*University of New South Wales Law Research Series*

# AUSTRALIA'S 'COVIDVSAFE APP': AN EXPERIMENT IN SURVEILLANCE, TRUST AND LAW

**GRAHAM GREENLEAF AND KATHARINE KEMP**

[2020] *UNSWLRS* 40

UNSW Law
UNSW Sydney NSW 2052 Australia

**E:** unswlrs@unsw.edu.au
**W:** http://www.law.unsw.edu.au/research/faculty-publications
**AustLII:** http://www.austlii.edu.au/au/journals/UNSWLRS/
**SSRN:** http://www.ssrn.com/link/UNSW-LEG.html

# Australia's 'COVIDSafe App': An experiment in surveillance, trust and law

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia, and
Dr Katharine Kemp, Senior Lecturer in Law, UNSW Australia*

*Work-in-Progress Draft 30 April 2020 This draft will be updated periodically according to developments. Comments are welcome to graham@austlii.edu.au or to k.kemp@unsw.edu.au .*

**Contents**



* The following colleagues have provided valuable comments on this draft, but all content remains the sole responsibility of the authors: Anna Johnston; David Vaile; Nigel Waters, Genna Churches and Jill Matthews.

## An experiment in surveillance and trust

The joint Australian governments' coronavirus contact tracing app, marketed as 'COVIDSafe', was released on 26 April 2020 for public download by the federal government, together with an emergency Determination under the *Biosecurity Act* (with Explanatory Statement)[1] to govern its operation, a Privacy Impact Assessment (PIA) by a law firm (Maddocks),[2] with the Health Department's response to that PIA,[3] and (not least) the App itself and its privacy policy.[4]

It is a package intended to create sufficient public confidence to result in downloads of the app by a sufficient percentage of the Australian mobile-phone-owning population, for it to have a significant effect on the tracing of persons infected with the COVID19 virus.

This launch creates three new reasons why this public confidence is not yet warranted: insufficient transparency; misleading statements by the government about the operation of the app; and flaws in the regulations. These may be remediable. This article analyses the steps that Australian governments need to take if public trust is to be justified.

One deadline for remedying these defects is when Parliament resumes, which will occur briefly on May 12 (as far as is known), when it is expected that the government will introduce real (Parliamentary) legislation to replace the non-disallowable[5] Determination that currently provides the only legal protections against the app's misuse. In addition, a Senate Select Committee is already taking evidence concerning the app, with submissions due by 23 May. It can be expected that many submissions will highlight deficiencies in the app's legal protections and transparency, unless those matters are remedied before then. This is an unusual situation, because the test this time is not whether the government can simply get away with whatever it pushes through Parliament. It also has to convince the public to continue to 'vote with their phones' that they trust what the government is doing, by installing the app, and by not uninstalling it.

### The app's operation and effectiveness

The app is based on the similar architecture of Singapore's TraceTogether app, utilising Bluetooth technology to record when two mobile phones come within a defined proximity specified for the app. This proximity is believed to be 'within 1.5 metres for 15 minutes', in the case of the Singapore app, but critically undefined in the case of COVIDSafe, as explained later. Details of its proposed operation are set out in the Maddocks PIA, the app's Privacy Policy, the FAQs to the app,[6] and (very briefly) the Explanatory Statement to the Determination. Ministerial explanations about its operation have sometimes been misleading (discussed later).

According to this documentation, the use of the COVIDSafe model of a tracing app is voluntary (this claim will be examined later but is plausible). It does not involve any tracking of the location

---

[1] *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020*, 25 April 2020, with Explanatory Statement <https://www.legislation.gov.au/Details/F2020L00480/Download>

[2] Maddocks *Privacy Impact Assessment (PIA) Report*, 24 April 2020 (hereinafter 'Maddocks PIA')

[3] Department of Health *The COVIDSafe Application – Privacy Impact Assessment – Agency Response*, undated (before 26 April 2020) (hereinafter 'Health PIA Response')

[4] COVIDSafe Application (the App) and Privacy Policy

[5] *Biosecurity Act 2015* (Cth), s. 477(2).

[6] Department of Health *CORONAVIRUS CONTACT APP FAQS, undated* <https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-app-faqs-coronavirus-contact-app-covidsafe-faqs.pdf> (hereinafter 'App FAQs')

of phones (it does not utilise GPS technology), nor the time at which contacts occur. Information about 'proximity events' and other 'COVID app data' is stored on each mobile phone. Only when the possessor of one of the phones is tested positive for coronavirus are they requested (by State/Territory contact tracing personnel) to allow the list of proximity events and other 'COVID app data' recorded on their phone to be uploaded to the National CovidSafe Data Store (NCSDS), where the telephone numbers associated with each proximity event (but not other and other 'COVID app data') may be accessed by State/Territory contact tracing personnel, and used to contact the other parties whose phones have been recorded as involved in 'proximity events'. This app therefore has elements which are decentralised (proximity event data is held on individual mobile phones for 21 days until deleted) and others which are centralised (some proximity event data may be uploaded to the NCSDS in the event of a positive diagnosis). Some other models are more decentralised (for example, the Google-Apple proposed model), but we do not characterise the COVIDSafe app as either fully decentralised or centralised: it is a mixture. Like Singapore's, Australia's app can be regarded as more on the centralised side, since it requires decryption at the central server, and particularly given the unrestricted uploading of contacts.

## Australia's experiment

There are no clearly successful examples of similar contact tracing apps implemented in any country as yet. The percentage of mobile phones in a jurisdiction on which it is necessary to have an app installed for it to have a significant effect on contact tracing is, at a minimum, claimed to be 40%. Australian government officials have stated that their aim is at least 50%, and some experts claim that it needs to be 80%. 'Success' is therefore disputable.

