The COVIDSafe App: A Question of Trust

How the Australian Government and Australian citizens can ensure the success of the new coronavirus tracing app.

A Pearcey Foundation paper

Pearcey
FOUNDATION

Summary

The Australian Government has now released its coronavirus tracing app, called COVIDSafe. To be effective, the app needs to be downloaded and used by a significant proportion of the Australian population.

There are some concerns that the app will not be downloaded because of privacy considerations. The Pearcey Foundation believes these fears are largely unfounded and that the Government has sufficient measures in place to ensure the security of the application and the privacy of the data.

It is a tracing app, not a tracking app. The data is stored only on a users' phone unless they give permission for it to be uploaded. This will usually happen only if that person becomes infected with the virus. To be effective, the app relies on trust, effectiveness and education. While the Pearcey Foundation believes all three issues are being addressed, more still needs to be done to ensure the public is fully informed and that all safeguards remain in place.

This Pearcey Foundation paper examines how this can be done. It is based on the collective views of a group of senior Australian ICT specialists, all of whom are of the belief that the app will be effective if widely implemented, that the government is doing enough to ensure its integrity, and that it is an important new weapon in the fight against the spread of the virus.

This paper aims to show what the Government, and we as individuals, need to do to ensure the success of the COVIDSafe app.

What is the COVIDSafe app?

The Federal Government has released its much-anticipated Coronavirus tracing app. It is called COVIDSafe, and is available on Apple and Android smartphones. The big question for most Australians is "should I download it?"

The app will be successful only if a critical mass of Australians do so. Although it will not be mandatory, the more people who download it the more effective it will be. The government hopes at least half of all Australian smartphone users will download the app, a sufficient number to ensure the critical mass required to make the app effective.

There are three factors that will determine the success of the app:

- Trust: Do people trust the Government not to misuse the data the app collects?
- Effectiveness: Will the app do what it promises? Is it easy to use?
- Education: Will enough people know about the app to even consider downloading it?

We address each of these factors in this Pearcey Foundation paper. Of these, by far the most important is trust, which is based on the perception and reality of privacy and security.

The Pearcey Foundation is an organisation of senior Australian technology professionals. Like all Australians, we want a speedy end to the coronavirus crisis, and we welcome any initiative that helps achieve that goal.

This paper aims to show what the Government, and we as individuals, need to do to ensure the success of the COVIDSafe app.

Trust

Can we believe what the Government says?

Like any new technology, the app has the potential to be used for good or for bad. On the positive side, it will help us trace the spread of coronavirus so that we can eradicate it more quickly. On the negative side, there are serious concerns that it will compromise people's privacy to the extent that it has the potential to do more harm than good.

Every person will make the judgement between self-interest (my risk, my benefit) and the group-interest (the benefit of a positive mass public health outcome).

The Government insists that the app will not compromise privacy. It is, in essence, asking us to trust it. Should we? There have been recent examples of governments not fulfilling their assurances regarding privacy, and of an increasing tendency towards surveillance working to the detriment of citizens' liberties and digital rights.

We do not believe that is the case with the COVIDSafe app. The Pearcey Foundation strongly believes all Australians should support this important initiative.

Is it secure?

The issue of security is largely to do with the integrity of the application. There are some key questions. Can we be assured that the application is going to do what it says it is doing (and what the Government says it is doing) and nothing more? Can we be assured that the application cannot be tampered with, or misused, to do something it is not intended to do? Can we be assured that the application cannot be repurposed in the future to do something different from what it is intended to do?

These questions can only be answered if the app is properly vetted and accredited, e.g. by the ASD (Australian Signals Directorate), the CSCRC (Cyber Security Cooperative Research Centre), or other academics and security experts.

One key aspect of security is where the data is stored. The Government has given assurances that all data will be stored in secure Australian data centres, which can be easily verified.

The source code should also be publicly visible to prove that it doesn't contain hidden functionality. This can happen through technology known as Open Source.

Can we inspect the app?

One way the Government can support the Australian public in establishing trust in the security of the application is by ensuring it is released under an Open Source licence. Such a licence has a number of criteria which enable anybody to verify the behaviour and security of the application.

