IIC Webinar, Thailand Chapter

Data privacy in the time of Covid-19

Wednesday 22 July 2020

Panel:

Prapanpong Khumon, Associate Dean, School of Law, University of the Thai Chamber of Commerce, Thailand (Chair)

Raymund Enriquez Liboro, Privacy Commissioner, National Privacy Commission, Philippines

Thitirat Thipsamritkul, Lecturer, Faculty of Law, Thammasat University, Thailand

Kevin Shepherdson, CEO, Straits Interactive Pte Limited, Singapore

Edwin Concepcion, Head, DPaaS Excellence and Support – ASEAN, Straits Interactive Pte Limited, Singapore

Introduction

Ed Khumon introduced the meeting by setting out the challenge the meeting was aiming to discuss: how technology, especially contact tracing apps, can be used to help address the Covid pandemic in ways that minimise privacy intrusions. Panel members summarised the current status in three markets – Thailand, Singapore and the Philippines.

Global privacy research

Commissioner Raymund Enriquez Liboro described the role of the Global Privacy Assembly (GPA) Covid-19 task force, including the role and the response of Data Protection Authorities in the face of tracing, testing and treatment, as well as considerations such as law reform, private sector engagement and examples of good practice.[1] Capacity building within Data Protection Authorities is a central role of the task force.

Commissioner Liboro presented the early findings from a GPA survey among 54 respondents conducted globally. The issues raising most concern involved contact tracing and location tracking, data sharing with health institutions and law enforcement agencies, and data handling. Social discrimination resulting from the disclosure of personal information also registered as a significant worry. On contact tracing, the majority of applications are voluntary to download and use, with only a small minority mandatory. This means that trust among the public over the use of data is critical if tracing apps are to be successful.

Privacy issues raised by tracing applications

- Proportionality
- Transparency
- Legal basis

[1] https://globalprivacyassembly.org/

- Data storage location
- Retention period
- Potential for misuse
- Security
- Privacy by design
- Anonymity of aggregated location data

As well as the core privacy issues, the research revealed concerns over the notion of interoperability, with data collected across borders, and how and when apps would be decommissioned. New technologies, such as wristbands designed to check on social distancing and scans using 'health cameras', raise similar questions of privacy.

Thailand

Professor Thitirat Thipsamritkul described the data privacy measures taken in Thailand under the Emergency Act. General measures included the compulsory collection of names and phone numbers on entering public venues, voluntary checking in and out via a tracing web app ('Thai Chana'), and body temperature checks at the entrance to buildings. Domestic travellers quarantined compulsorily at home or at designated locations. Checking in is via QR code and phone number, but many people fail to check out. 'Mo Chana' is an independent mobile app designed to help health professionals assess risk with data stored in the Amazon Cloud.

Thai Chana has 37m users – half the population. Unusually, it is developed by the Krung Thai Bank, with data held on-site. The fact that the app is owned by a commercial bank raises an alarm for people. It also, perhaps strangely, uses the same privacy policy as other bank products.

In Thailand, privacy notices come in two forms. One is for the user, but for the shops and restaurants the notice could allow other uses of the information not related to public health.

Automatic thermal scanning, with face detection, is in use in some spaces. It introduces the possibility of combining data with a face scan, raising a potential new issue of privacy in the future.

Impacts of contact tracing applications

Some of the most obvious concerns about the applications include its accuracy and the potential for discrimination if, for example, someone were to refuse to provide the information requested. There are also concerns about data sharing, retention and the potential for phishing links

On the other side of the debate are concerns over the response from users. They may refuse to use the app or simply pretend to scan. The app also raises awareness of privacy issues in general, and may introduce questions of privacy in other contexts.

Professor Thipsamritkul pointed out that even if it were desirable to enforce the use of apps, it would not be practically possible. Increasing voluntary usage means thinking about 'user-friendliness', by providing the information and transparency necessary in order to build confidence.

Singapore

Kevin Shepherdson began by describing the challenge of Singapore's 293,000 migrant workers. Many lived in crowded conditions, with 50-100 people living together in dormitories. While Singapore was experiencing an average of 200-300 cases per day, only 10 of these were among permanent residents. So while community cases are pursued using contact racing, migrant dormitories are monitor via proactive screening.