Singapore's TraceTogether app, five weeks after release, is reported to have obtained less than 20% take-up, and Singapore now has a very significant 'second wave' of infections. Other countries claimed to have been successful in keeping infection rates low, and to have used apps as a significant part of their strategies (for example, China, Taiwan, South Korea, Israel), have not used apps similar to COVIDSafe, but have instead used apps which (variously) are compulsory to use, are used in combination with compulsory access to geolocation information, or are used in combination with compulsory privacy-invasive access to government registers, credit card information, and other contact-revealing data. They are not examples of the success of the COVIDSafe type of app.

The Australian government claims that, in the first three days of its release, 2.8 million people downloaded the app. How many will use it (it requires Bluetooth to be turned on) remains to be seen. An estimated 20 million Australians own mobile phones,[7] so the current download figure represents about 14% of the potential uptake. Public trust must become more widespread, before success is likely to follow.

How and when should the success of this experiment in supposedly 'benign surveillance' be measured and tested? The purpose of the app is primarily to identify persons (via their phones) who might be infected by COVID19, so that they can be tested, to help avoid possible infection of other persons if they test positive. The theory is that, if not for the proximity app, some of these potentially infected persons might have not been identified at all as part of contact tracing, or it may have taken longer to identify them, increasing the risk that they have infected other people in the interim. Australian governments have not published details of any proposed studies to test whether the COVIDSafe app will in fact achieve these goals, but in our view they must do so. This is the first of a number of transparency deficiencies in relation to the COVIDSafe app and its operation.

[7] 2019 estimates vary from 18.6 million (Roy Morgan) to 20 million (Statista)

## Transparency? No, Minister

Confidence needs to be based on public belief that the government is disclosing everything the public needs to know to make informed decisions as to whether to download the app. There is a lot missing.

### Justifications not disclosed

For the Health Minister to make the Determination under s. 477 *Biosecurity Act* on which the app's operation depends, s/he must be satisfied that the Determination's requirements concerning the app are 'likely to be effective' for its purpose, which is 'to make contact tracing faster and more effective, by encouraging public acceptance and uptake of COVIDSafe' (Determination cl. 4). The requirements must be 'appropriate and adapted' to that purpose, and 'no more restrictive or intrusive than is required in the circumstances'. The Determination's Explanatory Statement says the Minister relied on the advice of three officials to be satisfied that the Determination was necessary 'to prevent or control the … spread of COVID-19 in Australian Territory'. These advices by the CEO of the Digital Transformation Agency (DTA), the Acting Secretary of the Health Department, and the Commonwealth's Chief Medical Officer (CMO) have not been made public.

They should be made public, because this app should not be introduced unless it is effective, necessary and proportionate, based on convincing expert advice related to Australia's current situation. Unless the Australian public sees the advice, it cannot be sure of that. Ideally, there should be evidence – from health experts not politicians – that this app will be more effective than the same resources used to increase testing and (human) tracing.

### The secret source, and other flavours

Media reports cite Ministers saying that the source code of the app – or at least those parts of it which do not pose 'security issues' – will be made available in the coming weeks. On 18 April 2020, Minister Stuart Robert said 'The source code will be made public.'[8] In the Privacy Impact Assessment, Maddocks recommended public release of the source code for the app,[9] and the Department in its response agreed, 'subject to consultation with the Australian Signals Directorate's Australian Cyber Security Centre'. On 27 April 2020, the federal Health Minister said 'The source code will be released within two weeks. The reason for that is there's constant review of the safety and security. Our first task is to make sure that the security assessment is done and that there is absolute protection of privacy above all else but at the same time, working on the same basis as countries such as Singapore, we will be releasing the source code so as there's full assessment …'.[10]

If this means that only part of the source code for the app will be released, it strains credibility that this would increase trust, because of the possibility that malignant code could be in the non-disclosed part. In any event, even if the Health Minister's timetable is adhered to, the source code will not be released until the time before (or perhaps after) the legislation concerning the COVIDSafe app goes before Parliament in mid-May.

---

[8] Services Australia, Australian Government, 'Transcript: Doorstop interview, Gold Coast: The Hon Stuart Robert MP, Minister for Government Services' (18 April 2020) https://minister.servicesaustralia.gov.au/transcripts/2020-04-18-doorstop-interview-gold-coast

[9] Maddocks PIA Report, Recommendation 1.

[10] AM with Sabra Lane, 'Federal Health minister says govt will release COVIDSafe source code' (ABC website, 27 April 2020) https://www.abc.net.au/radio/programs/am/heath-minister-says-govt-will-release-covidsafe-source-code/12187634 (around 3:20 in the audio)

Some argue that an app based on the Singaporean TraceTogether model (which this is supposed to be, but without source code, how can experts be sure?) is not going to be as privacy-protective as one based on some other protocol (eg the Google-Apple model, or the European one). We are not in a position to say, but nor are experts unless they receive much more technical information, including source code.

### Privacy impact assessments and absences

The Maddocks' PIA report says is '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.' Some of these risks identified by Maddocks (summarised as seven risks where 'further work needs to be undertaken'[11]), and the responses of the Department of Health, are discussed in this article. The purpose of the PIA is to consider whether the app (and its proposed operation) has been developed, by the various federal, State and Territory agencies involved, to achieve compliance with the Privacy Act 1988, and particularly the Australian Privacy Principles (APPs).[12] Its purpose is constrained in this way, and is not to consider public policy issues, or 'privacy at large'.

