University of New South Wales Law Research Series

AUSTRALIA'S COVIDSAFE EXPERIMENT, PHASE III: LEGISLATION FOR TRUST IN CONTACT TRACING

GRAHAM GREENLEAF AND KATHARINE KEMP

[2020] *UNSWLRS* 24

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 experiment, Phase III: Legislation for trust in contact tracing

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

Work-in-Progress Draft 15 May 2020 – 22,800 words – Acknowledgments[*]
This draft is based on G. Greenleaf & K. Kemp 'Australia's COVIDSafe Experiment, Phase II: A Draft Law for Surveillance and Trust' (2020) UNSWLRS – on SSRN <https://papers.ssrn.com/abstract_id=3595947>. *That paper was about the exposure draft Bill, not the Act (enacted yesterday) which is the subject of this version. Comments are welcome to* graham@austlii.edu.au *or to* k.kemp@unsw.edu.au .

Contents

[**] Katharine Kemp's research is part of the UNSW Grand Challenge on Trust. UNSW's Grand Challenge on Trust aims to deepen our understanding of trust, of distrust, and their effects on society. By building interdisciplinary networks, and facilitating critical discussions, the Grand Challenge examines the nature of trust deficits, abuses of trust, the consequences of declining or improved trust, and what is necessary to become worthy of trust.

[*] 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, Roger Clarke and Jill Matthews.

1. An experiment in surveillance and trust, Phase III

A week after the Australian governments released a coronavirus contact tracing app for public download, marketed as 'COVIDSafe', the federal government released an exposure draft[1] of the Privacy Amendment (Public Health Contact Information) Bill 2020 (Cth) ('the COVIDSafe Bill') on 4 April 2020. The federal Parliament was to re-commence on 12 May, so interested parties had only a week to comment on the draft Bill before Parliamentary debate commenced. In addition, a Senate Select Committee is already taking evidence concerning the app, with submissions due by 23 May, and the Parliamentary Joint Committee on Human Rights will consider the human rights implications of the legislation.

The app was released by the federal government for public download on 26 April 2020, together with a non-disallowable[2] emergency Determination under the *Biosecurity Act 2015* (Cth) (with Explanatory Statement)[3] to govern its operation, a Privacy Impact Assessment (PIA) by a law firm (Maddocks),[4] with the Health Department's response to that PIA,[5] and (not least) the app itself, its privacy policy,[6] and FAQs concerning its operation.[7] We have previously analysed Phase I of the development of this surveillance system, and criticised many deficiencies in the Determination,[8] and Phase II, where the draft Bill to replace the Determination was published, but many deficiencies remain.[9] All other documents (PIA, Departmental response, FAQs and app Privacy Policy) retain their relevance.

This article concerns the Bill (with amendments to the exposure draft Bill) introduced into Parliament on 12 May,[10] and passed on 14 May. The Explanatory Memorandum[11] to the Bill includes significant explanations of some clauses. Now that the Bill has been enacted, the purpose of this article is to provide a reasonably comprehensive explanation of the provisions of the *COVIDSafe Act* and important aspects of their Australian context. Significant deficiencies in both

---

[1] Exposure draft Privacy Amendment (Public Health Contact Information) Bill 2020 <https://www.ag.gov.au/RightsAndProtections/Privacy/Pages/COVIDSafelegislation.aspx>

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

[3] *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>

[4] Maddocks, *Privacy Impact Assessment (PIA) Report*, 24 April 2020 (hereinafter 'Maddocks PIA') <https://www.health.gov.au/resources/publications/covidsafe-application-privacy-impact-assessment>

[5] Department of Health *The COVIDSafe Application – Privacy Impact Assessment – Agency Response*, undated (before 26 April 2020) (hereinafter 'Health PIA Response') <https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-application-privacy-impact-assessment-agency-response.pdf>

[6] COVIDSafe Application (the app) and Privacy Policy < https://www.health.gov.au/using-our-websites/privacy/privacy-policy-for-covidsafe-app#what-personal-information-will-be-collected-and-why-is-it-being-collected>

[7] COVIDSafe FAQs < https://www.health.gov.au/resources/publications/covidsafe-app-faqs>

[8] G. Greenleaf and K. Kemp 'Australia's 'COVIDSafe App': An experiment in surveillance, trust and law', 1 May 2020, Work-in-Progress draft at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589317>.
The Determination will be repealed once the Act receives the Royal Assent.

[9] G. Greenleaf & K. Kemp 'Australia's COVIDSafe Experiment, Phase II: A Draft Law for Surveillance and Trust' (2020) UNSWLRS <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3595947>.

[10] Privacy Amendment (Public Health Contact Information) Bill 2020 <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6556>

[11] Explanatory Memorandum, Privacy Amendment (Public Health Contact Information) Bill 2020 (Cth) <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6556>

the extent of transparency around the introduction of the COVIDSafe app, and the privacy-protective provisions of the Act, are identified and improvements suggested. These extensive suggestions are made because debate over the app and the Act is not over, and opportunities to obtain improvements may arise, particularly through the operation of the two Parliamentary committees examining Australia's COVID-19 response, and the human rights implications of the Act.

1.1. Trust: A two-way street

All phases of this development are intended to be a package which will create sufficient public confidence to result in downloads of the app by a sufficient percentage of the Australian population,[12] for it to have a significant effect on the effectiveness of tracing of persons infected with the COVID-19 virus. The Australian Communications Consumer Action Network (ACCAN) has pointed out that rural Australians and 'some of Australia's most vulnerable communities' will not be able to use the app effectively, due to '[l]ack of individual ownership of mobile phones, sharing of mobile devices and lack of internet and mobile coverage'.[13]

The government claims that over 5.6 million people[14] have downloaded the app within the first 20 days, which is about 25% of the estimated phone-owning population in Australia,[15] perhaps 20% of the whole population.. The number of people who have installed it and put it in use will be lower than this. The government has not made any fixed claim as to how many people it estimates will need to use the app before it is effective, although it initially suggested 40%.[16] There does not seem to be useful scientific evidence on this question, which underlines that what Australia is doing is an experiment.

This Act is in an unusual situation, because the test of success is not whether the government can simply get away with whatever law pushes through Parliament, and then implement it. It also has to convince the public to continue to 'vote with their phones' that they trust what the government is doing. In this sense, the government is trusting the public to install and use an app, in sufficient numbers to make it effective, and to keep it installed. However, for the public to act in this 'trusting' manner, a sufficient portion of the public must believe that the government is being open with them as to how the app actually works, and that the privacy protections it is providing in legislation can be relied upon. It is a situation where mutual trust is necessary for success.