The COVIDSafe app is based on TraceTogether, an application jointly developed by Singapore's Ministry of Health and Government Technology Agency. It is based on a protocol called BlueTrace, which has been released under an Open Source license called GNU General Public License (GPL). By releasing this underlying protocol under an Open Source licence, Australian Government agencies and community members alike are able to independently verify the behaviour and security of the application.

The Government has not yet made the source code available, but in the short time since the app has been released a large number of technical professionals have been able to inspect the behaviour of both the Apple iOS and Google Android versions. Since the release it is evident from these inspections that the app is behaving as the Government has said.

The Apple (iPhone) version does not request permission to access location. The Google (Android) version requests location permissions, as this is required to access Bluetooth. Inspections of app behaviour have verified that no location data is actually being used.

Is my privacy assured?

Privacy is different from security. Security concerns the integrity of the app and the data, while privacy is about what information is being collected and how it is used. It means that we must ensure that the data is used only for the specific purpose of tracing coronavirus and nothing more.

This means the data must have a defined and well understood lifecycle through its collection, release, analysis and erasure. Protections here include analysis by the Australian Privacy Commissioner and auditing by the Australian National Audit Office.

Privacy also means that the data cannot be released to other government bodies, including courts and other law enforcement agencies, academic institutions, or to commercial organisations such as the media.

There are also other considerations. You will be notified if your data is downloaded for analysis, but this will only happen if you have been co-located with a device held by an infected person This could be very alarming and result in anxiety for some people, particularly the ‘Worried Well’ who might then seek health advice. Telehealth consultations as a first point of contact will be an efficient and cost-effective way to complete initial assessment without compromising anyone’s privacy or unduly alarming them.

With access to the source code of the application available to the community via an Open Source licence, the next issue to address is what happens to the data generated by the application. The Australian public want assurances that any personal information generated by the application is used only for the purpose for which the data was given to the Government – the tracing of coronavirus carriers and those who may have been infected through contact.

The Australian Privacy Principles are the cornerstone of the privacy protection framework in the Privacy Act. They are a set of principles designed to ensure that entities that manage personal information do so in an open and transparent way.

These principles were initially intended to be the basis for the privacy aspects of COVIDSafe, but in practice the level of privacy is much higher. The announced privacy provisions go significantly beyond the requirements of the Australian Privacy Principles, with a specific directive and severe penalties for use other than by State health departments (including not allowing employers to mandate the use of the app).

We are confident the Australian Government will provide assurances that the data generated by the application will be managed in compliance with these principles. This will ensure a framework of openness and transparency for the Australian public to trust the application and the management of the data the application generates.

Effectiveness

Will the app do what it says?

An important aspect of understanding the issue of trust lies in the nature of the COVIDSafe app and the benefits it will bring. It is not a surveillance app – it does not track people's movements. Rather, it is a proximity application on a smartphone that keeps an encrypted record of other phones that have been nearby (1.5 metres) for a set period of time (at least 15 minutes).

The technical details are important. They enable us to understand what the app is and what it is not. There is some confusion over this. The key is the difference between 'tracing' and' tracking'.

Tracing is a retrospective process that enables the identification of people you have been in contact with. **Tracking** is a real-time activity that allows others to monitor your location. The difference between the two is significant. When people download the app, they register their basic personal information – phone number, name, age range and postcode. This information is transmitted to the Government and stored in a central database. You can use a pseudonym or nickname instead of your actual name.

When your phone is close to another phone that also has the app installed, both phones exchange anonymised IDs using Bluetooth, the universally used standard for wireless data exchange over short distances. Encrypted IDs from phones you have come into contact with are then stored on your phone, and nowhere else. Similarly, the other phone stores your encrypted ID.

The COVIDSafe app cannot communicate with any other apps, nor can it identify phones without the COVIDSafe app installed and active. The ID is also rotated every two hours.

If you then get infected with COVID-19, you can voluntarily use the app to contact the authorities, giving them permission to give contact tracers access to the data on your phone. This data is nothing more than the list of anonymised IDs that show with whom you have been in contact. No geolocation or other personal data is collected. The anonymised IDs will help contact tracers quickly identify and contact people at high risk of infection.

Unlike just about every other app on your phone, information is stored only on the phone, and is not automatically uploaded to a central store (only your initial contact details are uploaded). If anybody subsequently identifies as COVID-19 positive, then the record of social interactions located on their phone will be uploaded, which will potentially identify you as having been close to the carrier at some stage.

