NORTON ROSE FULBRIGHT

Contact tracing apps in Australia

A new world for data privacy

As of December 1, 2020

To aid the safe lifting of current public health restrictions under the COVID-19 pandemic, 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 Australian Federal Government launched a contact tracing app (the COVIDSafe App) on April 26, 2020.

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)?

a) By the Australian Government

i. Function creep – There was initially concern regarding "function creep", with information being used for other law enforcement purposes but a Determination under the Biosecurity Act 2015 (cth) (Determination) prohibited this. The Determination was repealed on May 15, 2020 by the Privacy Amendment (Public Health Contact Information) Act 2020 (Cth) (the Privacy Amendment Act). This amends the Australian Privacy Act 1988 (Cth) and creates offences for using data collected by the COVIDSafe App for any purpose other than contact tracing.

ii. Tracking – There were also initial concerns around the Government tracking people, but such concerns have been allayed by the COVIDSafe App not using GPS.

iii. Privacy professionals – Privacy professionals are generally accepting that the COVIDSafe App does seek to protect Australians' privacy. On May 8, 2020 the Australian Government released the COVIDSafe App source code for public inspection, hosted on a GitHub repository. The source code for the COVIDSafe App is complete.

iv. Cybersecurity review – There has been a cybersecurity review by The Cyber Security Cooperative Research Centre, which has confirmed that the personal information collected is limited.

v. Technical – There are some technical concerns that on iOS the COVIDSafe App will need to be kept running in the background. In November 2020, new code was released for public review by the Australian Government targeted to better integrating with State level contact tracing processes and improved Bluetooth function.

(b) By private sector organisations

i. AWS – The data in the COVIDSafe App can not be used by private organisations. Amazon Web Services (AWS), will supply the infrastructure and associated support services for the National COVIDSafe Data Store. As such, the Privacy Impact Assessment made recommendations that the Government should confirm the arrangements with AWS and ensure the contract is sufficient. The Government has stated emphatically that it is not possible for the US Government to get access to the data via AWS.

ii. Centralised model – The Privacy Impact Assessment acknowledged the "increased intrusiveness" of a centralised model, but states that it is understood that this "...has been balanced from a policy perspective against the ability of government to most effectively track potentially infected persons and to reduce the spread of COVID-19 in a manner consistent with the objects of the Privacy Act". No recommendations to use an alternative de-centralised approach have been made.

App details

1. What is the name of app

COVIDSafe App

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

The Privacy Amendment Act provides that it is an offence to take any adverse action or refuse to allow another person to enter premises on the grounds that the other person has not downloaded / is not using the COVIDSafe App, or has not consented to uploading COVIDSafe App data to the National COVIDSafe Data Store.

The Privacy Amendment Act does not address "clean results".

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

No - Not excessive

According to the COVIDSafe App privacy policy, when an individual registers to use the COVIDSafe App the Australian Department of Health, with the support of the Digital Transformation Agency in its role as the COVIDSafe IT service provider, will ask the individual to consent to the collection of:

- the individuals' mobile phone number – so that the individual can be contacted if needed for contact tracing;
- the individuals' name – so the relevant health officials can confirm they are speaking to the right person when performing contact tracing. It is noted that it is easiest if the individual provides their full name, but a pseudonym or fake name may be used;
- the individuals' age range – so that health officials can prioritize cases for contact tracing, if needed; and
- the individuals' postcode – to make sure health officials from the right State or Territory working in the individuals' area can contact the individual, and to prioritize cases for contact tracing, e.g. hotspot areas.

5. Is GPS or Bluetooth used?

Bluetooth

6. Is data stored on a centralised server?

Yes

Only in respect of infected users that consent and those users who have come in contact with the an infected user who also consent to data being uploaded.

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

Yes

Yes, with the consent of the infected user, the infected status and data are uploaded and linked to the user's registration data. If an individual tests positive for COVID-19 and has been using the COVIDSafe App, and the individual consents at that time, the following information is uploaded to the database administered by, or on behalf of, the Commonwealth for the purpose of contact tracing (the National COVIDSafe Data Store):

- there was contact between that individual and any other users (and as such details of another user may also be provided);
- the individual's temporary unique identifier;
- the Bluetooth signal strength during the 'Digital Handshake' (i.e. the meeting of two devices within 1.5 metres for more than 15 minutes) (note that the 15 minute time period is referred to in the Privacy Impact Assessment relating to the COVIDSafe App, but is not a requirement under the Determination); and
- the date and time of the 'Digital Handshake.'

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 public health officers responsible for identifying and contacting persons who may have been exposed to a risk of contracting COVID-19, and they will only be provided with access to information about users in the State or Territory in which they are conducting contact tracing.