The launch of the app has created some new difficulties for the government in obtaining the public confidence that it needs: insufficient transparency; misleading initial statements by the government about the operation of the app; and flaws in the regulations (originally in the Determination, many continuing in the Act). These problems may be remediable. This article analyses the steps that Australian governments need to take if public trust is to be justified.

1.2. Surveillance: How the app will work (in brief)

At the time of the Bill's introduction into Parliament (12 May), the app was not yet fully functional even though it had been available for download for over two weeks. In that time, it is understood

---

[12] Although only owners of phones can download the app, the whole population is susceptible to coronavirus.

[13] See Letter from ACCAN and other NGOs to the Hon Greg Hunt MP, Minister for Health (11 May 2020) 2.

[14] As at 14 May 2020, according to ABC News online < https://www.abc.net.au/news/2020-05-13/coronavirus-tracing-app-covidsafe-now-fully-functional/12244616>

[15] 2019 estimates vary from 18.6 million (Roy Morgan) to 20 million (Statista), from a population of 25.5 million.

[16] See, eg, Prime Minister of Australia, 'Interview with Gareth Parker, 6PR' (Transcript, 15 April 2020) <https://www.pm.gov.au/media/interview-gareth-parker-6pr>

that devices of registered COVIDSafe users recorded information about devices of other COVIDSafe users within which they come into contact. This information could be uploaded to the National COVIDSafe Data Store (NCSDS) and decrypted in this period, but the data was only able to be downloaded by state and territory health officials on 13 May. The Deputy Chief Medical Officer indicated on 13 May that the Commonwealth had now reached the necessary agreements with the states and territories (these have not been published at the time of writing) and COVIDSafe was 'fully functional', but that he was not aware of any case where COVIDSafe data had been used for contact tracing at that point.[17]

A brief and simplified summary of how the app works follows, but much more detail is throughout the paper, and particularly in Part 5. Details of its operation are set out in the Maddocks PIA, the app's Privacy Policy, the FAQs to the app,[18] but only in passing in the Bill's Explanatory Memorandum. It is based to some extent on Singapore's TraceTogether app.

When a person chooses to download the COVIDSafe app, they become a 'COVIDSafe user' and their 'registration details' (name or pseudonym, phone number, age range and postcode) are recorded on the National COVIDSafe Data Store (NCSDS), operated for the federal Health Department. Upon registration, the NCSDS sends the user an encrypted ID, and sends a new temporary encrypted ID to the user every two hours (the transmission of this new ID will only succeed if the app is in operation on the user's device).

The app records 'contact events' when two 'communication devices' (usually mobile phones) running the app come within Bluetooth contact range of each other. All contacts between two phones running the app within Bluetooth signal range (which is variable, depending on numerous factors, but may be 10 metres or more), even for a brief period, are recorded (an encrypted 'digital handshake', or 'contact event'). The encrypted ID of the other app, and the signal strength, are recorded as part of the 'contact event', as are the time and duration of contact. The duration can be determined because digital handshakes are recorded every minute. Location at time of contact is not recorded (GPS technology is not used). Claims that the proximity required for recording of contacts is '1.5 metres for 15 minutes' are misleading.[19] Each contact event is stored on the mobile device for 21 days, then deleted.

Only when the user of one of the mobile devices running the app is tested positive for coronavirus are they requested by State/Territory contact tracing personnel to allow the set of contact events recorded on their device to be uploaded to the NCSDS. If they agree they are given a PIN to enable this.

The NCSDS then allows the appropriate State or Territory contact tracing personnel ('contact tracers') to access contact event data that has been uploaded to the NCSDS by the user tested as positive and decrypted at the NCSDS, as well as the telephone numbers of the other users whose IDs match the IDs found in the contact even list that has been uploaded. They can then start the process of contact tracing.

---

[17] Georgia Hitch, 'Coronavirus tracing app COVIDSafe now fully functional, Deputy Chief Medical Officer confirms' (ABC online, 13 May 2020) <https://www.abc.net.au/news/2020-05-13/coronavirus-tracing-app-covidsafe-now-fully-functional/12244616>

[18] 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')

[19] See, eg, 'Transcript, Sunrise interview with Natalie Barr'(Australian Government, Services Australia website, 17 April 2020) <https://minister.servicesaustralia.gov.au/transcripts/2020-04-17-sunrise-interview-natalie-barr>

However, according to the Department of Health, contact tracers are only allowed to access the details of those contact events which come within a defined proximity (probably based on recorded signal strength and duration of contacts). The defined proximity (popularly believed to be '1.5 metres for 15 minutes'), and how it is enforced, has not been made public. This sub-set of contact events can be called 'proximity events'.

This app therefore has elements which are decentralised (contact event data is held on individual mobile phones for 21 days until deleted) and others which are centralised (some contact event data may be uploaded to the NCSDS in the event of a positive diagnosis, and the distinction is made there between contact event and proximity event data). Some other models are more decentralised (for example, the Google-Apple proposed model),[20] 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 registration and decryption at the central server, and particularly given the uploading of all contact events.

1.3. The Australian political context: No fundamental privacy rights

The introduction of a contact tracing app against COVID-19 is different in Australia than in many other countries, because Australia is unusual in having no fundamental privacy rights. As a result, the introduction of a government-run surveillance system enabled by legislation cannot be challenged in Australian courts, or international courts, in any significant way.[21] The Australian Constitution does not include any protections of privacy (or most other human rights), nor does Australia have significant treaty obligations, or even common law protections through tort or equity that are significant. Protections of privacy in Australia are essentially creatures of statute, particularly the *Privacy Act 1988* (Cth) (*Privacy Act*), and various state and territory Acts. The courts have been largely irrelevant to the development of privacy protections in Australia since such developments commenced around 1970, with party politics usually being determinate.[22]

This is unusual compared with the large number of countries, including those in the EU, that have constitutional rights of privacy which must be complied with if contact tracing systems are introduced, or that are parties to international agreements protecting privacy, such as the *European Convention on Human Rights*, Article 8. In many cases, these constitutional or treaty provisions will result in legal requirements that such systems be 'necessary and proportionate' measures to deal with an emergency such as pandemic, and challenges before local or international courts are possible. But that is not so in Australia.

