Article Information

Author: Michael Bacina
Service: Blockchain, Intellectual Property, Intellectual Property & Technology
Sector: Health & Life Sciences, IT & Telecommunications

Is the COVIDSafe App safe to use?

The app and enabling legislation has been fast-tracked and even if it had not, we would expect a government app which collects data about citizens interacting with each other to receive a lot of scrutiny. The Australian government has not had the best history of handling Australian's data.

The Australian government this week released the COVIDSafe App.

What does it do?

The App essentially serves two purposes:

1. It notifies you if you have been in contact with someone with COVID-19;
2. If you are diagnosed with COVID-19, it enables you to automate your assistance in contact tracing to help notify others that they need to be tested.

Really? Is that all it does?

There have been concerns raised about the COVIDSafe App including:-

1. Is this App a form of government surveillance?
2. Is it tracking locations?
3. What protections are there for personal information collected by the App?
4. Is the data collected going to be managed properly?
5. Will data be released or stored offshore or available to other governments or used for some purpose other than contact tracing to stop COVID-19?

And critically, is there any verification for the answers to these questions?

How does the App work?

Before we get into the legislation (which I know you all came to hear about), first how does the App actually work:

1. The App runs in the background;

2. The App exchanges a unique code (not your phone name or anything identifiable) via Bluetooth with any other phone that has the App installed, and logs how long a user was close to another user;

3. That proximity data is **not** location based, so the App doesn't record where the user is, just that the user is near another user. The data is stored locally and locked to App access only;

4. Any proximity data older than 21 days is automatically deleted from the phone;

5. If requested, the user can upload their data, with a 2 factor authentication code being used;

6. Uploaded data is stored in an encrypted form on Amazon Web Servers in a geofenced Australian datacentre.

What happens next?

If the proximity data is uploaded, then the Department of Health takes over and sends a notification to all the users who were in proximity to that user (after we presume confirming that user has COVID-19).

How do we know the App does what they say it does?

The Government has committed to releasing the source code, which is a fundamental step forwards in application design by any government. However, we don't need to wait for that, because some kind IT professionals have decompiled the Android code and confirmed that the App in fact does what it says and does not have any back-doors or location tracking or other nefarious surveillance. The same is happening with the Apple source code.

The Legislation

In addition to knowing that the code is sound (but like all code, could be improved), let's turn to the enabling legislation.

We start with the *Biosecurity Act 2015 (Cth)*, which permits the Minister for Health, at s.477, to make determinations during a human biosecurity emergency. Such an emergency was declared (for the first time) on 18 March 2020 by the Governor-General of Australia under s475 of the Act.

Once that declaration was made, the Minister for Health was empowered to make the *Biosecurity (Human Biosecurity Emergecny) (Human Coronavirus with Pandemic Potential (Emergency requirements – Public Health Contact Information) Determination 2020* (the **Determination**).

S.6(1) of the Determination prohibits a person from collecting, using or disclosing COVID app data except as provided by s.6(2). So we start from a negative proposition, no use of any data unless permitted under subsection (2).

So what are these reasons:

1. **The App itself working** The App transmitting the encrypted identifier (s.6(c)) to other COVID-19 Apps, or uploading the proximity data to the department of health;

2. **Contact Tracing once proximity data is uploaded** At s.6(a)(ii) and s.6(b)(ii), the COVID app data can be used for contact tracing (which is defined in s.6(3) as the process of identifying persons who have been in contact with a person who has been positive for COVID-19) or making sure the App works.

3. **Prosecuting someone who has breached the restrictions on use** This one confuses some people, one of the permitted uses of data at s.6(d) is in investigating whether a requirement of the Determination has been breached or if someone has breached the Determination (here the Determination refers to s.479 of the *Biosecurity Act 2015*, which makes it an offence to fail to obey a Determination), Put simply if someone hacks or gets hold of the data, they can't object to evidence of their crime being used in Court on the basis of it being illegal under the Determination to use the data.

4. **Statistics (in a de-identified way)** The App data, if de-identified, can be used for statistical information.

The Determination also prohibits anyone:

1. Uploading App data using the App unless the user consents to that upload.

2. Making the App data stay stored for more than 21 days

3. Once uploaded, the data cannot be kept on an overseas database or disclosed to any person outside Australia, other than for the purpose of contact tracing.

There has been some talk of businesses and groups banning entry or service to individuals who don't install the COVIDSafe App. That's prohibited by s.9 of the Determination.

Finally, section 7(5) of the Determination requires the Federal Government to delete their records of the COVIDSafe app which have been uploaded after the pandemic has concluded, and this overrides any other requirement which might cause the data to need to be archived.

So it's perfect then?

Of course not, there's been a number of challenges which still should be addressed, but none of those should be used as a reason for not supporting the App, while calling for improvements.

Some issues which need attention:

1. Most urgently, the App won't work in Apple's IOS unless the app is open in the foreground (i.e. is on your screen). Apple needs to patch this urgently or the App is next to useless.

2. Government messaging has been that only signals within 1.5m for more than 15 minutes will be recorded, but the App right now collects any signal it can pick up. This is totally understandable but the messaging should be clarified.

3. The requirement in s.7(1) for consent from the person "*in control*" of the phone to upload the COVIDSafe should changed to the person "*ordinarily in possession or control*" of the phone.

4. Some oversight of a Parliamentary Committee or the Privacy Commissioner and formal arrangements with the States and Commonwealth would assist in closing any further potential gaps.

5. The Determination can be amended at will by the Health Minister, so it should be replaced with an actual law which requires parliament to amend it.

6. The Apple/Google contact tracing models are likely to have better baked in systems for tracing outbreaks.

The final word

While the source code for the IOS app isn't yet available (and the Government hasn't officially released the source code as yet) it's clear from the de-compiled analysis that the app isn't tracking location, the data is securely stored locally, and there is no secret surveillance going on.

There are definitely improvements which could be made to the architecture and security of the app as well as the Determination and legislation, but given what is at stake right now, and the minimal amount of information which would be uploaded as Australia continues to stay ahead of the coronavirus curve, on balance we suggest Australians do their civic duty and help end this disease, push for improvements in the COVIDSafe App, then once the pandemic ends, delete the App from their phones.