It is important to understand that no data is transferred in real time. The app collects minimal information – only anonymous IDs and the time of the interaction. For proximity, the Bluetooth scan is once every minute and other users' encrypted IDs will only be stored if they are repeated 15 times (15 minutes). The upload of data is voluntary, and the app can be deleted at any time along with its data.

Why do we need an app?

COVIDSafe is essentially an automation of the existing manual tracing process. Currently, thousands of people are employed to check (i.e. trace and identify) people who have come into contact with anyone who has contracted COVID-19. Those people who have been identified are then alerted and asked to test for the virus.

Without the smartphone app this process is manual, time-consuming and laborious. It is also error-prone, as it relies on people's memories, which may be incomplete or faulty. COVIDSafe vastly automates the tracing process, while ensuring integrity and accuracy.

Again, remember it is a tracing app, not a tracking app. The contact data that is stored locally on the phone is automatically deleted after 21 days, and you can opt out at any time by deleting the app or turning Bluetooth off.

Legislation only allows authorised health officials to access uploaded data. The Biosecurity Act makes illegal (bans) any secondary use of data including use by other government agencies. The app passes a thorough independent privacy review, published in the COVIDSafe Application Privacy Impact Statement.

But even with this very limited scope, there are a few important questions that most people would like to understand.

How will contact take place?

There are some concerns over what happens if you inform the authorities that you have contracted COVID-19. The information on the app mentions this procedure, but it needs to be spelt out more clearly.

If you contract the virus and inform the authorities, you need take no further action. The tracing team will manually inform those people you have come into contact with, warn them that they may have become infected, and advise them to be tested. They will not be informed of your identity, nor will any tracking take place to ensure that they have acted upon the advice of the authorities. You have no further obligations, and other people have no way of knowing with whom they came in contact and who may have infected them.

This is simply a continuation of the current manual tracing process, except that it is much more efficient. A central telehealth service could provide a rapid and personalised service to establish degree of infection or exposure and advise on further precautions and reporting of individual's health progression and could be considered for future epidemics. These are important safeguards that need to be fully spelt out in any public education program.

Who is responsible?

Even if we have security, privacy, uptake and trust, there still needs to be a group of people responsible for the entire project. The Australian Government Department of Health is the responsible product owner and states the app is an important public health initiative to help keep us safe from further spread of coronavirus through early notification of possible exposure.

The Federal Government's Digital Transformation Agency (DTA) is listed as the app developer in app stores and is responsible for the design, build, distribution, maintenance and support of the app and the process. DTA has carriage of the Australian Digital Service Standard which is a set of best-practice principles for designing and delivering Government services. There is also the management of the project implementation and the reporting about the project's effectiveness which we recommend to be undertaken by an independent cross-sectoral body to build public trust in future initiatives.

Every aspect of the project needs appropriate controls, checks and balances. The system needs to be auditable and the people running it need to be accountable. There needs to be oversight and proper reporting. This project is much bigger than just the application. Who owns that responsibility is critical in gaining the trust and adoption of the community.

Human rights and civil liberties will need to be fully protected and there is a concern that the data might be linked to other collected data that Government agencies have access to, and which are not limited by Commonwealth or State legislation. It is good to see the Department of Health Privacy Impact Assessment has considered these implications and is committed to address concerns throughout deployment of the app. This has to be an ongoing and transparent process for the initiative to be effective in achieving the stated public health outcomes.

Education

Uptake and impact

Even if the app is secure and the data is private, there needs to be mass uptake to have any chance of it being effective. Here group-interest is much more important than self-interest. It is about social obligation. If you contract the virus then you should feel a mutual obligation to help other people know that they are at risk, and help the authorities identify and contact affected people to reduce the spread of the virus. The Government has specifically stated this cannot be used for identifying breaches of social distancing regulations. This is a welcome provision.

Many of the working population will find it very difficult to socially isolate in the future, especially when commuting or at work. This is where the application has its greatest impact – to protect the spread of a virus where public proximity is a way of daily life. Today this is a mobile app but, in the future, we recommend it be part of a mobile device functionality that can be switched off, such as location services can be currently, or left on to provide the data when requested.