It is a matter for serious criticism that the PIA was only made public at the same time as the app was made public, so there was no time for public consideration or debate, as the Australian Privacy Foundation has noted (among other defects of the PIA process).[13]

There is no mention in the Explanatory Statement of any assessment of COVIDSafe being made by the federal Privacy Commissioner. Nor does the PIA state that input was received from the Privacy Commissioner. While such advice from the Commissioner is not necessary under s. 477 *Biosecurity Act*, or as input into a PIA, some such advice to the public clearly is necessary in order to satisfy public concerns concerning privacy on as important a privacy issue as this. None of the 3 sources of advice mentioned in the ES are privacy experts – in fact they could all be considered as having conflicts of interest when it comes to privacy – so the Commissioner's opinion is necessary for public trust. It might not be sufficient, but it is necessary.

The federal Privacy Commissioner made a brief statement at the time of the release of the app.[14] The Commissioner 'said that important safeguards have been put in place', that it was positive that the government had accepted recommendations in the PIA, and that her office had provided advice to government as the PIA process developed. The Commissioner also noted that her office 'will have independent oversight of personal information handling by the app and the National COVIDSafe Data Store', has the capacity for audits and complaint investigation, and will monitor the adoption of the PIA recommendations. The Commissioner has not made any statements to the public about the necessity and proportionality of the COVIDSafe app.

## Flaws in the Determination

The Determination made by the Minister for Health under s. 477 is a non-disallowable instrument, and one that can be modified or repealed and replaced by the Minister at any time. A step such as a contact tracing app which could pose extreme risks to many civil liberties including privacy,

---

[11] PIA Report [3.2]

[12] PIA Report [2.5]

[13] Australian Privacy Foundation (Media Release) 'How [NOT] to earn public trust for the Contact Tracing App?', 27 April 2020 <https://privacy.org.au/2020/04/27/how-not-to-earn-public-trust-for-the-contact-tracing-app/>

[14] Australian Privacy Commissioner 'Privacy protections in COVIDSafe contact tracing app' 26 April 2020 <https://www.oaic.gov.au/updates/news-and-media/privacy-protections-in-covidsafe-contact-tracing-app/>

freedom of movement and freedom of association, should have been exposed to full Parliamentary scrutiny and debate, and the passage of legislation, before the app was released. The government would no doubt say that the extreme risks posed by the pandemic created a situation of urgency which justified bringing the app into operation with no prior opportunity for debate. But by concealing the advices on which the Minister's decision was made, there is no credible expert evidence of this.

Having this Determination as a fig-leaf of public protection is better than no law at all, but only on the assumption that it will very rapidly be replaced by legislation which cannot be overridden by Ministerial fiat. If the Determination lapses without legislation being enacted, this would be a disastrous result. Parliament should now decide what law prevails in the pandemic we already know we are in.

The content of the Determination is the only guide we have as to what is likely to be in that legislation, so identification of how it needs to be improved is important, both in terms of improving what is already there, and adding missing protections. We will now undertake this.

## National COVIDSafe Data Store (NCSDS) and the CLOUD

There are circumstances where the US Clarifying Lawful Overseas Use of Data Act (2018) (CLOUD Act) could be used to compel Amazon Web Services (AWS), as a provider of a remote computing service that is subject to US jurisdiction, to disclose the contents of a record to the US government even if the record is located outside the US. At this stage, AWS is not entitled to bring a motion to quash or modify that legal process in a US court, on the basis that disclosure would contravene a law of Australia, since the Australian government is not a "qualifying foreign government" under the CLOUD Act. Home Affairs Minister Dutton introduced a bill in March 2020[15] (the IPO Bill) essentially to allow Australian and US law enforcement agencies to reciprocate and cooperate in obtaining access to communications and records under the CLOUD Act processes. If the IPO Bill is passed, the Australian government may become a "qualifying foreign government" under the CLOUD Act.

An answer to the question whether records held by AWS as part of its COVIDSafe contract would be subject to the US CLOUD Act or the IPO Bill is not straightforward. Given the uncertainties, and the importance of the issue for public confidence, two conclusions follow:

(i) Whatever advice the government has received concerning the accessibility of COVID app data under the CLOUD Act should be made public; and

(ii) The IPO Bill should not be passed without an amendment to clarify that it excludes COVIDSafe app data or data derived from COVIDSafe app data from being subject to any agreement allowing US access.

## Defects of scope and missing definitions

The Determination attempts, in clause 6, to establish a comprehensive set of controls over what it calls 'COVID app data', but its current wording fails to capture and protect critical personal data created and used in the process of COVIDSafe contact tracing. This section shows deficiencies in four areas of defining scope: defining 'COVID app data'; application to State/Territory health authorities; de-identified data; the lack of a definition of 'proximity'; and uncertainties around who controls the 'National COVIDSafe Data Store'.

---

[15] Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (IPO Bill).

***'COVID app data'*** The first deficiency lies in the scope of 'COVID app data' itself, which is defined in cl 6(3) as data relating to a person that 'has been collected or generated through the operation of' the COVIDSafe app and 'is, or has been, stored on a mobile telecommunications device'. This definition is unlikely to capture data at the heart of the COVIDSafe scheme, namely the decrypted contact logs of infected users at the NCSDS. While the original encrypted contact records would come within the definition, decrypted contact logs are not collected or generated through the operation of the app, nor are they stored on the user's device. The definition should be amended to expressly include data transformed or derived from the data originally collected or generated through the operation of the app, including data transformed or derived by state / territory health authorities.

***State/Territory health authorities*** Clause 6(1) creates a general prohibition ('a person') on all collection, use or disclosure of COVID app data outside those specifically permitted under cl 6(2). It is not clear whether this general prohibition applies to state/territory health authorities. Further, while the note to cl 6(2) states that the *Privacy Act 1988* continues to apply except to the extent that it is inconsistent with the Determination, pursuant to s. 477(5) of the *Biosecurity Act*, the *Privacy Act* would not usually bind the state/territory health authorities, which are instead subject to state/territory legislation. The Maddocks PIA notes that, aside from community concern about use of the data by state/territory health authorities:[16]

> 'There is also an additional risk because Contact Tracers in the different States and Territories will be subject to different privacy regimes in relation to their handling of any personal information, with some regimes being more comprehensive than others.'

