Contact tracing apps in China

A new world for data privacy

As of May 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 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)?

China established a nationwide telecom data analysis platform under the leadership of the Ministry of Information Industry Technology after the COVID-19 crisis outbreak. Based on this platform, telecom carriers (China Mobile, China Unicom and China Telecom) may provide a tracking record of the cell phone users' location in the past 15 days or up to 30 days.

In addition, various apps with similar functions were introduced in different regions of China to achieve a dynamic certification of health status of the local residents. Different status (red, yellow or green) will impose a different level of restrictions or regulations.

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)?

When the personal data is collected and used for public security purposes, no consent from individuals providing it is required. This is the principle established by the Personal Data Security Specifications. The notice issued by the Cybersecurity Administration of China supporting mechanisms to control COVID-19 (Notice) provides that entities authorized by National Health Committee are entitled to collect this data without consent.

In practice, both the Government or authorized private sector organizations may have access to personal data, but the mechanism for the processing, use and storage of the personal data lacks transparency, with the potential for abuse of personal data in the future.

App details

1. What is the name of app

Health Code or similar name which can be a separate APP or integrated into Alipay and WeChat

2. Is the app voluntary?

Yes

Whilst not technically compulsory, a clean result (i.e. green status) of the app is required to be presented for access to certain public buildings or areas.

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)?

Yes

The purpose of the health code system is to control and monitor movements around China based on the risk profile of a user. Individuals are allocated a QR "health code" which is either green (low risk and free to move around), amber (which means at risk and must quarantine for seven days in some regions) or red (which means high risk and must quarantine for 14 days in some regions). QR codes must be scanned before entering public places such as subway stations and shopping malls, and in some cities, before leaving apartment complexes and access will be denied and the authorities alerted if the individual should be in quarantine in accordance with their QR health code.

In practice, not all the operators of public workplaces, e.g. office buildings or restaurants, are strictly implementing the restriction of access based on the results of the app.

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

Yes

Name, ID card number and facial scan.

The exact data varies with the apps. Users are required to complete a detailed questionnaire setting out medical and travel history, national identity number, possible symptoms they may have etc.

5. Is GPS or Bluetooth used?

The technology rationale of these apps is not publicly available, but it is based on the records of the individuals' location.

6. Is data stored on a centralised server?

Yes/No

This information is not publicly available.

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

Yes

The identity and basic information of the infected user must be reported to the disease control and prevention center within a designated timeline.

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

Yes

Based on the investigation and management guidelines of proximates, the proximate must fill out the relevant forms and report to the local disease control and prevention center. The proximate's and the infected user's identity is required to be filled out by the proximate.

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

No

The app used in Beijing does not require consent to share or upload the data. Outside of Beijing there are regional differences in the app which is beyond the scope of this survey.

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

Yes

Please refer to our response above.

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

No

The app used in Beijing only generally indicates that data collection is compliant with the law and only for the purpose related to COVID-19, without incorporating "privacy by design" or indicating if a privacy risk assessment has been completed. There are regional differences in the apps.

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

No

The app used in Beijing does not make any reference to the data retention term. There are regional differences in the apps.

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

Yes

According to the Notice, the data controller is responsible for the data security and must take strict management and technical measures to prevent data leakage. It is unclear however what measures have been taken.

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

Yes

As provided by the Notice, only the organizations authorized by the National Health Commission according to the law can collect the data for the COVID-19 related purpose without consent from data subjects. Other unauthorized organizations must secure consent from data subjects before data collection.

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

Yes

The Notice clearly states that the use of personal data is limited to COVID-19 related purposes.

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

The Chinese Government encouraged the introduction of apps for the dynamic certification of health status in a notice released by the State Council Joint Defense or Control Mechanism in February 2020.

The clean result of the app is compulsory when the user goes to hospital or tourist sites and certain other locations.

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)?

Yes

Employers and owners of office buildings may require clean results of location tracking records before the resumption of work.

Some public workplaces may require visitors to provide dynamic certification of health status before granting access.

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