Questions and Issues Around the COVIDSafe App

Pearcey Foundation Response Paper

Overview

On 28 April the Pearcey Foundation released a Discussion Paper on the Australian Government's COVIDSafe tracing app. The paper can be found on our website at: https://pearcey.org.au/blog-pearcey-covidsafe-app-paper/

The purpose of a Discussion Paper is to encourage discussion. That is just what has happened. There was a substantial response, with articles in the press, the whole paper included with the Engineers Australia newsletter, and dozens of emails from the technology community.

The Pearcey Foundation would like to thank everybody who took the time to comment. Many of these observations are important contributions to the debate. This Response Paper summarises these views and looks at the issues they have raised in light of subsequent developments. We also include many references to articles and other material about COVIDSafe.

The Paper is presented in the form of a number of questions, with relevant comments and references. We repeat our recommendation for all Australians to download and use the app. Our original conclusion that the advantages far outweigh the concerns still stands. Indeed, it has been strengthened by the responses we have received and subsequent events.

Are the security risks worth it?

A key issue with COVIDSafe is the concept of the trade-off. What do you get compared to what you give up.

There is a whole industry — risk analysis — dedicated to the theory and practice of security trade-offs. The essence of risk analysis is to determine the most efficient use of time and money on mitigating any risk. For example, a power failure may be tolerable in a business, but in a hospital it cannot be tolerated, so back-up generators need to be put in place.

In a risk assessment, the critical assets are identified, the likelihood of failure determined, and the impact on the system or business of any failure is assessed. Trade-offs also apply to an attacker. Hackers will choose the easy targets first. There is a cost-benefit to them. The hacker will tend to go after the easy-to-break businesses, such as those with unpatched systems, rather than those that are well protected. Equally, the hacker may spend a lot more time and effort going after juicier systems, such as a financial or payroll system because the rewards are so much higher. This means that it is unwise to concentrate high value information in a single place, for example all medical data in a single database.

Is Bluetooth safe?

Much of the feedback concerned the app's use of Bluetooth and its vulnerabilities. The Pearcey Committee responsible for the Discussion Paper agreed that the Government clearly retained competent software developers and architects to define and code this app. They had high levels of skills in the areas of security and privacy, as demonstrated by delivery of a high quality app.

One of our committee members, Mr Rick Harvey, commented at length. He is an acknowledged expert in this area and is recognised internationally for his intellectual contributions to security matters. He believes that while there are risks with Bluetooth, they are not significant enough to change our recommendations. A key issue with Bluetooth, he believes, is one of scale.

A Bluetooth attack is a proximity attack, and is risky for the perpetrator because of the need for physical presence and timing. It relies on the attacker being nearby and performing a man-in-the-middle attack along with a sequence of interactions with the phone to pull it off. It doesn't scale. The chance of hundreds of attackers going after millions of people is statistically insignificant. Compare this to your risk of being hit by a car. A car accident is much more likely than a Bluetooth attack and the impact is much worse.

Now think of it from the attacker's point-of-view. Random attacks are of marginal utility to the attacker. There is no guarantee that the attack will succeed and no guarantee that anything valuable will come from a compromised phone. In the case of COVIDSafe, everything in the app is encrypted, so of zero value to any attacker. It's just not worth the attacker's time and effort.

Endpoint attacks don't scale. A much higher rate of return will come from an attack on a centralised database. Here COVIDSafe has a different set of safeguards, and these are the ones that need to be strongest. There was much discussion about emerging alternative initiatives, with even more anonymity and security built in. But these are months away and the Australian Government is in a rush to get something out. We believe that what they have released, in the time available, is an acceptable trade-off.

Over half the smartphones on the planet have Bluetooth enabled, because of its convenience, e.g. wireless earphones, connecting to the car, etc. It is unlikely the COVIDSafe app will cause any appreciable increase in the number of people enabling Bluetooth on their phone, so it won't change the overall risk to society. Criminals have little (or no) interest in Bluetooth attacks because there are so many other, bigger juicier targets, with much greater returns. By analogy, fisherman don't try and catch minnows one-at-a-time if the pond is a smorgasbord of sea life.