The PIA recommends that the Department of Health should enter contractual arrangements with the state/territory health authorities to ensure the privacy protections are enforceable as contractual obligations against these authorities once the data 'has been disclosed to Contact Tracers' and is then beyond the Department's 'effective control'.[17] The Department's Response accepts that there is this limitation in the Commonwealth's control, and that 'other arrangements' will be necessary, but it only refers to developing an 'acknowledgment' by State/Territory public health officials of the 'terms and conditions of use' of the information.

The problem with such 'acknowledgments' is that they give the individuals whose data is at risk of abuse no rights to sue for breaches of any of the protective provisions by State/Territory officials,

The PIA recommends that 'ideally' State and Territory officials would be required to comply with the Privacy Act 1988 as if they were an APP entity, so that there is uniform protection across jurisdictions. We agree that the COVIDSafe Act should do this, but there are constitutional issues here which make the possible extent of Commonwealth powers uncertain.

Nevertheless, the legislation should clarify that it is the Commonwealth's intention that the general prohibition under clause 6(1), and the Australian Privacy Principles, apply to the state / territory health authorities in respect of their handling of the COVID app data.

***De-identified data*** Aside from contact tracing, the Determination permits the government to use the COVID app data 'for the purpose of, and only to the extent required for the purpose of, producing statistical information that is de-identified' under cl 6(2)(e). 'De-identified' is given the same meaning as under the *Privacy Act 1988*. However, given the increasing difficulty in successfully de-

---

[16] Maddocks PIA, p 56 paras 6.19-6.20.

[17] Maddocks PIA, Recommendation 12.

identifying personal data,[18] and the government's recent failure, for example, to adequately de-identify health data which was released to the public and subsequently re-identified,[19] trust is likely to require more than this broad concept of de-identification. Serious concerns about risks of supposedly de-identified data could be fatal to the continuing trust on which the COVIDSafe app depends.

The legislation should not rely solely upon the Privacy Act definition, but should also be required to specify (at least in delegated legislation) what form of de-identification will be used, what sort of de-identified data the government will use, and what entities will carry out these processes. It should provide for an independent assurance process for this de-identification, including the involvement of the COVIDSafe Privacy Advisory Committee that we recommend.

***'Proximity'*** There is no definition of 'proximity' in the Determination. It is only mentioned when a person is defined as being 'in contact' with another person, namely when the COVIDSafe app indicates 'the person may have been in the proximity of the other person'. However, the Determination does not indicate when this is so, it depends simply on the technical settings of the COVIDSafe app, and can therefore be changed at any time by those controlling the app (including through updates). Proximity is, in popular belief, '1.5 metres for 15 minutes', but as discussed below, this is a misconception promoted by the government. The app collects a far broader amount of data (on 'bystanders') than the data which is eventually passed to Contact Tracers, which is where the substantive meaning of 'proximity' resides.

This is an unjustifiable situation: the extent of the interference with privacy posed by the COVIDSafe app is left completely unexplained in its current regulatory instrument, and is in fact left completely to the (changeable) discretion of those who control the app. That controller is, it seems, the un-named party acting 'by or on behalf of the Commonwealth' in providing the app (cl. 6(3), definition of 'COVID app data'), a controller that can be changed at the whim of the government. Is it the Health Department, or perhaps Homeland Security – or might it be in future? The COVIDSafe Act must define both 'proximity' and the controller of the COVIDSafe app, in ways that cannot be changed without further legislative amendment.

***'National COVIDSafe Data Store'*** The'National COVIDSafe Data Store' (NCSDS) is defined as 'the database administered by or on behalf of the Commonwealth for the purpose of contact tracing'. The NCSDS is referred to nine further times in the Determination. Which Commonwealth body 'administers' this entity? It will make a great deal of difference to public trust if the answer – either now or in future – is the Department of Homeland Security, or some other law-enforcement or surveillance-oriented agency, rather than the Department of Health. Are they the same agency that is the controller of the COVIDSafe app

It does not matter who the Explanatory Statement, the FAQs, or other explanatory material says it is, or who it actually is, at the moment. The only thing that matter is that the Determination is silent. If there is to be public trust, then the COVIDSafe Act must state who is this data controller, , in ways that cannot be changed without further legislative amendment.

---

[18] See, eg, Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2019) 36 *Law in Context* (forthcoming).

[19] OAIC, 'Department of Health: enforceable undertaking' (OAIC website, 23 November 2018) https://www.oaic.gov.au/privacy/privacy-decisions/enforceable-undertakings/department-of-health-enforceable-undertaking/

## Controlling dealing with 'COVID app data', and its deletion

The 'Treatment of COVID app data', set out in clause 7 of the Determination needs improvements in the COVIDSafe Act, as follows:

- In clause 7(1) 'consent of the person who has possession or control of the device' is not sufficient protection to ensure individual consent to upload, because a Health Dept or Police Officer could have possession or control of a mobile phone. The words 'and of the person who normally uses the device' need to be added.
- Clause 7(3) is a necessary instance of data localisation, but its effectiveness in the face of the US CLOUD Act must be established.
- Clause 7(5) requiring deletion 'after the COVID19 pandemic has concluded' does not sit very well with the s. 477(4)(e) requirement that requirements must be 'only as long as is necessary'. The Explanatory Statement says this 'would be determined based on advice from the Australian Health Protection Principal Committee'. Those words should be added to the COVIDSafe Act's equivalent of cl 7(5) to provide assurance that the objective advice of health experts, not political advice, should decide when the pandemic has concluded. The advice should also be required to be made public.
- The Clause 7(5) requirements for deletion do not deal with data held outside the NCSDS, particularly that which is held by State/Territory health authorities. Most of this data will not relate to individuals who have received a positive diagnosis, they have only been identified as potentially relevant contacts to trace. Given the importance placed on the voluntary nature of the app, there needs to be effective deletion requirements for this data, if the public is to trust government assurances that this is temporary collection and use of data. Whether Commonwealth legislation can establish such a regime is questionable. This highlights the need for complementary State and Territory legislation, as discussed below.
- The note to cl 7 says its provisions will override any more permissive provisions in the Privacy Act, which is essential. That is not exactly what Biosecurity Act 2015 s. 477(5) seems to say, but it is probably effective in ensuring that the Privacy Act is over-ruled. The COVIDSafe Act needs to ensure that the same result is achieved.