1.4. Benchmarking COVIDSafe: Australia's initial success against COVID-19

Any assessment of the effectiveness of the COVIDSafe app must start with the fact that Australia has been relatively successful in suppressing the COVID-19 pandemic, prior to any use of a contact tracing app. As at 9 May 2020, before the COVIDSafe app was able to be used, Australia's fatality rate was four persons per million of population, fourth lowest of countries where reliable figures are

---

[20] Fred Sainz, 'Apple and Google partner on COVID-19 contact tracing technology' (Apple website, 10 April 2020) <https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>

[21] It is possible for proceedings to be commenced against Australia before the UN Human Rights Committee because of Australia's ratification of the First Optional Protocol to the *International Covenant on Civil and Political Rights*. See Part 2.2 below concerning Statements of Compatibility with Human Rights under the *Human Rights (Parliamentary Scrutiny) Act 2011*.

[22] Greenleaf, G. 'Privacy in Australia' in Rule J and Greenleaf G (Eds) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, 2008. <https://ssrn.com/abstract=3072270>.

available.[23] The numbers of new reported infections per day are also very low, with zero cases reported in almost all Australian states and territories on 11 May, the exception being one cluster of cases in Victoria. These rates go slightly up and down each day, but Australia is, at this stage, one of the few countries where the 'first wave' of infections is close to being eliminated. Of course, this relative success might not be maintained, and it is entirely possible that there will be a higher rate of infections in subsequent waves, as aspects of economic and social life are re-opened, and as winter provides a more conducive environment for the virus.

Nevertheless, the near-elimination of new infections before the app came into use must not be disregarded, and it does set a very high initial benchmark against which the effectiveness (or lack of effectiveness) of the app must be measured, even though it is a benchmark which may change over time. As discussed in Parts 2.1 and 2.2 following, we do not yet have any official statements of how Australian health officials (and politicians) propose to measure the effectiveness of the app, even though the *COVIDSafe Act* requires this in order to determine when use of this tracing system should cease. As we will see, although there is no legal requirement in Australia that a measure that interferes with privacy through surveillance, such as the COVIDSafe system, must be 'necessary and proportionate', such a standard has been adopted by the government in its Statement of Compatibility with Human Rights which accompanied the COVIDSafe Bill.

1.5. Australia's experiment: Voluntary adoption

There are no clearly successful examples of similar contact tracing apps implemented in any country as yet. Singapore's TraceTogether app, five weeks after release, was 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.

Putting questions about the potential inaccuracy of contact tracing apps to one side for the moment,[24] 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.

The Australian government claims that, in the 10 days since its release, 5.1 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,[25] so the current download figure represents around 25% of the potential uptake. Public trust must become more widespread, before success in uptake is likely to follow.

---

[23] Australia is behind Taiwan (0.3), Hong Kong (0.5), Singapore (3), and equal with New Zealand (4). Compare Canada (117), US (232), Sweden (301), France (398), Britain (451) and Italy (495), and the magnitude of Australia's success (to date) is apparent. Source: Peter Hartcher 'Credit to Hunt, a quiet achiever' *Sydney Morning Herald*, May 9-10, 2020, p30.

[24] 'Don't rely on contact-tracing apps' (The Economist online, 16 May 2020) <https://www.economist.com/leaders/2020/05/16/dont-rely-on-contact-tracing-apps> , referring to both false positives and false negatives produced by Bluetooth contact tracing apps.

[25] 2019 estimates vary from 18.6 million (Roy Morgan) to 20 million (Statista).

2. Transparency? Not yet, perhaps never

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 and continue using the app. As yet, the government has fallen short on four fronts.

2.1. Independent measures of success of the COVIDSafe app

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 COVID-19, 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 not have been identified at all as part of contact tracing, or it may have taken longer to identify them, increasing the risk that they would have infected other people in the interim.

The extent to which the COVIDSafe system is effective in delivering these results, and assessment of whether the allocation of resources to operate this system is a better use of public funds than (say) more extensive infection testing and/or antibody testing, are matters for scientific assessment and report to governments and the public. Concerns have already been raised that contact tracing apps may hinder containment efforts by producing false positives and false negatives about which individuals have been at risk of infection.[26] This is complex and imprecise research, and the answers concerning relative effectiveness will no doubt change over time. Such assessments are also essential for the decisions that must be made under s. 94Y to determine the end of the COVIDSafe data period, particularly under s. 94Y(1)(b). These determinations may be very contentious politically, and need to be credible, independent, and free from political considerations.

In Australia, public confidence in how governments have dealt with the pandemic has been increased by our receiving daily information on infection and death rates, and on the causes of transmission and fatalities, from health authorities and Chief Medical Officers (CMOs). The public has regarded this information as being credible and independent (with few exceptions – one now before an independent inquiry). The uptake of the COVIDSafe app has without doubt benefited from this unusual degree of public confidence in government.

However, Australian governments have not published details of any proposed studies to test whether the COVIDSafe system is in fact achieving its objectives, or to guarantee that such reports will be objective and credible. In our view, they must do so if the scientific credibility of the reasons for introducing the app in the first place is to be maintained. Such studies must be done and publicised not only by CMOs, but also by independent scientific experts, because CMOs have been among the most ardent promoters of the public downloading the app. They therefore have a vested interest in its success – colloquially, they 'have skin in the game'.

The Act does not provide any guarantees of independent scientific advice on whether the app is continuing to be of practical benefit or should be terminated in favour of more effective pandemic-fighting measures. The Act should provide that independent academic experts will be provided with access to such information as is necessary for them to make periodic assessments of the extent to which the COVIDSafe system is achieving its objectives, and to make such assessments public. Commonwealth, State and Territory officials should be required to provide this information. The first such assessment should be made not later than three months after the app was launched (ie by 1 August 2020), and at least quarterly after that. This process could be considered analogous to

[26] See 'Don't rely on contact-tracing apps' (The Economist online, 16 May 2020) <https://www.economist.com/leaders/2020/05/16/dont-rely-on-contact-tracing-apps>.

Privacy Impact Assessments. Oversight of this assessment process should be by the various Australian Privacy Commissioners, acting collectively (see part 10.5). One function of such assessments will be to state accurately how the COVIDSafe system works, which may be different from inaccurate or over-simplified political statements (see parts 5.3 and 5.4).

Ministerial reports on 'operation and effectiveness'

The Act contains a new provision (s. 94ZA) requiring the Health Minister to produce a report to Parliament 'on the operation and effectiveness of' the COVIDSafe app and the NCSDS, after Part VIIIA has been in operation for six months, and six-monthly thereafter so long as the app remains in operation, or within three months of the Minister making a determination under section 94Y(1) (to end the 'COVIDSafe data period: see part 9.4).