Does the app actually work?

Quite apart from the privacy and security issues, there is the important question of whether the app will actually work as intended. One article on the ABC questioned whether it functions properly on Apple's iPhone, which disables Bluetooth for background apps: https://www.abc.net.au/news/2020-04-26/coronavirus-tracing-app-covidsafe-apple-iphone-covid-19/12187448

Canberra academic and consultant Dr Roger Clarke has written two papers, one of which examines 'The Effectiveness of Bluetooth Proximity Apps in Tracing People with COVID-19 Exposure Risk': http://www.rogerclarke.com/EC/EBPA.html

The other looks at whether the numbers stack up. Even if it works, will it be worth the effort?
http://www.rogerclarke.com/EC/CSAF.html

A British medical paper examines the effectiveness of isolation, testing, contact tracing and physical distancing:
https://www.medrxiv.org/content/10.1101/2020.04.23.20077024v1

Is the 15-minute dwell time the right length?

As designed, the app records a contact only after 15 minutes of proximity. There was some debate over whether this is the right length of time, and comment about whether the ID lifetime, currently updated hourly, should be reduced to ensure it lasts no longer than 15 minutes, getting multiple IDs from the server in one request as it is done with the original Singapore version of the app.

Some found the 15-minute rule to be a problem. “Most people are not travelling on public transport and are being very careful around strangers, and do not come close to spending 15 minutes with them. In fact, those that are not already being careful like this are unlikely to ever download the app anyway.”

Given that there does not seem to be a data volume concern, perhaps the dwell time should be whatever the doctors say is the expected minimum time of exposure for either contact or airborne infection. That is a medical question, not a technical or privacy matter.

Why did the Government choose Amazon Web Services?

There was much discussion about the Government’s decision to host the back end of the COVIDSafe application on a server from Amazon Web Services. The use of AWS attracted some controversy because, as a US supplier, they are subject to the provisions of that country’s Patriot Act and other laws. The consensus is that, because the data is encrypted and held in Australia, this is not a valid concern.

On 6 May, Digital Transformation Agency chief Randall Brugeaud told the Senate Select Committee on COVID-19 that the DTA’s decision to use AWS was because of its “combination of hosting, development and operational services”. “One of the benefits of a company such as AWS is that it can scale very quickly and provide a broader range of services than simply hosting.” https://www.itnews.com.au/news/dta-chief-defends-aws-pick-for-covidsafe-547844

Nevertheless, from a trust point of view, it would have been preferable for the data to be in the custody of a local entity. The Pearcey Foundation believes an Australian provider should have been selected, and that the Government should explain why one was not.

Why can't we see the source code?

There was some concern that the source code of the server software has not yet been released to allow it to be verified for vulnerabilities, or otherwise audited, by independent trusted experts. Whilst the government has signalled its willingness to release the source code, we believe it should be made available as soon as possible. In the meantime, many people have been able to examine what the software does.

A detailed blog post from developer site GitHub looks at reverse engineering the app: https://github.com/vteague/contactTracing

How many downloads are needed?

The Pearcey Foundation believes the Government needs to explain the criteria which will determine the success of the app. It has been very vague about the numbers of downloads it believes will be needed. Figures of 40% and 50% of been mentioned, but there has been little mention as to how these figures have been determined.

We believe a better explanation will go a long way towards encouraging people to download the app. Sydney University has done a detailed analysis of the number of downloads needed: https://endorsecovidsafe.com/graph/

An article in the press explores much the same issue: https://itwire.com/telecoms-and-nbn/how-many-covidsafe-downloads-do-we-need.html

To our knowledge there has been no mathematical analysis of the proportion of any population that would constitute critical mass for an application such as this.

On 6 May the Senate Select Committee on COVID-19 was told by acting Health Department Secretary Caroline Edwards that the figure of 40% was not provided by her department and that no modelling had been done to arrive at the figure. Centre Alliance Senator Rex Patrick said he was "baffled" by the lack of analysis on what level of usage would be effective and that the Government had not done its due diligence, especially given the detailed modelling of the spread of the virus. Government and Health Department representatives have said only that the more people who use the app the better.