## Improving the anti-coercion clauses

The provisions of cl 9 'Coercing the use of COVIDSafe' are generally a very good start to dealing with a serious potential problem, and are what we have previously been calling for to prevent 'pseudo-voluntary compliance'.[20]

Some important improvements are nevertheless necessary:

- Clause 9(1)(b) should say 'installed or in operation', for avoidance of doubt.
- Clause 9(1)(b) needs to have added at its end 'or disclose whether they do have it installed or in operation'.
- Clause 9(1)(c) should have added 'or to any other location'.
- Clause 9(2) is very broad and protective, with (a)-(f) not requiring alterations.
- However, an additional sub-clause should provide that the prohibitions in (a)-(c) also apply to any requirement that the prohibited conduct is a condition of exceptions to 'stay

[20] G. Greenleaf 'Australia's COVID-19 contact tracing app must not be pseudo-voluntary', *UNSW Newsroom*, 2020 https://newsroom.unsw.edu.au/news/business-law/australia%E2%80%99s-covid-19-contact-tracing-app-must-not-be-pseudo-voluntary

at home' orders and similar orders by any government, including under any emergency legislation.[21]

- Clause 9(2) (g), (h) and (j) need to be amended to make them consistent with the changes suggested above.

The scope of cl 9's equivalent in the COVIDSafe Act has to include all State and Territory government bodies and public corporations. The federal Attorney-General should be required to produce advice to this effect, other complementary State and Territory legislation (discussed below) will be necessary for this aspect as well.

## Data minimisation – over-collection of non-proximate device data

A very significant issue, which is contrary to the government's statements in the media and popular understanding of the app, and has the capacity to undermine trust, is that the Bluetooth collection of data extends to data about all other mobiles which have the app installed, and not only such devices as meet the proximity criteria.[22] The Government Services Minister has repeatedly stated in the media – and the media widely and constantly reported – that COVIDSafe only records contacts with other app users which are within 1.5 metres of the user for at least 15 minutes.[23] The Minister and others have also stated that, when an app user tests positive and gives their consent, the app only sends a log of contacts with devices of other app users who were within 1.5 metres of the user for at least 15 minutes.[24] Neither of these statements is true, but we are not aware of the government taking steps to alert the public to these misstatements and correct this misunderstanding.

---

[21] For a similar proposal, see Law Council of Australia *Principles for the design of a COVID-19 contact tracing app* April 2020, Principle 2.

[22] See Department of Health *CORONAVIRUS CONTACT APP FAQS, undated* <https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-app-faqs-coronavirus-contact-app-covidsafe-faqs.pdf>

[23] See, eg, Damien Haffenden, 'Coronavirus Australia: How COVID-19 tracking app will work' (Sunrise, 20 April 2020) https://7news.com.au/sunrise/on-the-show/coronavirus-australia-how-covid-19-tracking-app-will-work-c-982093 reported:

> '(It's) simply an app or digital way of replicating a manual process,' Government Services Minister, Stuart Robert told *Sunrise*.
>
> 'Right now, if you're (sic) tested positive for COVID-19, health officials will sit down and talk you through who you've been in contact with,' he said.
>
> 'The COVID trace app simply digitises that process, *so if your app has been within 15 minutes duration of someone, within 1.5 metres proximity, there'll be a swapping of phone numbers.* [emphasis added]
>
> 'That will stay on your phone and then of course if you test positive, you'll give consent, and those numbers will be provided securely to health professionals and they'll be able to call people you've been in contact with.'

See further Shannon Jenkins, ''No one is tracking you': Stuart Robert urges public to trust COVID-19 tracing app' (The Mandarin online, 17 April 2020) https://www.themandarin.com.au/130941-no-one-is-tracking-you-stuart-robert-urges-public-to-trust-covid-19-tracing-app/; Brett Worthington, 'Government insists coronavirus tracing app will not track people's locations, says data will be stored on phones' (ABC News online, 20 April 2020) https://www.abc.net.au/news/2020-04-20/government-insists-coronavirus-tracing-app-wont-track-locations/12163756; Evan Young, 'What is COVIDSafe, Australia's controversial new contact tracing app?' (SBS News online, 26 April 2020) https://www.sbs.com.au/news/what-is-covidsafe-australia-s-controversial-new-contact-tracing-app

[24] See, eg, Damien Haffenden, 'Coronavirus Australia: How COVID-19 tracking app will work' (Sunrise, 20 April 2020) https://7news.com.au/sunrise/on-the-show/coronavirus-australia-how-covid-19-tracking-app-will-work-c-982093; Max Koslowski, 'How does the coronavirus app work?' (Sydney Morning Herald online, 29 April 2020) https://www.smh.com.au/politics/federal/how-will-the-coronavirus-app-work-20200421-p54ltg.html

According to the PIA:[25]

> 'After the registration process is complete, if the User's App is open and running on the User's device, the App will use the enabled Bluetooth technology to continually seek out Bluetooth signals from other Apps that are open and running on the devices of other Users. When a Bluetooth signal of a User's device detects the Bluetooth signal of another User's device, each User's App will create an encrypted file (a Digital Handshake) and store this on the User's device.'

