Contact tracing apps in Singapore
A new world for data privacy
As of June 11, 2020

The COVID-19 pandemic has seen governments across the world restricting civil liberties and movement to new levels. To aid the safe lifting of current public health restrictions, new technologies are being developed – contact tracing apps – and rolled out to automate labour intensive tasks critical to containing the spread of the virus. Our contact tracing survey summarises the principal regulatory and policy issues applicable to contact tracing across a range of key jurisdictions in real time.

Is technology being used to the government to monitor and control the spread of Covid 19 (e.g. contract tracing app, CCTV, cell phone location data, credit-card history)?

The Singapore Government launched a contact tracing app (TraceTogether) on March 20, 2020. SafeEntry has also been rolled out by the Singapore Government. Safe Entry is a national digital check-in system that logs the NRIC/FINs and mobile numbers of individuals visiting hotspots, workplaces of permitted services, as well as selected public venues to prevent and control the transmission of COVID-19 through activities such as contact tracing and identification of COVID-19 clusters. Individuals check in/out from SafeEntry at entry/exit points through (1) using the SingPass Mobile app to scan a QR code or choose from a list of nearby locations using the 'SafeEntry Check-in' function, (2) having an identification card with a barcode (e.g. NRIC, Passion card, student pass and work permit) scanned by staff, or (3) scanning of a QR code displayed at the venue and submitting one's personal particulars.

To address contact tracing issues for those persons who may not have a smart phone, the Singapore Government also announced in early June that it would be making available a TraceTogether Token. This token is not an e-tag and has no internet connection or geo-location tracking functionalities but will record Bluetooth proximity data to the token for a 21 day period as with the TraceTogether smartphone app.

What are considered to be the major privacy concerns in relation to the app in your jurisdiction (in relation to its use (a) by the government; and (b) by private sector organisations)?

Concerns have focused on data security issues associated with the collection and storage of the data. The existence of data privacy issues associated with the TraceTogether app has been acknowledged by the Singaporean Prime Minister who commented at a national address on 21 April 2020 (which encouraged the use of the TraceTogether app) that “there will be some privacy concerns, but we will have to weigh these against the benefits of being able to exit from the circuit breaker [Singapore's lockdown measures] and stay open safely.”
App details

1. What is the name of app
   TraceTogether

2. Is the app voluntary?
   Yes
   The TraceTogether app is voluntary. Individuals may be denied entry to premises if they do not provide the necessary information via SafeEntry.

3. Is there any suggestion that use of the app and a clean result may be necessary to enter workplaces or any commercial or public buildings (or is this explicitly or implicitly prohibited)?
   No
   The Singapore Government has implemented mandatory measures to monitor movement and potential exposure of individuals. However, these mandatory measures are for data recording and there is no indication that a clean result is required for entry to commercial or public buildings.

   For general workplaces, the use of the TraceTogether App to record an individual's proximity to others remains recommended but not mandatory. There is mandatory requirement that owners of premises deploy the SafeEntry system to record access to a wide range of premises including workplaces, health care facilities, nursing homes and schools.

   The operators of foreign work dormitories and the employers of foreign workers living in those dormitories are required from June 2, 2020 to ensure that each worker downloads and activates the latest version of the TraceTogether App recording an individual's proximity to other app users.

4. What information is required to register for the app? Is the information collected considered excessive?
   No
   When a user registers for the TraceTogether app the user needs to consent to (i) store the user’s mobile number in the TraceTogether registry, and (ii) allow other TraceTogether users to send the Ministry of Health information of encounters with the user, if such other TraceTogether users are confirmed or suspected to have COVID-19.

5. Is GPS or Bluetooth used?
   Bluetooth is used for TraceTogether. QR Codes are used with the SafeEntry system, but there are other options for identification details to be entered by a barcode on an identification card (such as a driver’s licence, a transit card, work permit etc.).