The EM does not suggest how 'effectiveness' is to be assessed. It confirms that the reports cannot contain any COVID app data, as they are not an additional permitted use, but could (only) include the de-identified data on total registrations allowed by s. 94D(5)(d) ([160]-[163]).

In our view, an assessment of 'effectiveness' must take into account whether the continuing operation of the app, and the benefits to contact tracing obtained from it, continue to meet the criteria that the limitations on privacy that it imposes continue to be 'reasonable, necessary and proportionate'.[27]

These periodic reports by a Minister, while possibly valuable, are not even required to be based on the advice of the Chief Medical Officer. They do not satisfy any of the requirements of independent advice for which we argue, and the have no defined criteria for assessing 'effectiveness'.

2.2. Justifications for COVIDSafe not disclosed

For the Health Minister to make the Determination, under s. 477 *Biosecurity Act 2015,* on which the app's operation initially depended, it was necessary for the Minister to 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 stated that 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.

Even though the Determination is now superseded by the Act and will be repealed, the three advices on which it was based should still be made public, because this app should not have been 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 is likely to be more effective than the same resources used to increase testing and (human) tracing.

The legitimacy of the operation of the app will now depend upon the Act, not the Determination. Parliament is not bound by requirements equivalent to s. 477 before enacting legislation, other than the requirement of a Statement of Compatibility with Human Rights in the Explanatory Memorandum to the Bill,[28] which will be considered by the Parliamentary Joint Committee on

---

[27] See EM [24] and preceding paragraphs.

[28] The Statement is required by the *Human Rights (Parliamentary Scrutiny) Act 2011.*

Human Rights. This Statement considers the compatibility of the Bill with human rights and freedoms recognised or declared in specified international instruments.[29] The Statement considers international instruments concerning the right to health, concluding that the purpose of COVIDSafe, 'to assist relevant State and Territory health authorities with contact tracing', which is 'critical to containing the spread of COVID19' (at [6]). It says it will 'facilitate efficient and accurate contact tracing' (at [7]), with consequent health benefits. The Statement then considers the protection against arbitrary or unlawful interference with privacy provided by the International Covenant on Civil and Political Rights (ICCPR), Article 17. As the Statement notes (at [10]-[11]), the right to privacy under Article 17 'can be limited to achieve a legitimate objective where the limitations are lawful and not arbitrary'. 'Not arbitrary' is interpreted by the UN Human Rights Committee to require 'reasonableness', meaning that 'any limitation must be proportionate and necessary in the circumstances'.

The Statement argues that the Bill meets these requirements by enumerating the ways in which the app collects and uses data in a non-invasive way 'in order to achieve the legitimate aims and objectives of contact tracing', including the 'consent based model' in which the app 'is completely voluntary to download and use' and 'choice as to whether to upload close contact data' (at [13]-[15]). The Statement's conclusion is that the Bill 'is compatible with human rights because it promotes the rights to health and privacy, and to the extent that it may limit those rights, those limitations are reasonable, necessary and proportionate'.

The 'limitations' on the right of privacy which the Act creates are those constituted by the whole COVIDSafe system, a system of surveillance which did not exist before the Act and its predecessor Determination. The Act establishes a system of governance over the COVIDSafe system, including determining what can and cannot be done with the data resulting from it. It is this system which must be assessed in determining whether it is a 'reasonable, necessary and proportionate' means to achieve the legitimate goal of 'facilitat[ing] efficient and accurate contact tracing.'

The problem that remains with this legal justification for the COVIDSafe system (as governed by the Act) is that the Statement does not include any evidence, including expert opinion, that the system will be effective in improving contact tracing, to an extent that makes it 'necessary and proportionate'.

2.3. The semi-secret source

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' – would be made available in the weeks following its release. On 18 April 2020, Minister Stuart Robert said 'The source code will be made public.'[30] In the Privacy Impact Assessment, Maddocks recommended public release of the source code for the app,[31] 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

[29] As listed in s. 3, *Human Rights (Parliamentary Scrutiny) Act 2011*

[30] 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>

[31] Maddocks PIA Report, Recommendation 1.

on the same basis as countries such as Singapore, we will be releasing the source code so as there's full assessment …'[32]

At the very least, the source code should have been made available a week before the Bill went to Parliament, to allow independent (if rushed) assessment of this key part of the COVIDSafe technical infrastructure. In the event, the government release some of the relevant source code less than four days before the Bill was introduced in federal parliament.

On 8 May 2020, the Digital Transformation Agency released the source code for the COVIDSafe app (only),[33] providing it via the GitHub repository.[34] The DTA said, 'We are releasing the app code, but to ensure the privacy of individuals and integrity of the overall system, the code that relates to the COVIDSafe National Information Storage System will not be released.' The app code for both the iOS and Android versions is provided, but not (as stated above) the server code operating in relation to the NCSDS. The conditions of provision of the source code purport to include a condition that 'I am responsible for any costs of third party claims associated with my access to the App Code, and must pay those claims on request.' Whether or not this vague impost is enforceable, its effect may be to deter valuable inspections of the source code which could otherwise have revealed bugs.

Many computing experts consider that this does not constitute making public the source code for COVIDSafe, because the server code controls such things as the decryption of data uploaded to the NCSDS, which is where major security and privacy issues arise.[35] It is well-known that only part of the source code has been released, so the release of the app source code alone is unlikely to have resulted in a net increase in community trust in COVIDSafe.

Developers have also raised technical issues with the COVIDSafe app, including claims that it exposes users to risks that third parties will use the app to track their movements through signals containing a user's temporary identifier.[36] The government should respond to developers' proposals on how to fix these and other flaws.[37]

2.4. Privacy impact assessments and absences

The Maddocks' PIA report says the authors are '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'[38]), 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

---

[32] 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)

[33] 'DTA publicly releases COVIDSafe application source code' 8 May 2020 <https://www.dta.gov.au/news/dta-publicly-releases-covidsafe-application-source-code>.

[34] Terms and Conditions for access to COVIDSafe App Code <https://covidsafe.gov.au/app-code-terms-and-conditions.html>

[35] See Stilgherrian, 'Australia's wobbly start to COVIDSafe app' (ZDNet online, 11 May 2020) <https://www.zdnet.com/article/australias-wobbly-start-to-covidsafe-app-transparency/?&web_view=true>

[36] See Bernard Keane, 'Un-appy, Scott: flaws and inconsistencies start to mount for troubled surveillance app' (Crikey online, 7 May 2020) < https://www.crikey.com.au/2020/05/07/flaws-inconsistencies-covidsafe/>

[37] See Jim Mussared, 'Privacy issues discovered in the BLE implementation of the COVIDSafe Android app' (updated 5 May 2020) <https://docs.google.com/document/d/1u5a5ersKBH6eG362atALrzuXo3zuZ70qrGomWVEC27U/preview>

[38] Maddocks PIA, p 4, para 3.2.

proposed operation) has been developed, by the various federal, State and Territory agencies involved, to achieve compliance with the *Privacy Act*, and particularly the Australian Privacy Principles (APPs).[39] 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).[40]

There is no mention in the Determination's 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 2015*, 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 three sources of advice mentioned in that Statement 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.[41] The Commissioner 'said that important safeguards have been put in place', that she regarded it as 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' (see part 10 of this article), 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.