The PIA goes on to state:[26]

> 'A Digital Handshake will only include the following information (stored in an encrypted form on the User's device):
> 8.24.1 that there was contact between the User and the Contact User;
> 8.24.2 the Contact User's Unique ID;
> 8.24.3 the Bluetooth signal strength during the Digital Handshake; and
> 8.24.4 the date and time of the Digital Handshake.
> A separate Digital Handshake is created every minute.'

The COVIDSafe App records *all* 'Digital Handshakes' between users' phones when they are in Bluetooth signal range, regardless of duration or the distance between users. If a user tests positive and gives their consent, the App transmits to the National COVID Data Store a log of *all* Digital Handshakes that user's phone has recorded over the previous 21 days, regardless of duration or the distance between users.[27] When the log of encrypted user IDs is received at the National COVID Data Store, *all* contacts' encrypted IDs are decrypted, regardless of duration or the distance between users.[28] At that point, the Department of Health now states that it will put in place restrictions to ensure that contact tracers will only be permitted to access the contact details of users who were within the risk parameters, currently 1.5 metres of the infected user for at least 15 minutes.[29]

A corollary to the above is that, there will be users who have not tested positive to COVID-19, and have not been within the required proximity of a person who has tested positive, but who have come within Bluetooth signal range for any period during the past 21 days (ie outside the required proximity), data about whom will be uploaded to the National COVID Data Store and decrypted, because someone who never came within the required proximity to them tests positive and provides their consent. These users are the 'unexpected bystanders' of COVIDSafe tracing.

This means that vastly more potentially revealing data concerning a person's movements, associations etc may be collected than accords with the popular understanding, and it is data that is irrelevant to contact tracing.[30] Whatever are the fine details of the data collection, uploading and filtering involved, it is difficult to see that data minimisation principles have been observed. This serious over-collection of personal data greatly amplifies the dangers of the all risks of unauthorised access to, and disclosure of data from, the NCSDS central store, as well as the risks of decryption of the data on the mobile device itself.

---

[25] Maddocks PIA, p 19 para 8.21.

[26] Maddocks PIA, pp 19-20 para 8.24.

[27] Maddocks PIA, p 21 para 8.37, p 49 para 3.33.

[28] Maddocks PIA, p 21 para 8.39.

[29] Department of Health Response to PIA, p 17.

[30] See further Roger Clarke 'The Effectiveness of Bluetooth Proximity Apps' 29 April 2020 <http://www.rogerclarke.com/EC/EBPA.html>

These increased and unjustifiable risks support the need for remedial actions able to be taken by the data subject (mobile device owner). Technical solutions may also alleviate the problem.

In the PIA, Maddocks recommended that the Department investigate whether it is technologically possible to:[31]

- Only record handshakes on the device if they meet the risk parameters;
- If that is not possible, only upload handshakes to the National COVID Data Store upon a positive test if they meet the risk parameters;
- If that is not possible, automatically delete (or, if not, de-identify) handshakes that do not meet the risk parameters at the National COVID Data Store; or
- If that is not possible, limit access at the National COVID Data Store to handshakes that meet the risk parameters.

In its response to the PIA, the Department of Health only stated:[32]

> 'Agreed. Access restrictions to Digital Handshakes will be put in place. Personnel in State and Territory health authorities can only access Digital Handshakes which meet the risk parameters.'

The government has not indicated whether it is technologically feasible to meet any of the first three options which would minimize the data collected, transferred and stored. It only indicated it was opting for the alternative which maximizes the personal information collected at the National COVID Data Store. The government should investigate which of the first three options is technologically feasible, and implement that which minimises the data collected.

### Other data minimisation issues

Aside from this issue, it should be noted that the Determination does not define the types of data that will be collected and stored on the device. This information is only provided in the Privacy Policy. The legislation should specify the types of data that will be collected and stored on the device.

According to the Privacy Policy, as part of the use of COVIDSafe, the Department of Health will collect:

- The users' registration information, namely: their mobile phone number; their name;[33] their age range;[34] and their postcode;
- Information about the user's encrypted ID when the COVIDSafe App is open or running on their device;

---

[31] Maddocks PIA, p 13 Recommendation 18.

[32] Department of Health Response to PIA, p 17.

[33] While the Privacy Policy states that this may be a 'pseudonym or fake name', the App's user interface requests 'Full name' and shadows 'Firstname Surname'.

[34] The App's user interface requires users to select one of the following options: 0-15; 16-29; 30-39; 40-49; 50-59; 70-79; 80-89; 90+. Query whether medical evidence supports the need to distinguish age groups at this level for the purpose of triage. Would it be sufficient, eg, to have one rather than three options for over-70s?

- Information that the user has tested positive to COVID-19 if the user agrees to a health official sending the user an SMS to enable the user to upload their contact data;
- The user's contact data over the previous 21 days if they consent to upload their contacts after testing positive to COVID-19; and
- The user's contact with any other user who tests positive to COVID-19 and has been within Bluetooth range of the user for any time in the past 21 days.

The Privacy Policy states that '[a]n encrypted user ID will be created every 2 hours'. The use of the passive voice means it is not clear where the ID is created, but it seems from the PIA that the encrypted ID is created by National COVID Data Store.[35] The Privacy Policy continues, 'This will be logged in the National COVIDSafe data store …, operated by the Digital Transformation Agency, in case you need to be identified for contact tracing.'