Adoption of technology is never easy and in times of crisis, fear uncertainty and doubt (FUD) is heightened. This is perhaps the largest digital adoption initiative Australia has undertaken to date and the public health imperative may throw caution to the wind with such a short runway. It is important to keep in mind that central to this is behaviour change and the process of learning. People need to understand the potential of the app, accept that it will help to achieve public health goals, and the distribution needs to be both individual and collective to deliver the impact we need.

Digital inclusion implications must be considered for at risk communities who may have low access and device ownership or the digital skills to successfully use a mobile app. We know that COVID-19 has devastated marginal communities in the US partly due to existing socioeconomic determinants of health. In Australia we've seen the impact on the aged care sector and the potential for others such as disabled, indigenous, and cultural and linguistically different (CALD) communities is high. The specific risk if the virus takes hold in these communities needs to be considered in designing and rolling out of the app. Multilingual support and promotion are a must to ensure successful uptake across all Australian society.

Public awareness

Education and getting the right message out to all Australians will be difficult. Combating misinformation and distrust is necessary and important if the project is to succeed. To this end Pearcey has entered this debate with reasoned, evidence-based discussion and this resultant paper.

Australians are generally wary about the Government pushing a particular technology. Think back to the 1990s and the concerns about the Australia Card. Even if security and privacy issues are addressed and the COVIDSafe app can be shown to have mass health benefits, there will still be many who will use social media and other channels to promulgate FUD.

In recent years, more successful public awareness apps have been implemented by NSW and Victoria State Governments for emergencies, which are paired with a website. These digital tools have been used to great effect during the recent bushfires and have also been a valuable tool in disseminating information during the COVID-19 emergency. There seems to be no significant issue of trust in adopting these Government tools for our general or specific welfare.

Everyone must be involved, especially those sections of the community that are the most vulnerable and who will benefit most from the app. However, they may not trust an application that has the capability to be used for other means, which contains data that has recorded their movements and associations.

The evidence shows that up to one third of those who have already been diagnosed with a health condition will not trust the app. So how can we increase their confidence? By enlisting representatives they trust, in addition to the normal channels of healthcare delivery. Small businesses, charities and community associations can play a key role in communicating the message and encourage uptake through their trusted relationship with their respective communities. We believe organisations operating in this area will embrace the deployment of this app with some assistance from relevant government agencies.

Digital trust

Trust in the Government is in many ways a political issue and has been widely discussed in the media. Recent research indicates that trust in Government and other institutions has increased during the coronavirus crisis. During the pandemic we have seen the Government engage more pragmatic medical and other operational executives to help build trust, which has proven to be effective.

There is a curious bias in the issue of trust. Most mobile phone users do not appear to contemplate or worry about the issue of trust when using apps, particularly regarding location tracking. Commercial app providers have no great motivation to be trustworthy, and quite demonstrably many are not. When they ask users to trust them because they comply with the regulations, they are essentially asking the user to trust the Government.

Most phone users make no effort to suppress the sharing of their personal information through other apps. They express few concerns over the tracking of their movements and their interactions with others. This is largely because this tracking provides data and profiling through services that benefits them.

A lack of trust in government is not unique to Australia. Some aspects of it are imported, as is mobile phone technology. We need to find a way to have a discussion in Australia that grants us the luxury of trust in the institutions upon which we rely. Our politicians have not made it easy, but the current leadership has, overall, done well during the coronavirus crisis and this affords us a small window for a more reasonable discussion.

An important aspect of trust is whether guarantees made about the app can be checked by an independent authority, in the manner that an independent auditor verifies the financial accounts of companies. Auditing of software and how data has been used is still not especially mature. In order to facilitate checking of the software, one needs to ensure that the software has been written in a way that makes it easy to audit.

The other question is the independence of the auditor. There have been many documented instances of a lack of independence. The Government can readily address this issue by appointing an appropriate authority to give an independent assessment of any guarantees about the software and the usage of data.

Explaining the Benefits

A public health perspective is important to provide a basis as to ‘why’ uptake is needed. The ‘reason why’ needs to be addressed to explain the benefits beyond the individual. The Pearcey Foundation applauds the existing launch materials as an excellent start on this sustained journey of regular communications to the nation. As part of the on-going communications process, there will be a need to answer genuine community concerns:

Why you should sign up to and use the COVIDSafe app?