In our opinion, the federal Privacy Commissioner should have been requested by the Parliament to state and justify her opinion of whether the COVIDSafe app and its operation (including the proposed legislation) was a necessary and proportionate response to the risks to privacy that it involves, and to make any recommendations she considered necessary. State and Territory privacy commissioners should be requested by their respective governments (and by the Commonwealth Parliament) to do likewise in relation to the roles of State and Territory officials in its operation, and on the need for any complementary State and Territory legislation.

2.5. Official misinformation needs correction

Transparency requires correction of misinformation, at least that provided by government officials and agencies, particularly when they are aimed at promoting installation and use of the app. This will pay dividends in long-term public trust, just as misleading statements and broken promises about RoboDebt, MyHealthRecord etc have reduced the credibility of the federal government, particularly in situations where health and technology intersect. There has been an abundance of official misinformation about this app, aided by the non-disclosure of the source code. Examples are given in parts 1.2 and 5.4.

---

[39] Maddocks PIA, p 4, para 2.5.

[40] 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/>

[41] 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/>

2.6. Commonwealth agreements with States and Territories should be disclosed

The last missing piece in the jigsaw that makes up the COVIDSafe system is the set of agreements between the Commonwealth and each State and Territory, agreements apparently only completed on 13 May and not yet disclosed (see Part 1.2). These agreements are likely to be a critical part of the system, because they are expected to define how contact tracers can use the COVID app data they receive from the NCSDS, potentially also explaining how the complete 'digital handshake' data from contact events will be filtered before provision to contact tracers so that it only includes events within the proximity determined to be suitable for contact tracing (whether '1.5 metres and 15 minutes' or otherwise). See Part 5 for a full discussion.

We recommend that the Agreements between the Commonwealth and States/Territories should be made public because they include essential information on the extent of use of surveillance data collected by the COVIDSafe app .

2.7. What can now be done to restore transparency and increase trust?

We have recommended six steps to restore some transparency, albeit belatedly, to the process of ensuring that the introduction of the COVIDSafe system is necessary, proportionate, and effective:

(i) The Act should require, and guarantee, periodic independent scientific assessments, of the extent to which the COVIDSafe system is achieving its purposes, and their being made public.

(ii) The three advices on which the Minister relied to make the Determination should be released because they are the basis on which the release of the COVIDSafe system was justified.

(iii) The source code for the NCSDS should be released, unless the government can provide a convincing explanation as to why this could not be released (rather than a shorthand reference to 'security').

(iv) The federal Privacy Commissioner should be requested by the Parliament to state and justify her opinions on the privacy implications (at large) of the COVIDSafe system. The opinions of State and Territory Commissioners should also be obtained.

(v) Government agencies and Ministers should adopt a policy of telling the truth about how the app works, as well as whether and how technical flaws are being addressed, even if this cannot be reduced to simple and comforting sound-bites, because this will pay dividends in long-term public trust.

(vi) The Agreements between the Commonwealth and States/Territories should be made public because they include essential information on the extent of use of surveillance data collected by the COVIDSafe app.

3. Part VIIIA, *Privacy Act 1988: Regulating the COVIDSafe system*

3.1. Real legislation, replacing a non-disallowable instrument

The Determination made by the Minister for Health under s. 477 was a non-disallowable instrument, and one that could be modified or repealed and replaced by the Minister at any time. It was better than no law at all, but only on the assumption that it would very rapidly be replaced by legislation which cannot be overridden by Ministerial fiat. A step such as a contact tracing app which could pose extreme risks to many civil liberties including privacy, 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.

The Determination has now been replaced by legislation, and some improvements to privacy protections in the Determination and the Bill have been made in the process. The same criticisms of government failure to allow legislation to be debated and passed before the app was released can be levelled at this Act as are discussed above in relation to the Determination, and the same 'emergency' justifications would be put forward. The situation with which we must now deal is that over 5.6 million Australians are reported to have downloaded the app in a little over two weeks,[42] so a practical approach is to attempt to make the protections of privacy it provides as strong as is justifiable.

This article is written in the spirit of making proposals to strengthen those protections, which involves recognising valuable protections already provided, and identifying those points at which the Act is inadequate to provide such protections.

It is worth recognising at the outset that the Act has one of the most important positive starting points: use of the app (and inclusion in the NCSDS system) is voluntary, not compulsory. This is seen in at least five aspects of the Act: (i) downloading the app is voluntary (including uploading 'registration data' to the NCSDS); (ii) the device must be turned on to run the app, that is not automatic; (iii) if a person has tested positive for coronavirus, they must consent to have the COVID app data on their phone uploaded to the NCSDS, so that tracing can occur; (iv) users can delete the app from their device (and opt-out from continuing data collection); and (v) users can opt out from their registration data continuing to be held on the NCSDS.

Set against this, many view COVIDSafe as a system which is more at the centralised end of design of tracing apps, as opposed to a fully decentralised system.[43] That does pose additional privacy dangers, but for now,[44] Australia has already crossed that bridge, for better or worse.

3.2. COVIDSafe: An information system, not just an app

It is important to appreciate that what is being regulated here is an information system, which we can call for convenience the 'COVIDSafe system'. It comprises at least the following components: the COVIDSafe app; the devices on which it can be downloaded and run; the registration process;

---

[42] It is not clear whether these figures are accurate, as their only source seems to be statements by federal government officers and Ministers. For example, do they include those who have downloaded the app, but have not set it to run, or those who have downloaded but deleted it? See Georgia Hitch, 'Coronavirus tracing app COVIDSafe now fully functional, Deputy Chief Medical Officer confirms' (ABC online, 14 May 2020) < https://www.abc.net.au/news/2020-05-13/coronavirus-tracing-app-covidsafe-now-fully-functional/12244616> , quoting the Deputy Chief Medical Officer's statement that '5.6 million Australians' had downloaded the COVIDSafe app.