This frequency of cycling encrypted IDs and logging those IDs with the Data Store has two implications. First, creating a new encrypted ID only every 2 hours (as opposed to, say, 15 minutes) increases the risk that a user's series of contacts will be connected. Second, logging a user's encrypted IDs with the Data Store every 2 hours (as opposed to, say, once a day) means that the government is able to more closely monitor a user's usage of the app, and this is in operation.[36]

## Individual enforcement and remedies

The Determination's only means of enforcement is through the criminal law. Its various provisions say that 'a person' (Commonwealth official, private sector party, and at least in some cases State or Territory officials) 'must not' do various things. Failure to comply with Determination requirements is an offence under s. 479 *Biosecurity Act 2015*. Maximum penalties under s. 479 are $63,000 or 5 years imprisonment or both.

Desirable though such criminal penalties are, they are manifestly inadequate as a means of enforcement. The Commonwealth is unlikely to prosecute its own officers, much less those of States or Territories. Prosecution of employers, landlords, café owners etc under cl. 9 will be sporadic, if it ever occurs. If criminal penalties are the only means of enforcement of protections in relation to the COVIDSafe app, there is no reason why the public should have any confidence at all in them. It is very likely that most civil society organisations would argue that they are largely worthless protections, and should not be trusted.

The legislation governing the COVIDSafe app ('COVIDSafe Act') must provide remedies that individuals affected by breaches of the law can initiate for their own protection, and to obtain

---

[35] The Maddock PIA, p 19 paras 8.17-8.18, states:

> 'We understand that the National COVIDSafe Data Store will automatically generate new Unique IDs for each User every two hours and send these new Unique IDs to the User's App.
>
> The App will only accept the new Unique IDs if it is open and running. If the App successfully accepts the new Unique ID, an automatic message will be generated and sent back to the National COVIDSafe Data Store. This message will only effectively indicate a 'yes (new Unique ID successfully delivered)' response to the National COVIDSafe Data Store. If the App is not open and running, it will not be able to accept a new Unique ID. It will continue to store the previous Unique ID and use this when the App is opened, until a new Unique ID is generated and accepted.'

[36] See Chris Culnane, Eleanor McMurty, Robert Merkel and Vanessa Teague, 'Tracing the challenges of COVIDSafe', comparing the issuing and cycling of temporary IDs under the COVIDSafe app with Singapore's TraceTogether app https://github.com/vteague/contactTracing
.

compensation for harms.[37] Such remedies must include both injunctive relief and compensation. The avenues through which such remedies should be able to be obtained should include all of the following:

(i) The legislation should provide that any breach of a provision of the COVIDSafe Act is 'an interference with the privacy of an individual' within the meaning of the *Privacy Act 1988*, thus enabling a person to make a complaint to the Privacy Commissioner, and obtain such remedies as that Act provides. Such an approach has previously been taken by the Commonwealth in the data breach notification (DBN) legislation, s.13(4A).[38]

(ii) The ACCC has recommended that individuals should be able to seek the same remedies from a court as are available from the Privacy Commissioner under the Privacy Act. For the same reasons, such an avenue of redress should be available here.

(iii) For enforcement of provisions in some sectors, such as employers in cl. 9(2)(a) and (b), or businesses in cl. 9(2)(c)-(f), more effective and trusted enforcement could be obtained through other legal avenues (eg the Fair Work Act for (a) and (b)). These avenues should be enabled to provide remedies for breach of this law wherever possible, so that complaining to the Privacy Commissioner becomes only the residual option, or where there is some special reason to choose that route.

Dissatisfaction with the Privacy Commissioner being the sole source of remedies for breaches of data privacy rights is common, so there is a need for the COVIDSafe Act to also adopt approaches (ii) or (iii) above to be seen as going beyond the (ineffective) norm in order to encourage public trust.

## Complementary State and Territory legislation

The PIA Recommendation 12 and the Department's response can be read as implying that once a State/Territory contact tracer obtains decrypted data from the NCSDS, the Department of Health is admitting that its 'effective control' is gone, except for any contractual protections it gets the States and Territories each to agree to. The worst case interpretation is that Health is admitting, based on legal advice it has received, that cl. 6(1) cannot be applied against State or Territory officials, leaving the way open to demands by State/Territory officials with demand powers, including Police, anti-corruption bodies, and many more. A less 'worst case' scenario would see Commonwealth powers applying where the data is received from the NSCDS and is still in the hands of State/Territory tracing personnel, but too attenuated where the data goes to parties beyond that immediate receipt.

For reasons such as this, and the problem of deletion discussed earlier, there is a need for legislation complementary to the Commonwealth COVIDSafe legislation to be enacted by each of the States and Territories. In particular, such legislation must enable both offences to be committed by State and Territory officials, and enforcement actions to be taken by individuals under State and Territory laws (including under their privacy legislation).

---

[37] For a view supporting 'statutory compensation', see Law Council of Australia *Principles for the design of a COVID-19 contact tracing app* April 2020, Principle 7.

[38] Privacy Act 1988 (Cth) s. 13(4A*) Notification of eligible data breaches etc.* 'If an entity (within the meaning of Part IIIC) contravenes subsection 26WH(2), 26WK(2), 26WL(3) or 26WR(10), the contravention is taken to be an act that is an interference with the privacy of an individual.' The provisions referred to are those imposing obligations to make an assessment, make a statement to the OAIC, notify and comply with a direction to notify.

### Independent oversight: A COVIDSafe Privacy Advisory Committee

COVIDSafe is a joint scheme authorising and requiring collaborative actions by officials from all Australian jurisdictions. During the pandemic Australia has had a National Cabinet to make political decisions, and an Australian Health Protection Principal Committee (AHPPC) to advise it on medical issues. For there to be public confidence in the operation of COVIDSafe, there needs to be independent oversight of it by a body of equal national credibility.

All Australian jurisdictions except South Australia and Western Australia have privacy commissioners (under various titles). The Law Council of Australia (LCA) has recommended 'independent oversight by Commonwealth, State and Territory Privacy Commissioners, in accordance with the complaints, investigation and enforcement mechanisms under relevant privacy legislation'.[39] This is not a strong enough proposal, because individual Commissioners do not have sufficient weight or credibility, or licence to speak publicly on issues of public importance.

