Digital Contact Tracing in Southeast Asia

The Summary Report
Submitted to ASEAN Intergovernmental Commission on Human Rights (AICHR)

November 27, 2020

Following the COVID-19 global pandemic, six of the 10 ASEAN Member States (AMS) -- Singapore, Indonesia, Thailand, Vietnam, Malaysia, and the Philippines -- have adopted digital contact tracing as a means to control the outbreak. This raises serious concerns about privacy, since the approach involves gathering the personal data of millions of people. Digital contact tracing in the region has developed fast, while information about its impacts on human rights is limited.

This report is submitted to the ASEAN Intergovernmental Commission of Human Rights (AICHR) following the release of the DigitalReach project report "The Pandemic of Surveillance: Digital Contact Tracing in Southeast Asia". The project monitors the practice of digital contact tracing in the six countries as well as providing a regional overview of Southeast Asia. It tracks the development of digital contact-tracing apps in the region and analyzes its adherence to international standards regarding surveillance and the right to privacy. These standards are set out in Article 12 of the Universal Declaration of Human Rights (UDHR) and the 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 AICHR with information about how the adoption of digital contact tracing in the six ASEAN countries poses a threat to human rights as well as the digital security of vulnerable groups such as government critics, children, and migrant workers. We hope that AICHR will raise these concerns with the stakeholders. As a regional human rights body, AICHR issued a press release about COVID-19 on May 1, 2020. According to the press release, the commission expected AMS to "integrate human rights values and the principles of non-discrimination, participation and inclusion in their response to the crisis." Based on this report's findings, however, human rights are unfortunately still undervalued. Digital contact-tracing in the region was rolled out hastily without first conducting any impact assessment on human rights. The project found that digital contact-tracing in Southeast Asia has three main characteristics that can be considered a threat to 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 utilizes two main technologies: proximity contact tracing using Bluetooth Low Energy (BLE) and QR code scanning. These two approaches complement one other. However, the project found that the more contact tracing applications have been introduced, the greater the number of people whose personal data has been sought. The proximity contact tracing app has some limitations; it works only on newer model of mobile phones that not everybody can afford. QR code scanning was implemented to fill that gap; if an individual's device does not support scanning, they can use other means to record their presence and provide their personal information to the authorities.

The term "technical vulnerabilities" refers to ways that using the app could compromise users' privacy and personal data. Privacy was not a priority when developing these apps and the platforms they run on. Many of the apps in the region have privacy issues due to the way they function. The contact tracing apps deployed in Southeast Asian countries have tended to adopt a centralized approach in which collected data is stored in a single 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 the user. Data that is stored using the centralized approach is more vulnerable to being misused, exploited or exposed to a data breach.

Location tracking is one of the most visible characteristics of the apps used for contact tracing in the region. The Philippines' 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, the now-defunct *Gerak Malaysia* was rolled out to the public without approval from other government agencies due to the location tracking function. it was unclear 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 app that uses BLE; it may not be safe from the government in terms of surveillance. Two types of ID were found – temporary ID and fixed ID. The temporary ID is more privacy-friendly than the fixed ID, as the former changes continuously over a period of time. However, depending on how the temporary ID is generated, it may not be safe from the government even if it is safe from hackers, snoopers, and other users. In Southeast Asia, the project found, users have little or no control over their own personal data after they engage in digital contact tracing.

Apart from the technical vulnerabilities, all the countries that have adopted digital contact tracing have issues with transparency – particularly in making the deployed software open-source. The logic behind open-source software is that it can provide transparency; the source code is reviewed by a pool of technical experts in order to improve its security and privacy. Indonesia and the Philippines chose not to make their contact-tracing apps open-source at all. In Malaysia, the government announced that their software would be made open-source in April, 2020 -- but this never happened. With closed source software, not much is known about those apps' architecture, functions, protocols, data management and security design.

Although Singapore, Vietnam, and Thailand have released the source code of their digital contact tracing apps, they have done so in a way that defies the logic of open-source software. The released source code of Singapore's TraceTogether was not updated following the upgrade of the app. In Vietnam, the app allegedly has unreleased source code and the white paper does not reflect the reality of the app. In Thailand, the source code has been released without an open-source license. Our findings show that insufficient flexibility for these contact tracing apps or platforms to be truly open-source software. This is because they are government projects, and governments may not consider comments from technical experts to improve functionality because these changes might not conform with their interests and specifications.

Furthermore, some of the apps do not have a privacy policy available. We found that some countries post a link to the privacy policies of 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 there is no way to know how personal data is treated after the app has collected it.

Regarding the lack of policy enforcement, it is likely that existing laws on personal data protection cannot protect data gathered from digital contact-tracing software. Personal data laws exist in

Singapore, Malaysia, and the Philippines, but generally do not apply to government agencies when digital contact-tracing is a government initiative. Moreover, most of the countries that have adopted digital contact tracing do not have an oversight board to monitor how the collected personal data is used following its collection. In Vietnam and Indonesia, there are no laws about personal data at all.

Digital contact tracing is acceptable if there is a guarantee that the collected data will be stored safely and used only for public health purposes. No such guarantee exists in regional digital contact- tracing initiatives given the technical vulnerabilities, lack of transparency and lack of policy enforcement. In Southeast Asia, digital contact-tracing is a threat to privacy because it was rolled out without human rights protections. Governments that are concerned about human rights should not make citizens give up their right to privacy in return for public health benefits.

Given that AICHR is a regional human rights body, we would recommend that it take this issue seriously and raise it with stakeholders, particularly the AMS governments, for better human rights protection during the COVID-19 pandemic. The situation can be considered an important lesson in terms of how personal data is treated in a crisis. The ways AMS have dealt with the issue do not meet an acceptable standard regarding how personal data should be treated in a time of emergency.