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

Yes

The Privacy Amendment Act provides that it is an offence to require a person to download or have in operation the COVIDSafe App, or to require a person to consent to uploading COVIDSafe App data from a mobile telecommunications device to the National COVIDSafe Data Store. Consent is always required in order to upload the contact data. The data can not be shared with other users, even with consent.

The Privacy Amendment Act does not allow the COVIDSafe App data to be used for any purpose other than contact tracing (see 14 and 15 below). Contact tracing is defined by the Privacy Amendment Act as the process of identifying persons who have been in contact with a person who has tested positive for COVID 19, and includes notifying a person (or their parent/ guardian/ carer) that the person has been in contact with a person who has tested positive.

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

No

Please refer to our response above.

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

Yes

Yes, the COVIDSafe App incorporates "privacy by design". The Privacy Impact Assessment has also been made publicly available.

This Assessment made 19 recommendations.

The Department of Health has published its response to the Privacy Impact Assessment; in which it broadly accepts all recommendations.

In particular, the publicly released Privacy Impact Assessment states "We are satisfied that the Australian Government has considered the range of privacy risks associated with the App and has already taken steps to mitigate some of these risks. The PIA makes a range of recommendations to ensure privacy issues continue to be addressed as the App is rolled out and App information is collected and used."

One of the recommendations was to release the source code, which was released (see above).

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

- On a user device – all encrypted 'Digital Handshakes' are automatically deleted 21 days after they have been collected, or where it is not possible to comply with 21 days, within the shortest practicable period. In addition, after a 'Digital Handshake' is uploaded to the National COVIDSafe Data Store, it will be deleted from the user's device.
- COVIDSafe Data Store – The Privacy Amendment Act provides that the Commonwealth must cause COVIDSafe App data in the National COVIDSafe Data Store to be deleted after the Health Minister determines that use of the COVIDSafe App is no longer required to prevent or control COVID-19, or is no longer likely to be effective in preventing or controlling, COVID-19.

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

Yes

The Privacy Impact Assessment refers to:

- Data minimisation;
- all information uploaded to the National COVIDSafe Data Store from a user's device will be encrypted in flight;
- all information that is encrypted on the User's device will be deleted 21 days after it has been captured;
- public health officers responsible for identifying and contacting persons who may have been exposed to a risk of contracting COVID-19 will only be provided with access to information about users in the State or Territory in which they are conducting contact tracing;
- access to, and use of, the National COVIDSafe Data Store will be logged, and regularly audited; and
- ensuring that appropriate arrangements are in place with AWS, the Digital Transformation Agency and the States and Territories.

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

Yes

The Privacy Amendment Act provides that data from the COVIDSafe App may not be used other than as described in the Privacy Amendment Act.

The Privacy Amendment Act allows for collection, use or disclosure of COVIDSafe App data:

- by a person employed by, or in the service of, a State or Territory health authority, and the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing;
- by an officer, employee or contracted service provider of the Health Department or the Digital Transformation Agency for the purpose of, and only to the extent required for the purpose of enabling contact tracing, by persons employed by, or in the service of, State or Territory health authorities, or ensuring the proper functioning, integrity or security of the COVIDSafe App or of the National COVIDSafe Data Store;
- for the purpose of transferring encrypted data between mobile telecommunications devices or to the National COVIDSafe Data Store;
- for the purpose of investigating a potential contravention of the Privacy Amendment Act;
- for the purpose of prosecuting a person for contravention of the Privacy Amendment Act;
- producing statistical information that is de-identified about the total number of registrations through the COVIDSafe App;
- by a data store administrator to the extent required to delete data/ confirm deletion of correct data.

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

Yes

Please refer to our response above.

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

Yes

Specifically the Privacy Amendment Act, which is an amendment to the Privacy Act 1988 (Cth), which regulates Commonwealth Government agencies.

State and territory agencies are also subject to state privacy laws.

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

Yes

The Office of the Australian Information Commissioner (OAIC) provided a statement on April 26, 2020 that "important safeguards have been put in place to protect personal information collected through the app so it can be used to help address this public health crisis".

The OAIC also noted that it will continue to monitor implementation of the Privacy Impact Assessment recommendations and can audit COVIDSafe App and investigate complaints from the public about privacy.

The OAIC in a statement on May 14, 2020 noted, in respect of the Privacy Amendment, "The new law provides an expanded regulatory oversight role for the OAIC to ensure personal information is handled in accordance with the legislation's requirements".

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

Nick Abrahams
Global Head of Technology and Innovation
Sydney
Tel +61 2 9330 8310
nick.abrahams@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

Jim Lennon
Special Counsel
Sydney
Tel +61 2 9330 8426
jim.lennon@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Law around the world

nortonrosefulbright.com