A COVIDSafe Privacy Advisory Committee should be created by the COVIDSafe Act, and should include at least the various Privacy Commissioners, plus persons of similar stature from the other two jurisdictions. Its principal purpose should be to provide a collective voice from privacy authorities, with a statutory obligation to advise the National Cabinet and the public about all issues concerning the operation of COVIDSafe. It should have input into the studies which must be carried out into the effectiveness of the COVIDSafe scheme, and be entitled to interpret and comment on their results. It should have statutory powers to obtain any information it needs to carry out its role, including from its members (for example, arising from complaints in their jurisdictions). In these roles it would be similar to the EU's European Data Protection Board (EDPB) of 27 data protection authorities, which speaks collectively and independently on issues such as COVID19.

## Conclusions

We conclude that the conditions necessary to justify sufficient public trust in government for the Australian public to opt in voluntarily to the installation and use of the COVIDSafe app, and to not opt out, are lacking. Many of the main deficiencies we identify in this article are remediable: five deficiencies in transparency; and nine categories of improvements to the current Determination by the proposed COVIDSafe Act. However, the question of whether an individual Australian would be well advised to install and run the app remains a decision which depends on individual circumstances. We explain these conclusions in the following paragraphs.

### Lack of transparency, and misleading spin, detract from trust

The Australian public does not yet have sufficient reasons to trust that the operation of the COVIDSafe app is a necessary and proportionate response to Australia's current position in relation to the pandemic. For a significant portion of the public, the federal government's track record of serial breaches of public trust in relation to privacy is an obstacle to it obtaining the trust that is needed to ensure sufficient uptake of the app for it to be effective. A new contributor to this lack of trust is government's failures to be transparent in relation to the COVIDSafe app. To reduce this particular trust deficiency, Australian governments need to take the following steps:

1. The federal government should correct the misinformation it has given the public about how the app works, particularly in relation to the extent of data collected.
2. Australian governments should announce details of proposed studies to test whether the COVIDSafe app is in fact achieving its contact tracing goals.

---

[39] LCA *Principles*, principle 7.

3. The advice of health and security officials on which political claims that the COVIDSafe app and its operation is a necessary and proportionate response should be made public.
4. The full source code for the app should be made public, at least a week prior to the COVIDSafe Act being enacted.
5. The federal Privacy Commissioner should be requested by the Parliament to state and justify her opinion of whether the COVIDSafe app and its operation (including proposed legislation) is a necessary and proportionate response to the risks to privacy that it involves, and to make any recommendations they consider necessary. State and Territory privacy Commissioners should be requested by their respective governments to do likewise in relation to the roles of State and Territory officials in its operation, and on the need for complementary State and Territory legislation.

## Legislation needs stronger protections than the Determination provides

Although the Determination under the Biosecurity Act is providing some protections against misuse of the COVIDSafe app for the first month or so of its operation, we have shown in this article that there are many aspects that Parliamentary legislation needs to strengthen or to add. The most important improvements which should be included in the new 'COVIDSafe Act' (an Act amending the Privacy Act 1988), in something like their order of importance, are (as explained more fully in this article):

1. Individuals need to be able to take civil actions to enforce the law, obtaining both injunctions and compensation, and not be forced to rely on prosecutions initiated by government bodies.
2. The prohibitions against any persons coercing the use of COVIDSafe app, good though they are, need to be made even stronger through closing of loopholes. Individual rights of enforcement are crucial.
3. The collection of data by the app should be minimised, in line with the recommendations made in the PIA, recommendation 12. Prohibitions on State and Territory health officials from looking at decrypted data which they have no need to receive in the first place is not good enough protection.
4. Consent to upload data from a phone to the NCSDS must be required from 'the person who normally uses the device', not just from the person who is current in possession or control of it.
5. The conditions for termination of the operation of the app and deletion of all data collected as part of its use are not yet sufficiently precise. Whatever condition for termination is stated, it should have added to it that it 'is to be determined based on advice from the Australian Health Protection Principal Committee', and that such advice is to be made public as soon as it is given. This will provide assurance that the objective advice of health experts, not political advice, should decide when the pandemic has concluded.
6. The definition of 'COVID app data' must be broadened to include decrypted data.
7. There must be new definitions for 'proximity', for the controller of the COVIDSafe app, and for the controller of the 'National COVIDSafe Data Store', all to be defined in ways that cannot be changed without a further Act of Parliament.
8. The COVIDSafe app is a national scheme, and complementary State and Territory laws, with individual rights of enforcement, are needed to avoid problems of any limitations on Commonwealth power. Merely to have some agreement between the Commonwealth and the States, with no individual enforcement, is insufficient.
9. A COVIDSafe Privacy Advisory Committee should be created to exercise independent oversight and advise both the public and the National Cabinet.

## Individual decisions, unique balances of trust

In some respects, we are 'all in this together', but in other respects each person's individual circumstances are unique, due to a combination of factors such as age, underlying conditions, family composition and living arrangements, whether in self-isolation or back at work every day in essential services, and even ownership of the right type of phone. Individuals will also make different assessments of the extent to which their actions may or may not contribute to the public good, not just to their own protection or of those close to them.

It is possible that more transparency may occur, and legislation addressing some or all of the above concerns may be enacted, within a few weeks, but this is not yet certain. Individual circumstances can lead to the need to make decisions, even though all desirable information is not yet available, or may never become available. Some or all of the suggested transparency and privacy protections may be rejected. Privacy protection is significant, but never an absolute value. Decisions are always made in a context, and Australia is dealing with a pandemic that has already taken nearly 100 lives in this country. Decisions about whether to install and run this app remain individual decisions, but are best made after obtaining as much information as can reasonably be obtained and put in the balance.