What more should the Government be doing?

Much of the feedback suggested things the Government should be doing to improve take-up of the app and to better explain its workings and its implementation. These included:

- Legislation to ensure removal of all data after a use-by date.
- An independent review of all security and other technical issues.
- A more targeted and persuasive marketing campaign, where different groups are given tailored messages, delivered by someone trustworthy, and based on a clear value proposition developed for that specific group.

- An argument needs to be made about how a more widespread uptake will help in planning the exit from the crisis. "If you want restrictions lifted, download the app!". Or perhaps the targeted marketing and messaging could address the future need more explicitly.

- A succinct statement about how the target number of downloads was decided upon and what percentage of that target is enough to provide meaningful results in case of an outbreak.

Is the level of uptake fast enough?

As of 6 May 2020, there have been over five million downloads of the app, which is a very high number. However, the rate of uptake is declining and there is no certainty that the number of downloads will reach the Government's target, however that is calculated.

For many people, there is no sense of urgency. "We don't need it now, while we're in lockdown. We don't need it until some time in the future." People may be putting off any serious thought until a time when they think it will be necessary.

For example, if you're living in a rural or regional community where the incidences of the virus are low, most people know each other and can easily keep track of who they are meeting with, then the app doesn't really add anything at all. If there's a local outbreak, the manual tracing by health authorities will work fine. But once restrictions are relaxed, perhaps those communities will be less apathetic when city people start heading there for their holidays, or when the locals need to visit the city.

There was some concern about the revelation by the Government that the data currently being collected cannot yet be used because the backend systems are not complete. This may have had the effect of slowing uptake, but the consensus is that the collection of historical data will be useful for tracing purposes.

What are the legal and legislative safeguards?

One of the key objections to the app has been the Government's unfortunate track record when it comes to privacy and security. Its promises over data retention have not been fulfilled and many prominent individuals have publicly said they do not trust the Government with the data.

On 3 May the Government released its COVIDSafe draft legislation:
https://www.ag.gov.au/RightsAndProtections/Privacy/Pages/COVIDSafelegislation.aspx

The legislation will go before Parliament in the week of 11 May. In the meantime, privacy protections have been governed by the Biosecurity Act: https://www.legislation.gov.au/Details/F2020L00480

The Pearcey Foundation believes the Government has done what is reasonably necessary to safeguard privacy, and that any concerns are unfounded. Note that a key aspect of the legislation is that no-one can demand that anybody else use the app. It cannot be used as a condition for entry to a shop or a venue, or for carriage on public or private transport, or for any other purpose. Its use is completely voluntary.

Who is recommending the use of the app?

The Pearcey Foundation endorses the use of the app. It has also been endorsed by many other individuals and organisations:

The Australasian Institute of Digital Health (AIDH), in association with the Australian Healthcare and Hospitals Association (AHHA), supports the app, conditional on nine principles that it believes should shape its design and governance. It is an excellent overview: https://digitalhealth.org.au/wp-content/uploads/2020/04/COVID-19-App_AIDH_V3.pdf

The Australian Information industry Association (AIIA) has come out in support of the app after receiving what it says is a detailed briefing from the Government: https://www.aiia.com.au/__data/assets/pdf_file/0008/102779/AIIA-Digital-Tracing-App-SB-final.pdf

A group of prominent Australian lawyers has published an open letter endorsing the app: https://drive.google.com/file/d/1gb7TRy_1b0vQeObyKhInxDhH3ua9EyIq/view

An open letter from Sydney University academic endorsing COVIDSafe: https://endorsecovidsafe.com/

A blog from Anthony Woodward at Accelera: COVID-19: https://accelera.com.au/covid-19-should-i-install-the-app/

A series of blogs from Crush the Curve, 'A group of concerned citizens': https://blog.crushthecurve.today/

Conclusions

The Pearcey Foundation believes that many of the concerns over the security and privacy of the COVIDSafe have some justification, but they are minor compared to the benefits from the widespread use of the app. Similarly, any technical issues are comparatively insignificant.

We recommend that all Australians download and activate the app.

Pearcy Foundation COVID-19 Working Group

7 May 2020

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

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