVID-19 mobile app are incoming travellers and those enforced to undertake 14 days quarantine. For most of the population, contact tracing was done through CCTV footage,

2 See, for example Tom Ginsburg, Judicial Review in New Democracies: Constitutional Courts in Asian Cases, (Cambridge: Cambridge University Press, 2003).
3 Paul Mozur, Raymond Zhong and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags", New York Times, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html accessed 27 May 2020.
4 Milo Hsieh, "Coronavirus: Under surveillance and confined at home in Taiwan", BBC, https://www.bbc.com/news/technology-52017993 accessed 27 May 2020.
5 Global Forum for Cyber Expertise, Report on the "COVID-19 Tracking Technology" Session, https://thegfce.org/report-on-the-COVID-19-tracking-technology-session/ accessed 26 May 2020.
6 SGTech, "TraceTogether and BlueTrace Codebase are now Open Source!", https://www.sgtech.org.sg/SGTECH/Web/SGTech_News_2020/May20/TraceTogether%20and%20BlueTrace%20are%20now%20Open%20Source.aspx accessed 27 May 2020.

mobile phone tracking data, and electronic transaction records. The government broadcast text messages containing information on the places and times where infected people had visit to encourage voluntary testing. This broadcast information does not contain name and address of the infected people but the society still stigmatised people who happen to be in similar place and time. In South Korea, public prosecution can be more concerning than government punishment as the society holds *chae-myun* or "face-saving" culture, which makes the alert system concerning as it could make certain people lost face.[7] Additionally, the data gained through CCTV footage, mobile phone tracking and transaction records also brought question regarding privacy. Of course, people can try methods to avoid tracking, such as wearing camouflage, leaving their mobile phone behind and paying by cash.

Meanwhile, in the biggest democracy and second biggest population in Asia, India's tracking app Aarogya Setu is developed by Ministry of Electronics and Information Technology to track users' movement utilising GPS. The app has been downloaded by more than 90 million users because it is mandatory for government employees, public-facing service providers and food-delivery personnel, otherwise they are not allowed to do their work travels.[8] As it uses GPS, the phone location should be turned on. The data collected is encrypted, with users' ID anonymised and stored in the mobile phone until medical intervention is needed. There has been debates on accuracy of location, falsified data, compromise of privacy and users' security as civil servants oblige to use the app. Aarogya Setu is not open sourced, making it more difficult for independent coders to conduct security audit.

Lastly, Indonesia's PeduliLindungi is developed by Ministry of Communication and Information Technology in collaboration with Ministry of State-Owned Enterprises (SOEs). The app collects users' name, mobile number, headset identity, geolocation and timestamp. It gave alert whenever the users entering a "red zone", that is an area with close proximity with Coronavirus positive cases. The app is using Bluetooth, which, if not updated, can be a medium of spreading malware,[9] especially for older generation phone which software is dated. There is also a concern regarding data security on the app, but the Ministry of Information has convinced that data will be securely protected and once the pandemic ended, they will be deleted. However, the issuance of this app raised a discussion on the need to speed up the formulation of the country's Personal Data Protection Law to strengthen existing Information Ministry Regulation.

Aside from the mentioned countries that have run their COVID-19 apps, many more are still formulating by taking into account various local initiative and considerations. At the Global Forum for Cyber Expertise (GFCE) meeting on COVID-19 tracking technology mid-May 2020, the Netherlands shared its experience in conducting "appathon" or apps creation competition with requirement such as privacy and information security, no usage of GPS and data should be anonymised. All submissions were considered not ready for national rollout, making the government forced to set up the program themselves.[10] Switzerland is also developing its COVID-19 tracking app with principles including transparency and voluntariness. Meanwhile, the United States have different initiatives regarding contact tracing apps on the state level, with several states have rolled out COVID-19 app using Bluetooth and GPS, while federal level is still assessing the next step.

---

7 BBC News, "Coronavirus privacy: Are South Korea's alerts too revealing?", BBC, https://www.bbc.com/news/world-asia-51733145 accessed 27 May 2020 and Zuk-Nae Lee, "Korean Culture and Sense of Shame", Transcultural Psychiatry, 36(2), 1999, pp. 181–194.

8 Andy Greenberg, "India's COVID-19 Contact Tracing App Could Leak Patient Locations", Wired, https://www.wired.com/story/india-COVID-19-contract-tracing-app-patient-location-privacy/ accessed 27 May 2020.

9 Ni Nyoman Wira, "What to know before using PeduliLindungi surveillance app, according to cybersecurity expert", Jakarta Post, 21 April 2020.

10 Global Forum for Cyber Expertise, Report on the "COVID-19 Tracking Technology" Session, https://thegfce.org/report-on-the-COVID-19-tracking-technology-session/ accessed 26 May 2020.

Author attends the GFCE meeting and noted that countries are still assessing the effectiveness of their COVID-19 tracking app as the download and usage numbers are fraction of the population. Challenge remains in obtaining the trust and even accessibility for wider people to use, not only the tech-literate. It is worth noting that with many countries producing COVID-19 apps, the two biggest global companies providing operating systems and app stores, namely Google and Apple, have agreed to create interoperable platform for government health authorities. The two companies also said to jointly-build Bluetooth-based contact tracing functionality and integrate it into their platforms to reach wider population.[11] However, the concern would be whether the tech-giants will monetise the acquired health data in the future.

Key Takeaways

The usage of tracking apps come with the cost of increasing privacy and security risk of individuals and communities. There is already stigma toward people tested positive for Coronavirus, if and when data collected by location tracking app leaked it may also increase the risk for persecution, especially toward minority groups. However, applying technology is arguably useful to obtain large scale data in an efficient and timely manner that, in this day and age, can save lives. It is also worth to remember that having COVID-19 tracking app is not a panacea, as beside apps for mobile phone users, other technologies such as facial recognition for managing people movement, drones for aid deliveries, live geo-location map for available ventilators and Artificial Intelligence for modelling upcoming outbreak spots have been used around the world. The challenge remains whether access to resource and knowledge exist, and politics are in support to apply them, especially in developing and less developed countries.

Before deciding on the pro and cons of applying COVID-19 technology, it is useful to remember that the *raison d'être* of having tracking apps is to collect data that can be indispensable for formulating policy in times of public health emergency. Without data, policy is often misguided and/or based on impulsive decision-making that may not be effective and less thorough. However, it is understandable if people, feeling that they are in high risk of espionage especially if their data is leaked and obtained by foreign entities, are concern with their devices' identity, location or movement. The challenge before us now is between health or privacy, which of these that people prioritise in specific settings, and whether government can ensure the population that their data is safe and will not be used against them.

CSIS Indonesia, Pakarti Centre Building, Indonesia 10160
Tel: (62-21) 386 5532| Fax: (62-21) 384 7517 | csis.or.id

COVID-19 Commentaries Editors
Philips J. Vermonte, Shafiah Muhibat, Vidhyandika Perkasa, Yose Rizal Damuri, Beltsazar Krisetya

11 Apple, "Apple and Google partner on COVID-19 contact tracing technology", https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-COVID-19-contact-tracing-technology/ accessed 26 May 2020.