Making privacy core business

COVIDSafe app – Are you sitting on the fence?

Practical privacy and security considerations

4 May 2020

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000

COVIDSafe app – Are you sitting on the fence?

Annelies Moens, Managing Director, Privcore **4 May 2020**

It is Privacy Awareness Week in Australia – and what a time to have one of our largest real-world case studies to analyse, the COVIDSafe app. It raises all those thorny community, individual, economy, health, government and social licence perspectives which make the privacy and security disciplines so interesting. The challenges to consider in designing privacy safe processes and technologies and the critical thinking needed to be a privacy professional explain why I have been working in this field for almost 20 years.

When the Australian COVIDSafe app was first released on 26 April 2020, the privacy community was largely silent because there are so many important perspectives to consider. Although some opinions have recently started to be published, I think it will take weeks and months to see how this fully plays out as the COVIDSafe app's source code is yet to be released and a legislative framework is still to be put in place. The success of the app's objective to make contact tracing faster and more effective will also only be known after time passes, especially as not everyone has up to date technology.

A privacy impact assessment (PIA) was conducted and published soon after the release of the COVIDSafe app. The PIA was conducted "from the perspective of Health, as the Commonwealth agency responsible for the implementation and operation of the App and the National COVIDSafe Data Store, and not from the perspective of any other agency or other entity" (p.15 of the PIA). Therefore, other stakeholder perspectives and ecosystem privacy risks were not in scope for detailed analysis.

My view is that there are important questions addressing privacy ecosystem risks requiring detailed analysis including:

1) Will foreign governments potentially be able to access the National COVIDSafe Data Store relating to COVID-positive people and their Bluetooth handshakes? Why is it centralised and retained until an undefined pandemic end date, especially once contact tracers in the States and Territories have downloaded the data needed from the Data Store? An American cloud service provider, Amazon Web Services is hosting the data in potentially Chinese-owned data centres in Australia with encryption keys stored in the same cloud infrastructure as the data.

2) What are the downstream protections of the COVIDSafe app data and connected data? Once contact tracers in the States and Territories have the COVIDSafe app data of a COVID-positive person's potentially exposed contacts from the last 21 days, as the Australian Department of Health determines from the Bluetooth handshakes, what happens to it? It may be transformed and matched with other data sets, but only the COVIDSafe app data as defined in the interim Minister of Health's Biosecurity Determination will have the strict privacy protections. The States of Western Australia and South Australia also do not

have privacy laws (though SA has public sector guidelines), and whilst there is a mandatory data breach notification law in the federal Privacy Act, there are none at State level.

3) What happens if something goes wrong with the technology or data is inappropriately collected, used or disclosed? What happens if there are false-positives (over-collection of data and more people are quarantined whilst waiting for testing than need to be in response to a COVID-positive person) or false-negatives (people who have in reality been in close proximity to a COVID-positive person are not notified and therefore not quarantined or tested)? Where can people obtain consistent remedies in light of the Commonwealth, State and Territory jurisdictions involved – who has accountability?

4) What are the expectations of the community, technologists, security and privacy experts, state and territory health agencies and other stakeholders outside the Australian Department of Health? Developing agile, inclusive and open processes where that input can be provided is integral to the development of privacy by design solutions and legislative frameworks that effectively manage the consequences of the corona virus pandemic.

Whilst all the above issues will get their full air time in due course, the immediate question for you is: do you install and use the COVIDSafe app or not? (Please note that not everyone is in the position to be able to do so). Individuals who can make a choice have to weigh the risks and benefits to themselves and the community. There are many perspectives to consider as mentioned earlier. As a privacy professional, I have created a short list of practical privacy and security considerations below. They are far from complete; they are merely a starting point for those who would like to increase the privacy and security of their devices when deciding whether or not to install and use the app.

Practical privacy and security considerations

The Australian Department of Health has produced a Technical Help section for the COVIDSafe app. The app works on Android and iPhones as follows:

- For Android, you need Android 6.0 (Marshmallow) or higher.
- For iOS, you need iOS 10 or higher. You will need an iPhone 5S model phone or higher.

So, if you don't meet that first hurdle you do not have to consider this decision any further, as you won't be able to download the app (unless you are able to upgrade your device or mobile operating system). To upgrade your mobile operating system on Android check these steps. To upgrade your mobile operating system on iPhone check these steps.

If your device at least meets the above technical specifications, consider the following:

- **Having Bluetooth on all the time – is that safe for your personal circumstances?** The e-Safety Commissioner says there are many ways to reduce the risk of Bluetooth and to connect to it safely.

- **What's the impact of having Bluetooth on for your other apps and data held on your device?** Think about when you go to the shopping centre and other places. Whilst the COVIDSafe app is not collecting your location, your other apps may start to, if you otherwise hadn't already enabled Bluetooth. If this is of concern, review what other apps you have on your device and their permissions. For steps on how to do this, visit Android and iOS support pages.
- **What other steps can you take to further protect your privacy and security, whilst enabling the COVIDSafe app?** Ensure you have the latest security and Bluetooth patches for your device. For some general privacy and security considerations, if you have an Android device see the tips from protonmail.

Mobile devices are often used to connect to personal accounts, banking and crypto-wallets and to work data and systems, particularly when working remotely or from home. Therefore, it is important that your mobile device is secure not just for yourself, but others around you, including your family, friends, employer and your service providers.

Not everyone has up to date technology to help to make contact tracing faster and more effective through the installation and use of a scalable contact tracing app. For those that do and are sitting on the fence undecided, maybe the above considerations will help with your decision by providing you with some resources to increase your privacy and security on your device(s) and those of others whose data you may hold.

Once you are confident of your device security and privacy settings, then you have reduced your privacy and security risk as best you can. When you are in public crowded spaces, the potential benefits of using the COVIDSafe app are likely to outweigh the risks, assuming a strong legislative framework is put in place to address outstanding questions, there are no negative surprises in the source code, and continuous improvements are made to the ecosystem as medical and technical knowledge advances.

About Us

Privcore's team with 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens.

Annelies Moens, CIPT, FAICD, CMgr FIML, a privacy professional practising since 2001 founded Privcore and is a former President of the International Association of Privacy Professionals which she co-founded. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She had the benefit of resolving hundreds of privacy complaints whilst working at the Australian privacy regulator and consults globally on privacy. Her bio is available at: www.privcore.com/bios.