NORTON ROSE FULBRIGHT

Contact tracing apps in Hong Kong

A new world for data privacy

As of February 26, 2021

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 by the government to monitor and control the spread of COVID-19 (e.g. contact tracing app, CCTV, cell phone location data, credit-card history)?

Quarantine monitoring – mandatory wristbands have been introduced for those arriving from overseas and are required to be worn for a 14 day home quarantine period. The wristband is linked to an app, StayHomeSafe. Contact tracing - on November 16, 2020, the Hong Kong Government launched a voluntary contact tracing app, LeaveHomeSafe. The app allows users to record the date and time they visited different venues by scanning the venue QR code at participating venues to log their arrival and clicking the "Leave" button in the app to mark their departure. If a confirmed case is later discovered at a participating venue, the app will notify users who have visited the same venue at a similar time to the confirmed case together with health advice.

The app also allows users who are infected with COVID-19 to voluntarily upload the encrypted visit records to the Centre for Health Protection (CHP) for epidemiological investigations.

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)?

StayHomeSafe: The key privacy concerns are excessive data collection and that data may be used for other purposes such as tracking. The Hong Kong Government addressed this concern by using geo-fencing technology rather than GPS location tracking. Other privacy concerns include storage and access to the data, as the privacy policy of the app does not contain clear information regarding retention of and access to such data.

LeaveHomeSafe: There are similar privacy concerns as with the StayHomeSafe app. However, according to the Hong Kong Government, LeaveHomeSafe does not use positioning services or any other data on the users' mobile phones and the data is encrypted and stored only in users' mobile phones.

App details

1. **What is the name of app**

   StayHomeSafe and LeaveHomeSafe

2. **Is the app voluntary?**

   N/A

   StayHomeSafe: Use of the app is required for all overseas arrivals during the 14 day mandatory home quarantine period. After the quarantine period is completed, the app can be deleted.

   LeaveHomeSafe: the app is voluntary.

3. **LeaveHomeSafe: the app is voluntary.**

   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)?

   StayHomeSafe: N/A

   LeaveHomeSafe: Yes

According to the Prevention and Control of Disease (Requirements and Directions) (Business and Premises) Regulation (Cap. 599F) Annex 1, members of the public are required to scan the LeaveHomeSafe QR code with their mobile phones or register their names, contact number and the date and time of the visit before being allowed to enter certain premises, including restaurants, sports premises, museums and public libraries, with records to be kept for 31 days for contact tracing if a confirmed case is found.

4. What information is required to register for the app? Is the information collected considered excessive?

StayHomeSafe: Yes

LeaveHomeSafe: No

StayHomeSafe: Phone number. However, when wristbands are allocated on arrival in Hong Kong, a significant amount of personal data is collected and tied to the wristband. The wristband is associated with the app and therefore the wristband wearer is identifiable.

LeaveHomeSafe: User registration is not required. Users who are confirmed COVID-19 cases who wish to upload his/her visit records to the CHP will need a personal one time password from the CHP.

5. Is GPS or Bluetooth used?

StayHomeSafe: Bluetooth and Geolocation

LeaveHomeSafe: No

StayHomeSafe: Bluetooth and geo-fencing technology to alert the authorities if the wearer leaves their home during their quarantine period.

LeaveHomeSafe: The app will not use positioning services or other. It relies on users to scan QR codes and uses the app to log their visit records.

6. Is data stored on a centralised server?

StayHomeSafe: No

LeaveHomeSafe: No

7. Does the identity of the infected user get captured centrally?

StayHomeSafe: N/A

LeaveHomeSafe: N/A

8. Is the identity of the infected user disclosed to proximate users or public health authorities? Is it disclosed to anyone else?

StayHomeSafe: N/A

LeaveHomeSafe: Yes

LeaveHomeSafe: Users can voluntarily upload the encrypted visit records to the CHP for epidemiological investigations.

9. Is consent needed to share data with other users/ upload the data to a centralised system?

StayHomeSafe: N/A

LeaveHomeSafe: Yes

LeaveHomeSafe: Users can voluntarily upload the encrypted visit records to the CHP for epidemiological investigations.

10. Is the identity of the proximate users disclosed to public health authorities? Is it disclosed to anyone else?

StayHomeSafe: N/A

LeaveHomeSafe: N/A

11. Does the app incorporate "privacy by design" and was a privacy risk assessment completed?

StayHomeSafe: Yes

LeaveHomeSafe: Yes

StayHomeSafe: According to the Hong Kong Government, the app underwent a security and privacy assessment and audit before it was launched.

LeaveHomeSafe: According to the Hong Kong Government, the app adheres to personal data privacy principles.

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

StayHomeSafe: No

LeaveHomeSafe: Yes

LeaveHomeSafe: According to the Hong Kong Government, venue check-in data which are saved on users' devices only will be deleted automatically from their phones after 31 days. If an infected user decides to upload his/her visit records to the the CHP, it is unclear how long the data will be kept by the Centre.

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

Yes

StayHomeSafe: According to the Hong Kong Government, the system is stored on the Government's private cloud and protected by "multiple layers of defence to ensure information security".

LeaveHomeSafe: The Hong Kong Government said the venue check-in data will be encrypted and saved on users' devices only.

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

StayHomeSafe: No

LeaveHomeSafe: Yes

StayHomeSafe: The PICS for the app states that the personal data provided will be used by the Department of Health and may be disclosed to other governmental departments or unspecified "relevant parties."

LeaveHomeSafe: As the venue check-in data is encrypted and saved on users' devices only and will not be uploaded to the Government or any other system, only the users can access his/her own logs. Matching of users' check-in data and the issuing of health alerts will only be carried out within the app. If an infected user decides to upload his/her visit records, the CHP will have access to the records.

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

StayHomeSafe: No

LeaveHomeSafe: Yes

StayHomeSafe: The PICS for the app states that the personal data provided will be used by the Department of Health for the purpose of preventing the occurrence or spread of an infectious disease" pursuant to the Prevention and Control of Disease Ordinance, Cap. 599, therefore the data cannot be used for any other purpose without the consent of the app user.

LeaveHomeSafe: As the venue check-in data is encrypted and saved on users' devices only and will not be uploaded to the Government or any other system, the Government cannot use the data. If an infected user decides to upload his/her visit records, they will be used by the CHP for epidemiological investigations only.

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

Yes

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

Yes

Privacy Commissioner for Personal Data issued a statement that it considers the app to be in compliance with the relevant requirements of Personal Data (Privacy) Ordinance and noted that it has adopted the "decentralized" storage model.

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

Contacts

Anna Gamvros
Head of Data Protection, Privacy and Cybersecurity, Asia
Hong Kong SAR
Tel +852 3405 2428
anna.gamvros@nortonrosefulbright.com

Marcus Evans
Head of Data Protection, Privacy and Cybersecurity, Europe
London
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Chris Cwalina
Global Co-Head of Data Protection, Privacy and Cybersecurity
Washington DC
Tel +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

Ffion Flockhart
Global Co-Head of Data Protection, Privacy and Cybersecurity
London
Tel +44 20 7444 2545
ffion.flockhart@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Law around the world

nortonrosefulbright.com