A national task force co-ordinates the response, with contact tracing run by the Ministry of Health (MOH). Government technology initiatives include a 'safe entry' check-in/check-out web app. This combines a QR code scan with an individual's national identity number. This data goes to the MOH but is locked.

'TraceTogether' uses Bluetooth. It collects the mobile number and assigns randomised user ID. The phone collects data from other mobile apps via Bluetooth, and this 'close proximity' information is encrypted and stored on the user's phone for 21 days. When the user falls ill, the temporary ID is decrypted, and the MOH seeks consent to share close proximity information. It was noted that this was more secure than manual data collection, where information collected in registers is exposed to anyone.

Privacy issues

The Privacy commission was involved in the design of the applications from the outset. As a result, issues such as data storage were included in the Privacy Notice and no GPS data is stored, only the individual identity codes. TraceTogether not subject to Singapore's Personal Data Protection Act, but is consistent with the Act's obligations and principles.

Now, however someone has had the idea to integrate TraceTogether with Safe Entry. It's probably the result of a desire for convenience, but in practice it enables GPS and camera access and therefore unnecessarily complicates the privacy arrangement.

A version of TraceTogether is being developed with a 'tag-tracing system', involving a token designed for use by those, especially older people, without phones. It records data in the same way as the mobile app, with interactions kept for 25 days. After a positive test, the user hands over the token to the authorities. It is not yet in use, but one concern already evident is how it can be turned off, given that the mobile version can be switched off by the user at any time.

Covid apps in ASEAN

- Almost all apps are voluntary
- Take-up is variable, from 50% in Thailand to 1% in Philippines
- Importance of 'privacy by design' to engender trust
- Best practice is to separate 'entry' apps from 'tracing' apps
- There is still no 'ideal' app

Philippines

Edwin Concepcion outlined the high levels of mobile data penetration in the Philippines. With 173 million phone connections, 73 per cent of Philippines residents have two connections. Overall penetration is at 98 per cent.

The Emergency act established an Inter-Agency Task Force. From this emerged the 'StaySafe' reporting, tracing and social distancing system, incorporating cybersecurity, data privacy and confidentiality laws. StaySafe is a privately-developed web and mobile-based app which uses GPS and Bluetooth and combines all components of pandemic management:

- Community driven contact tracing
- Health condition reporting
- Social distancing system
- Health pass (using a QR code)

However, while StaySafe is the official app, there are a plethora of others, all privately created, which have resulted in fragmented contact tracing and low app penetration. StaySafe has been downloaded by less than 1 per cent of the population.

Privacy issues

The 'all-in-one' nature of the StaySafe app makes the privacy situation complicated. Users are able to self-declare their health status, and with no means of checking this is prone to misuse. The use of GPS and Bluetooth could enable 'behavioural tacking' and there was widespread disinformation about the app over social media. Identity theft had been experienced by some individuals. However, the main issue was discrimination. There were examples of health professionals not being allowed to return to their homes and districts. Some, through a combination of fear and confusion, had been physically attacked.

In other cases, mistakes had resulted in the details of returning overseas workers had been stored in a publicly available Google drive. Accuracy of testing had also been an issue, with tests publicly declared positive, subsequently turning out to be negative.

Learning

Developers need a better understanding of the principles of data privacy. For example, the privacy statement declares that personal information is not collected, but the app uses GPS and Bluetooth location data capable of identifying individual movement. A privacy impact assessment would result in a better identification of the risks involved in an app as multi-functional as 'StaySafe', and its development should have incorporated 'privacy by design', as it did in Singapore and other countries. App development should follow a life-cycle approach, so that risks assessed at the beginning are audited, reviewed and amended once the app is in use.

Regional co-operation

Commissioner Liboro said that, for contact tracing apps to succeed, they need to be trusted and inclusive. These issues are of concern all over the world. Of all of the apps created, there has not yet been one that has definitively solved both of these requirements. International co-operation is important in this area, especially given the inter-connected nature of the ASEAN economies. Although some discussions had taken place, there was room for more co-operation in the future at both a regional and global level. There were also ideas to be exchanged on the best way for the

public and private sectors to collaborate in the use of technology during pandemics. Professor Thipsamritkul pointed out that the ability to co-ordinate app usage depended, on some extent, on the authority of governments under the law to access the necessary data, and this varied in different countries in the region.