[43] See David Crowe, 'Privacy advocates raise new concerns with COVIDSafe app' (The Sydney Morning Herald online, 11 May 2020) <https://www.smh.com.au/politics/federal/privacy-advocates-raise-new-concerns-with-covidsafe-app-20200511-p54rwb.html>; Gary Parkinson, 'Why COVID-19 contact tracing apps are causing deep division in Europe' (CGTN online, 7 May 2020) <https://newseu.cgtn.com/news/2020-05-07/Why-COVID-19-contract-tracing-apps-are-causing-deep-division-in-Europe-Qhq5NSZgTm/index.html>

[44] Some continue to argue for a decentralised system, such as the collaboration between Google and Apple, for Australia: see Priya Dev, 'COVID tracing app needs a makeover, not new laws to keep privacy safe' (The Sydney Morning Herald online, 13 May 2020) <https://www.smh.com.au/national/covid-tracing-app-needs-a-makeover-not-new-laws-to-keep-privacy-safe-20200509-p54rfe.html>. See further Sam Langford, 'Questions remain about the effectiveness of Australia's COVIDSafe contact tracing app' (SBS The Feed online, 9 May 2020) <https://www.sbs.com.au/news/the-feed/questions-remain-about-the-effectiveness-of-australia-s-covidsafe-contact-tracing-app>, reporting that the Head of the DTA had stated that 'that Australia will be "one of the first adopters" of new contact-tracing technology set to be released by Apple and Google'.

the NCSDS; users and former users of the app; COVID app data; other personal data collected; the data store administrator; contact tracers; state or territory health authorities; the federal health department; the Commonwealth Chief Medical Officer; state or territory privacy authorities; and the federal Privacy Commissioner. Information system experts would add to this list.

Earlier proposals for collecting personal data on Australians were similarly part of a system. The Australia Card was not just a card, nor was the Access Card. They were simply the most visible component of proposed complex information systems, as the COVIDSafe app is here. Both proposed regimes failed primarily because of other features of their information systems.

In this case it is necessary to keep the whole 'COVIDSafe system' in view as the object of regulation, and to be acutely aware of the possibility of some aspects of the system not being included in the regulatory footprint although they should be.

3.3. Objects of the legislation

The object of the new Part VIIIA of the *Privacy Act* is (s. 94B) as follows

> The object of this Part is to assist in preventing and controlling the entry, emergence, establishment or spread of the coronavirus known as COVID-19 into Australia or any part of Australia by providing stronger privacy protections for COVID app data and COVIDSafe users in order to:
>
> (a) encourage public acceptance and uptake of COVIDSafe; and
>
> (b) enable faster and more effective contact tracing.

Its object is therefore 'to assist in preventing …' 'by providing stronger privacy protections for …' data and users 'in order to' achieve ultimate goals (a) and (b). The enunciation of these objectives is a significant step in defining the constraints that should be imposed on the scope of data collected, the purposes for which it may be used, and the period for which it should be retained (discussed below).

4. Scope of Part VIIIA

4.1. Constitutional basis for extension to State and Territory health authorities

The Commonwealth is making a concerted effort to extend Commonwealth jurisdiction over State and Territory health authorities,[45] and thus over the staff of those authorities who will carry out contact tracing. The Act asserts that the Commonwealth *Privacy Act* applies to those authorities, 'as if the authority were an organisation', but only to the extent that they deal with, or their activities are related to, COVID app data (s. 94X). This will mean that not only the provisions of Part VIIIA will apply to these health authorities, but also other *Privacy Act* provisions, including the Australian Privacy Principles (APPs). This is an instance of the importance of this law regulating the 'COVIDSafe system' systematically.

Any limitations in the definition of 'COVID app data' will therefore limit this extension of jurisdiction. As explained in the following sub-part, this definition does include decrypted, derived and transformed data, by virtue of clarification in the EM. However, it does not include information obtained by state and territory contact tracers which was received from a source other than the NCSDS.

---

[45] '*State or Territory health authority* means the State or Territory authority responsible for the administration of health services in a State or Territory.' (s. 6(1))

The basis for the assertion of Commonwealth jurisdiction in s. 94X is indicated by the provision that Part VIIIA relies, not only on the heads of power on which the *Privacy Act* normally relies (s. 12), but also on the quarantine power, the 'legislative powers with respect to matters that are peculiarly adapted to the government of a nation and cannot otherwise be carried out for the benefit of the nation', the matters incidental powers (s. 94C).

4.2. Categories of data: 'COVID app data', 'registration data'

'COVID app data': Encrypted and decrypted logs

'COVID app data' is defined, in part, as data relating to a person that 'has been collected or generated … through the operation of COVIDSafe' and 'is stored, or has been stored … on a communication device' (s. 94D(5)). It is unclear merely from its wording whether this definition captures data at the heart of the COVIDSafe scheme, namely the decrypted contact logs of COVIDSafe users held 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.[46] This uncertainty is now sufficiently resolved by the statement in the Explanatory Memorandum that the use of 'collected' and 'generated' is 'to ensure that data that is calculated or otherwise derived from within the COVIDSafe app on a communication device is also caught within the definition' [56].

The EM states further at [57]:

> 'Data falls within the definition of COVID app data both when it is held on a user's communication device (in the case of data other than registration data), and after that data is uploaded to the National COVIDSafe Data Store. Additionally, the process of encrypting or decrypting COVID app data at any point through the normal operation and administration of COVIDSafe or the National COVIDSafe Data Store (as permitted under subsection 94(2)) is not intended to be material when considering whether data is COVID app data.'

The definition also expressly includes data collected, generated or stored in the weeks before Part VIIIA was enacted.

'COVID app data': 'Registration data'

It is now clear that 'registration data' comes within this definition of 'COVID app data'. A person's 'registration data' is defined as 'information about the person that was uploaded from a communication device when the person was registered through COVIDSafe' (s. 6(1) definition).

The definition of 'COVID app data' now expressly states that it includes 'registration data' (s. 94D(5)(b)(i)).[47] Registration data therefore obtains the full protections provided by Part VIIIA, and not only protection as 'personal information' under the *Privacy Act* (discussed in the following part).

Not 'COVID app data': Other data used for contact tracing

However, 'COVID app data' does not include 'information obtained from a source other than directly from' the NCSDS, used for contact tracing by state or territory health authorities (s. 94D(5)(c)). As the EM puts it, when these authorities collect tracing data, 'even where that contact tracing was facilitated by COVID app data, the information subsequently collected is not COVID app data' [59]. This will be so, even when it duplicates COVID app data, such as when a

---

[46] In our 'Phase II' article we therefore recommended that 'The definition should be amended to expressly include data decrypted, transformed or derived from the data originally collected or generated through the operation of the app, including data transformed or derived by state or territory health authorities.'