6. Is data stored on a centralised server?
   Yes
   For TraceTogether, the signals are logged and stored on a user’s mobile phone for 21 days and will only be accessed by the central authority if a user tests positive for COVID-19 and consents to their data logs being uploaded to the server. Such data, after decryption by the central authority, would allow them to identify the User IDs of users who have been in contact with the infected user.

   For SafeEntry, the data collected is encrypted and stored in a Government server but only accessed by the authorities when needed for the purpose of preventing or controlling the transmission of COVID-19.

7. Does the identity of the infected user get captured centrally?
   Yes
   The information on the infection is gathered by the Ministry of Health from infection testing, but the fact of infection is not gathered on the TraceTogether or SafeEntry systems themselves.

   Both the TraceTogether app and the SafeEntry system require registration with a national identification number or other form of individual ID.

8. Is the identity of the infected user disclosed to proximate users or public health authorities? Is it disclosed to anyone else?
   No
   Generally information is not disclosed to anyone other than the Ministry of Health officials responsible for identifying and contacting persons who may have been exposed to a risk of contracting COVID-19.

9. Is consent needed to share data with other users/ upload the data to a centralised system?
   No
   If a user falls ill with COVID-19, the Ministry of Health will ask the user to provide data on their recent contacts and the user is under a legal obligation to provide that information. This would include information from the tracing app's logs.

10. Is the identity of the proximate users disclosed to public health authorities? Is it disclosed to anyone else?
    Unclear
    The TraceTogether app and SafeEntry data collection system are run by government departments engaged in contact tracing and COVID-19 control measures. According to the TraceTogether and Safe Entry websites, the collected data will only be used for contact tracing and COVID-19 purposes only but it is unclear the extent to which this may involve disclosure to a range of government agencies outside of the Ministry of Health.
11. Does the app incorporate “privacy by design” and was a privacy risk assessment completed?

Unclear

It is not known what kind of privacy by design analysis has been conducted in the development of the TraceTogether app and SafeEntry systems.

12. How long will the data be kept for, are there clear lines around timing?

- The data collected by the TraceTogether app will be automatically deleted after 21 days. It is unknown when the data will be deleted from the central server if pulled from the mobile app for contact tracing.
- The data collected through the SafeEntry system is retained for 25 days. The data will be purged when it is no longer needed for purposes such as contact tracing and identification of COVID-19 clusters.

13. Has data security been addressed expressly (e.g. encryption)?

Yes

When the TraceTogether app is running on a user’s phone, it will create a temporary ID, generated by encrypting the user ID with a private key that is held by the Ministry of Health. Data collected via the SafeEntry system is also encrypted when stored in the Government server.

14. Are there clear limitations regarding who may have access to the data?

Yes

Only the Singapore Ministry of Health will access the data from the TraceTogether app, but it is unclear if that information may then be further shared with other government departments. It is unclear which government departments will have access to the data collected by the SafeEntry system, but businesses are not granted access to the daily entry/exit logs collected through SafeEntry.

15. Are there clear limitations on the purposes for which the government may use the data?

Yes

The TraceTogether and SafeEntry websites both clearly state that the data will be used solely for prevention and controlling of COVID-19.

16. Is the government of your country bound by privacy laws in respect of the contact tracing data?

No

The Government of Singapore is not bound by the Personal Data Protection Act 2012 (PDPA). However, there are internal Government guidelines on the handling of data that an independent review in 2019 found to be equivalent to the PDPA. These guidelines are not made publically available.

17. Has the regulator commented/ provided guidance on the technology?

No

The Personal Data Protection Commission has issued guidance on the use of personal data for contact tracing generally and on the uses of apps that collect data for monitoring of entry to premises, but has not issued guidance specific to the TraceTogether app.

18. Are there any private sector initiatives you are aware of to use/ integrate the app or the information from the app (e.g. to reflect the results back to workforces)?

No

Not aware of any such initiatives.