Digital Contact Tracing in Southeast Asia

The Summary Report
Submitted to the United Nations Special Rapporteur on the Right to Privacy
Prof. Joseph Cannataci

December 8, 2020

Southeast Asia came to know digital contact tracing app in 2020 when Singapore first rolled out its digital contact tracing app in March 2020. Following the COVID-19 global pandemic, six countries of the ASEAN Member States (AMS) which are Singapore, Indonesia, Thailand, Vietnam, Malaysia, and the Philippines have adopted digital contact tracing. Concerns about privacy has arisen from the use of such approaches as they aim to gather personal data *en masse*. The digital contact tracing in the region has developed fast, while information about its impact on human rights is limited.

This report follows the release of our project "The Pandemic of The Pandemic of Surveillance: Digital Contact Tracing in Southeast Asia". The project covers digital contact tracing in the six countries above as well as a regional overview of Southeast Asia. It tracks the development of digital contact tracing apps in the region and provides analyses on their implications for surveillance and the right to privacy based on the international standards. These international standards are the Article 12 of the Universal Declaration of Human Rights (UDHR) and World Health Organization (WHO)'s Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 contact tracing.

The objective of this summary report is to provide the Special Rapporteur on the Right to Privacy with information about how the adoption of digital contact tracing in six AMS can pose a threat to human rights as well as digital security of vulnerable groups such as human rights defenders, regime critics, children, and migrant workers. This enables the Special Rapporteur to raise concerns with stakeholders using the available mechanisms that protect the right to privacy. As Special Rapporteur on the Right to Privacy, your office has provided a report on a preliminary evaluation of the privacy dimensions of public health responses to the COVID-19 pandemic on July 27, 2020 and in a statement during the 75th session of the General Assembly on October 29, 2020. Both documents raise concerns about the adoption of digital contact tracing globally and its effects on surveillance. Based on the findings of our project, this situation also applies to Southeast Asia. Digital contact tracing in the region was rolled out hastily without any impact assessment on human rights being done prior to its application to the public. Our report finds that digital contact tracing in Southeast Asia have three main characteristics that we considered as threats to the human rights, particularly the right to privacy. These characteristics are (1) technical vulnerabilities, (2) lack of transparency, and (3) lack of policy enforcement.

Digital contact tracing in the region adopts two main approaches, proximity contact tracing that uses Bluetooth Low Energy (BLE) and QR code scanning. These two approaches complement each other. We find that with more contact tracing approaches being introduced, there are increased attempts by governments to enroll people into the efforts. The proximity contact tracing app has several limitations. They tend to work only on newer model of mobile phones that not everyone can afford.

QR code scanning was introduced to fill in the gap as people can scan the QR code or provide their personal information to authorities for the purposes of recording their presence in the absence of a working device.

Technical vulnerabilities refers to those vulnerabilities found in the operation of the apps that may harm users' privacy and personal data. All of the apps and platforms used are unlikely to have privacy as primary consideration. Many of the apps in the region have privacy issues due to their technical functions. In their contact tracing apps, Southeast Asian countries have tended to adopt a centralized approach in which collected data is stored in one place for authorities to access. This is in contrast to a decentralized approach in which the collected data is usually stored in the phone of a user. Data that is stored using the centralized approach is more vulnerable to being misused, exploited, or implicated in a data breach.

Location tracking is also visible among the apps used for contact tracing in the region. The Philippines's contact tracing app, *StaySafe.ph* has location tracking as an option. However, the function would not be implemented in the first place in a privacy-first contact tracing app. In Malaysia, a now-defunct *Gerak Malaysia* was rolled out to public without approval from other government agencies due to the location tracking function. However, it was not transparent on how the app managed to overcome the issue before becoming publicly accessible.

There is also an issue with the ID used in a proximity contact tracing apps that uses BLE. They may not be safe from state surveillance. Two types of ID were found which are the temporary ID and fixed ID. The temporary ID is more privacy-friendly than the fixed ID as the ID is continuously changed over time. However, even if the temporary ID is generally safe from hackers, snoopers, and other users, it may not be safe from the state agencies. In Southeast Asia, users have little or no control over their own personal data after they engage in digital contact tracing.

Apart from the technical vulnerabilities, all Southeast Asian countries with digital contact tracing approaches have issues with transparency. The main issue is about making the software used in digital contact tracing open-source. The logic behind the open-source software is that it can provide transparency to the software as the source code is reviewed by a pool of technical experts in order to improve the software's security and privacy. Indonesia and the Philippines chose not to have their contact tracing apps open-source at all. In Malaysia, the government announced publicly that the software used for contact tracing would be made open-source in April, 2020 but it has never happened. Being a closed source software, those apps' architecture, functions, protocols, data management, and security design are unknown.

Singapore, Vietnam, and Thailand have released the source code of their digital contact tracing apps. However, their practices do not follow the logic of the open-source software. The released source code of Singapore's *TraceTogether* has not been updated following the upgrade of the app. In Vietnam, the app allegedly has an unreleased source code and the whitepaper does not reflect the reality of the app. In Thailand, the source code for its contact tracing app, *Mor Chana*, has been released without an open-source license. According to the findings, we find that these apps have difficulty following the logic of the open-source software. Governments may ignore advice from technical experts to improve functionality as this may not meet with their interests and specifications.

Furthermore, some of the apps do not have a privacy policy available. Some countries put a link of privacy policies from the app's developer or the ministry-in-charge of the app rather than the app's

privacy policy itself. Having no privacy policy means how the app collects personal data from the app and how such data is treated after it has been collected remains unknown.

Regarding the lack of policy enforcement, it is likely that the existing laws on personal data protection cannot protect personal data gathered from digital contact tracing even if personal data laws exist in places such as Singapore, Malaysia, and the Philippines. Most of these laws do not include state agencies as part of the laws and digital contact tracing are state initiatives. Moreover, most of the countries that have adopted digital contact tracing do not have an oversight board to oversee how the collected personal data is used following the adoption of digital contact tracing. In Vietnam and Indonesia, a law on personal data does not exist at all.

Digital contact tracing is acceptable if there is a guarantee that the collected data will be safe and used only for public health purposes. However, trusting digital contract tracing in Southeast Asia is difficult due to technical vulnerabilities, the lack of transparency, and a lack of policy enforcement. Digital contact tracing in these cases can threaten human rights given their inadequate rights protection frameworks. States concerned about human rights should not make citizens give up their right to privacy over public health benefits.

Given the above situation, we hope that the Special Rapporteur takes the findings into consideration and raise the issue with stakeholders using available mechanisms. It is key that enhanced threats to privacy not be ignored in spite of the COVID-19 pandemic. The current situation provides lessons learned in terms of how personal data is treated under crisis situations. Current inadequacies in protecting the right to privacy as practiced by states in response to the pandemic must not become an acceptable standard of how personal data should be treated in the time of emergency. This is particularly the case with digital contact tracing.