[47] This clarification was not in the exposure draft Bill. Our 'Phase II' article recommended such a change.

name or phone number originally obtained from registration data is verified through tracing. The consequences of this are explained in the next part.

There are therefore two types of data used by state and territory health authorities for contact tracing: (i) 'NCSDS-derived data' (including registration information); and (ii) 'other tracing data'. Type (i) is 'COVID app data', irrespective of who holds it, but type (ii) is not.

'Personal information' and COVID app data

The Act clarifies that COVID app data 'relating to' an individual is taken to be 'personal information' about the individual for the purposes of the federal *Privacy Act* (cl. 94Q). Accordingly, the obligations imposed by the APPs apply in respect of COVID app data to the extent that they are not inconsistent with the provisions of the Act. The use of the words 'relating to' rather than 'about' in section 94Q suggest that even metadata collected or generated by the operation of the app, and stored on the mobile device, will be treated as 'personal information', avoiding the uncertainty that currently exists about when metadata will constitute personal information under Australian law.

Registration data is 'personal information', both because a person is identifiable from it, and because it is 'COVID app data'.

However, section 94Q does not turn 'other tracing data' into 'personal information' under the federal Privacy Act, because it is not COVID app data, and the section does not apply.

'Sensitive information'

'Sensitive information' is defined exhaustively in s. 6(1) of the *Privacy Act*, and the only category within the definition which is likely to be relevant to COVID app data is '(b) health information about an individual'. 'Health information' is further defined, and in turn depends on the definition of 'health service'. Without going into details, it is uncertain from these definitions whether COVID app data would qualify as sensitive information.

However, as a matter of policy, 'COVID app data' should be classified as 'sensitive information', and the Privacy Act should be amended to that effect. Furthermore, because the fact of whether a person has or has not installed the COVIDSafe app on their device is supposed to be a matter of choice, and is something that section 94H prohibits others from requiring (and should prohibit them from requiring to be disclosed), the definition of 'sensitive information' should also include 'information about whether a person has downloaded or installed COVIDSafe'.

Clarifying that all three of these categories of information are 'sensitive information' will have the advantage that APP 3.3 (restricting collection') and other APPs referring to sensitive information will apply (subject to Part VIIIA overriding other Privacy Act provisions).

'Property'

The Act provides that 'COVID app data is the property of the Commonwealth', and that this is so even after the data is disclosed to or used by others, including state and territory health authorities (s. 94ZC). The rationale for this is, we understand, that treating COVID app data as Commonwealth property strengthens the Commonwealth's constitutional position, particularly when that data is in the hands of State and Territory health officials. It might be seen as a ground for arguing that the Commonwealth is providing consideration under any relevant contract between the Commonwealth and the states or territories.

However, data or information *per se* is not recognised as an object of property rights under Australian law,[48] and this seems a very 'back door' attempt to introduce a concept with potentially

[48] See Lyria Bennett Moses, 'Who Owns Information? Law Enforcement Information Sharing as a Case Study in Conceptual Confusion' (2020) *UNSW Law Journal*, forthcoming.

far-reaching consequences. We support the view that this provision should be amended to replace the reference to 'property of the Commonwealth' with a more explicit statement of rights and powers retained by the Commonwealth, and the exclusion of uses by other actors, if that is the intention.[49] If the goal is to establish the respective rights of the Commonwealth and the States and Territories, a less controversial approach may be to establish that the Commonwealth has copyright in the data in the particular form in which it is captured in the NCSDS (if other conditions for the subsistence of copyright can be established). Alternatively, treating COVID app data as confidential data disclosed by the Commonwealth under circumstances of confidence may be worth exploring. Either approach, if effective, would be preferable to simply treating data as property.

4.3. Results of asserting Commonwealth powers

The Commonwealth has only asserted legislative powers over state and territory health authorities to a very limited extent.

Contractual arrangements with States and Territories

The need for such assertions of Commonwealth powers can be seen in the Maddocks PIA Recommendation 12 and the Department's response. 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'.[50] 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. This 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.[51] 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 of Part VIIIA by State/Territory officials.

The Maddocks PIA notes that, aside from community concern about use of the data by state/territory health authorities:[52]

> '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 agreements negotiated by the Commonwealth with state and territory governments have not yet been made public.

Application of federal Privacy Act to States and Territories

The Maddocks PIA recommends that 'ideally' State and Territory officials would be required to comply with the *Privacy Act* as if they were an APP entity, so that there is uniform protection

---

[49] We have had the benefit of discussions with Professor Lyria Bennett Moses in this respect.

[50] Maddocks PIA, Recommendation 12.

[51] The worst case interpretation is that the Department of 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.

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

across jurisdictions. The Act has in s. 94X adopted this recommendation, up to a point, subject to it not being challenged and found to be constitutionally invalid.[53]

The *Privacy Act* applies in relation to a State or Territory health authority, but only 'to the extent that the authority deals with, or the activities of the authority relate to, COVID app data' (s. 94X(1)). It is reiterated in the section that, in relation to state or territory health authorities, this does not 'have the effect of applying this Act in relation to data or information that is not COVID app data' (s. 94X(2)(b)). There is a further derogation that APP 9 (government related identifiers) does not apply to State and Territory health authorities in relation to identifiers assigned by the State or Territory authority, such as a driver's licence number.[54]. To the extent they are not overridden by the provisions in the Bill, the remainder of the APPs will apply to State and Territory health authorities but only in relation to COVID app data.

The result is that 'COVID app data', when in the hands of state and territory health officials, must be dealt with so as to comply with the federal Privacy Act, including Part VIIIA. Dealings with other tracing data (as defined above) need not comply with federal law, but if they deal with personal information (as is likely), then they will need to comply with state or territory privacy laws, where they exist.

4.4. Over-riding application of other laws

Section 94ZD(1) 'cancels the effect of a provision of any Australian law' (which includes State and Territory laws) which would permit or require conduct, or an omission, which would otherwise be prohibited by Part VIIIA. This cancellation does not apply to provisions in any later-enacted Acts if the provision of the later Act 'expressly permits or requires the conduct or omission despite the provisions of' Part VIIIA (s. 94ZD(2)). This exception is very narrow, because, as well as only being prospective, and only applying to Acts and not delegated legislation, the overriding provision must expressly refer to at least Part VIIIA, if not to those specific provisions within Part VIIIA that are to be overridden.

