NORTON ROSE FULBRIGHT

Contact tracing apps in Canada

A new world for data privacy

As of July 1, 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)?

The Government of the Province of Alberta has introduced a mobile contact tracing app, "ABTraceTogether" (Alberta App), which utilizes Bluetooth with the aim of letting users know if they have been exposed to COVID-19 or exposed others. Alberta's "ABTraceTogether" app was developed using the same code that formed basis of Singapore's "TraceTogether" App.

Currently the government of the Province of Alberta is the only Canadian government to introduce a COVID-19 contact tracing app. The Federal Government of Canada has begun testing a mobile-based contact tracing app to be used nationwide. The app, which also will utilize Bluetooth technology, will compile confirmed positive COVID-19 cases nationwide and will notify Canadians when they have been in close proximity to others who have received a positive diagnosis of COVID-19.

The Federal Government of Canada has signalled that the voluntary, free app will be available for download beginning in early July. The Federal Privacy Commissioner of Canada (Canada's Federal Privacy Regulator) has not yet issued a set of specific recommendations regarding the proposed Canada-wide 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)?

The App is viewed to be minimally intrusive from a privacy perspective (especially in light of Alberta Privacy Commissioner's positive comments) as it is voluntary and collects very little information, which is only used for the limited purpose of contacting users in the event of a positive test. Major privacy concerns centre around employers potentially requiring employees to download the app as a condition of being permitted to return to the workplace.

Currently a major issue is that there is insufficient uptake within the population for the app to be effective and technological issues in that the app is always required to be open and on to work properly and transmission can be interrupted while other phone applications are being used (i.e. email).

App details

1. What is the name of app

ABTraceTogether (operational exclusively in the Province of Alberta)

2. Is the app voluntary?

Yes

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

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

Yes

Phone number. As configured, information collected is likely considered reasonable as the phone number is only used to contact users if they have been in contact with an individual who has tested positive for COVID-19 (and who has also downloaded the app and voluntarily indicated the public health authorities may access contact logs stored as part of the app. Users have consent to allow public health authorities access to data where user has tested positive for COVID-19.

5. Is GPS or Bluetooth used?

Bluetooth

6. Is data stored on a centralised server?

No

No. contact logs (and temporary ID) stored locally on user's phone. Contact logs and Temporary ID not captured centrally unless user tests positive for COVID-19 and voluntarily provides Alberta Health with access to contact logs stored on phone.

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

No

No. Temporary ID stored on App and uploaded to public health authority but identity of user that generated Temporary ID not captured centrally unless user tests positive for COVID-19 and voluntarily provides Alberta Health with access to contact logs stored on phone.

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

No

The identity of infected user is to be disclosed to public health authorities who will in turn contact proximate users who may have come into contact with infected user. The app uses Bluetooth to approximate distance to other phones running the same app. The app will communicate with nearby phones for a limited period. When in close proximity to another phone also running the app, both phones use Bluetooth to exchange a temporary ID. Phone model and Bluetooth strength are also exchanged and stored on user's device. Temporary ID stored by phone and exchanged with nearby phones is refreshed regularly. The temporary ID is encrypted and only possible to be decrypted by Alberta Health and Alberta Health Services (if infected user consents) and does not reveal user's identity or other individual's identity.

If a user tests positive for COVID-19, user may voluntarily provide Alberta Health Services with access to app data to facilitate contact tracing. If a user has been in contact with another user who has tested positive for COVID-19, the user will receive a phone call from Alberta Health.

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

Yes

Consent obtained at the time of signing up for app.

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

No

See above. Temporary ID provided to public health authorities but does not disclose identity of users.

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

Yes

Government of Alberta has indicated that a privacy impact assessment and security threat risk assessment was completed.

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

Yes

The mobile application maintains contact logs for 21 days on a user's phone. Alberta Health similarly maintains contact logs (which are uploaded from user's phones) for 21 days. "Non-identifying information" about the use of the app is collected by Alberta Health for "reporting purposes and analytics" and maintained for 18 months. Summary reports and conclusions from analytical assessments are maintained in accordance with records retention and disposition schedule for Alberta Health.

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

Yes

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

Yes

Only Alberta and Alberta Health Services (which are both departments of Health for the Province of Alberta) will have access and be able to use the data.

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

Somewhat

Data collected expressly indicated to be collected for the purpose of reporting total numbers of registered users and that contact information of individuals receiving a positive diagnosis will be collected for the purpose of contact tracing. Anonymized data will also be used for analytics including for "health system management and planning, policy development and analysis of the public health emergency".

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 of Alberta has indicated that the app is minimally intrusive to the privacy rights of individuals as it is voluntary, collects minimal information, uses decentralized storage of de-identified Bluetooth contact logs and allows users to control use of the app. Individuals diagnosed with COVID-19 are also able to decide whether to disclose to public health officials the contact log stored on their phone.

The Federal Privacy Commissioner of Canada along with Provincial Privacy Commissioners have issued a joint statement requesting that governments ensure that COVID-19 tracing apps respect key privacy principles. The joint statement called on governments to respect the following privacy principles: contact tracing apps must be voluntary; contact tracing apps must have a clear legal basis and consent from users must be meaningful (including separate consent provided for all specific health purposes and personal data not accessible by service providers or other organizations); the measures being introduced must be necessary and proportionate, science-based and tailored for a specific purpose; personal information of individuals must be used for its intended health purpose and no other purpose; de-identified data should be used wherever possible; measures and apps should be time-limited and personal data should be destroyed once public emergency ends; governments should be transparent and individuals fully informed about the information to be collected, how it will be used, who will have access to it, how it is stored and when destroyed; governments are to develop a monitoring and evaluation plan regarding the effectiveness contact tracing apps which includes oversight by an independent third party; and appropriate legal and technical safeguard are to be implemented to prevent unauthorized access of personal data.

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

John Cassell
Partner
Calgary
Tel +1 403 267 8233
john.cassell@nortonrosefulbright.com

Julie Himo
Partner
Montréal
Tel +1 514 847 6017
julie.himo@nortonrosefulbright.com

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

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

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

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

NORTON ROSE FULBRIGHT

Law around the world

nortonrosefulbright.com