- It is for your own protection and that of your family members, as well as those you may come in contact with as society opens up again.
- Your health is your most critical concern. The app will help you to know when you have been exposed to the virus when out in public places.
- Early detection and intervention has been shown to be the best course of action for you and your family.
- If you have a diagnosed chronic health condition, then you may be at higher risk of infection and development of fatal health conditions.

Why you should trust the Government to collect and use your tracing data in an emergency?

- This virus spreads very rapidly through many channels of our community and the Australian Government is the most appropriate body to manage a nationwide emergency that crosses State borders.
- Every precaution and law to protect your rights and liberties as well as the use of the tracing data is being taken on a national basis for the benefit of the community and not for any other purpose.
- Access to your data will take place only in the event of a risk to your health being identified.

Why I should encourage my family, friends and associates to use the COVIDSafe app?

- The greatest benefit is gained when the majority of Australian citizens are using the app.
- Identifying those at risk is more efficient when there are no gaps in the data.
- You would not want someone to infect a member of your family and not be notified early because someone decided not to allow their proximity data to be traced.

The Bottom Line

The Pearcey Foundation wholeheartedly supports the introduction of the COVIDSafe tracing app and encourages all Australians to download it and use it. We believe the Government has clearly addressed the privacy, security and other concerns. But we also believe industry and community organisations need to collaborate with the Government as it continues to encourage people to use the app, and so allay community concerns.

This can be achieved through total transparency at every stage of the process. It needs the right messaging, from the right people, through the right channels. The app will only succeed if it achieves a critical mass of usage – it is not enough to build it and hope they will come.

Pearcy Foundation COVID-19 Working Group
27 April 2020

- *Susan Andrews, ICT Consultant and Mentor*
- *Martin Aungle, Director, Explore Communications*
- *Jo Dalvean, Project Manager, Research Data Services, RMIT University*
- *Colin Farrelly, Principal, Indago Partners*
- *Wayne Fitzsimmons OAM, Chair, Pearcey Foundation*
- *Simon Foster, Chair, Pearcey NSW and General Manager, Asia-Pacific, Storecove*
- *Paul Gampe, Chair, Pearcey Queensland*
- *Jordan Green, Chair, Pearcey Victoria, and Melbourne Angels*
- *Rick Harvey, CEO, Layer Security*
- *Kelly Hutchinson, Deputy Chair, Pearcey Foundation and Founder DSI4AU*
- *Dr Philip McCrea, Former Director, Austrac and CEO, ac3*
- *Graeme Philipson, Analyst, writer and computer industry historian*
- *Len Rust, Analyst, mentor and facilitator. Founder, The Rust Report*
- *Dr Elaine Saunders, Chair, Innovation Precinct Industry Advisory Board, Swinburne University*
- *Dr Leon Sterling, Professor in the School of Computing and Information Systems, University of Melbourne*
- *Denis Tebbutt, Chairman, Pearcey Institute*
- *Dr Peter Thorne AM, Former Head of the Department of Computer Science, University of Melbourne*

About the Pearcey Foundation

The Pearcey Foundation was founded in 1998 to celebrate Australia's ICT heritage. It is named after Australian computing pioneer Trevor Pearcey, who designed and built the world's fourth computer, CSIRAC, in 1947.

The purposes of the association are to: advance awareness, knowledge and public recognition of ICT and related innovation and entrepreneurship in Australia; promote public debate and research into ICT policy in Australia to advance the socio-economic development of the nation encouraging investments in the ICT sector; and champion the social and public value of ICT to benefit all sections of Australian society.

The Foundation operates broadly across the Australian Information Communication Technologies (ICT) sector celebrating achievements through national and state awards including the Pearcey Entrepreneur of the Year, Pearcey Hall of Fame and Pearcey Medal.

For more information contact:
Wayne Fitzsimmons OAM
Chair, Pearcey Foundation
wayne.fitzsimmons@m-group.com.au
+61 418 382 625

Pearcey FOUNDATION

The Pearcey Foundation Inc. is a registered charity with the ACNC
Level 1, 159 Dorcas Street, South Melbourne, Victoria 3205
admin@pearcey.org.au
www.pearcey.org.au
ABN: 78091361382