Among its effects, s. 94ZD makes ineffective provisions in the *Privacy Act* (or its state or territory equivalents) that are more permissive than Part VIIIA concerning disclosure of data, or demands to provide data.[55]

4.5. De-identified data

Aside from contact tracing, the Act permits the data store administrator to use the COVID app data 'for the purpose of, and only to the extent required for the purpose of, producing de-identified statistical information about the total number of registrations through COVIDSafe' (s. 94D(2)(f)). This wording gives the impression that COVID app data may be de-identified for the purpose of determining the total number of COVIDSafe registrations and no other purpose. The definition of

---

[53] The alternative would be for legislation complementary to the Commonwealth COVIDSafe legislation to be enacted by each of the States and Territories. In particular, such legislation would need to 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). This would be very difficult to achieve.

[54] This avoids placing limitations on state and territory health authorities (as 'organisations') using their own state or territory identifiers.

[55] The note to cl 7 of the Determination 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 for the period the Determination is in force.

'COVID app data' (s. 94D(5)(d)) now states that it does not include data de-identified for the specific purpose permitted by section 94D(2)(f).[56]

'De-identified' has its usual meaning under section 6(1) of the *Privacy Act*. However, given the increasing difficulty in successfully de-identifying personal data,[57] and the government's recent failure, for example, to adequately de-identify health data which was released to the public and subsequently re-identified,[58] 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 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.

5. Collection

5.1. The COVIDSafe app as a collection device

While the COVIDSafe app[59] is in operation, the relevant communication device acts as a data collection device for the purpose of 'facilitating contact tracing'[60] (s. 6(1), definition of 'COVIDSafe'). However, the Act is unacceptably vague about the types and scope of data collected, used and disclosed by the app.

5.2. Data collected

The Act does not define the types of data that will be collected and stored on the device (s. 94D(5)). 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;[61] their age range;[62] and their postcode;

---

[56] In the exposure draft Bill, the definition of 'COVID app data' excluded any 'de-identified data'. In our 'Phase II' article, we recommended the addition of the words 'pursuant to section 94D(2)(f)' to clarify that permitted de-identification is limited in this way. The new definition in the Bill is to the same effect.

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

[58] 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/

[59] A new definition in s. 6(1) provides '*COVIDSafe* means an app that is made available or has been made available (including before the commencement of this Part), by or on behalf of the Commonwealth, for the purpose of facilitating contact tracing.'

[60] The definitions provide that '*contact tracing* has the meaning given by subsection 94D(6)'.

[61] 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'.

- Information about the user's encrypted ID (date and time of contact, and Bluetooth strength of other COVIDSafe users 'with which you come into contact') when the COVIDSafe app is open or running on their device;
- Information that the user has tested positive to COVID-19 if the user agrees to a health official sending the user a PIN by 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 NCSDS.[63] 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.'

The developers of the Singaporean contact tracing app, 'TraceTogether', in Singapore's Government Technology Agency, have released an overview of 'BlueTrace, the privacy-preserving protocol that underpins TraceTogether'. The protocol includes numerous recommendations for preserving privacy through the design of the app, including the issuing and cycling of encrypted temporary encrypted identifiers. According to the protocol:[64]

> 'TempIDs have a short lifetime (we recommend 15 minutes). This helps mitigate the impact of replay attacks, by reducing the window of opportunity for exploitation. If malicious users impersonate other users by rebroadcasting their messages, they will only be able to do so for a short time before the message expires. This duration would likely be below the threshold duration of close contact, and hence not result in false positives …'

The developers also point out that using temporary identifiers can 'prevent users from being tracked over time by third parties'. They emphasise the importance of sending batches of temporary identifiers from the central data store:[65]

> 'In order to ensure that devices have a supply of valid TempIDs even when the internet connection is unstable, devices pull batches of forward-dated TempIDs from the health authority's back-end service back-end service each time …'

---

[62] 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?

[63] 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.'

[64] Jason Bay et al, 'BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders' (Government Technology Agency, Singapore, 9 April 2020) 2.

[65] Jason Bay et al, 'BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders' (Government Technology Agency, Singapore, 9 April 2020) 2.

The protocol suggests that issuing batches of these temporary identifiers on a daily basis 'has a secondary benefit of allowing the healthy authority to understand adoption and usage levels of the app … and its potential effectiveness in epidemic control'.[66] That is, if the batch of TempIDs is successfully delivered, it indicates to the government that the app is actually in use.

In contrast to these recommendations, the NCSDS sends one temporary identifier to the user's mobile device every two hours. The frequency of cycling COVIDSafe encrypted IDs and logging those IDs with the NCSDS has two implications. First, creating a new encrypted ID only every two hours (as opposed to 15 minutes) increases the risk that a user's series of contacts will be tracked over time by third parties, including, for example, perpetrators of domestic violence.[67] Second, logging a user's encrypted IDs with the NCSDS every two hours (as opposed to once a day) means that the government is able to more closely monitor a user's usage of the app.[68]

5.3. 'Proximity'

There is no definition of 'proximity' in the Act. It is only mentioned when a person is defined as being 'in contact' with another person, namely 'if the operation of COVIDSafe in relation to the person indicates the person may have been in the proximity of the other person' (s. 6(1)). (The definition should more accurately refer to an indication that one user's device has been in the proximity of the other user's device.) However, the Act does not indicate the criteria for this 'proximity' occurring. 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, and transfers to the NCSDS when a user requests, a far broader amount of data (on 'bystanders') than the data which is eventually passed to contact tracers. The substantive meaning of 'proximity' is determined in the interactions between the NCSDS and the contact tracers, [69] but the details of this are not yet public.

This is an unjustifiable situation: the extent of the interference with privacy posed by the COVIDSafe app is left completely unexplained in the Act, and is in fact left completely to the (changeable) discretion of those who control the app or (more likely) the NCSDS. The COVIDSafe Act should define 'proximity', or at least how it is determined. The inadequate definition of the controller of the COVIDSafe app, and of the administrator of the NCSDS, is discussed in Part 6..

5.4. 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 collection of data extends to data about all other mobiles within Bluetooth signal range which have the app installed, and not only such devices as meet the original proximity criteria, stated by the Health Department,

---

[66] Jason Bay et al, 'BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders' (Government Technology Agency, Singapore, 9 April 2020) 6.

[67] See Letter from Australian Communications Consumer Action Network (ACCAN) and other NGOs to the Hon Greg Hunt MP, Minister for Health (11 May 2020) 2, expressing concern that security weaknesses in the COVIDSafe app could 'enable a perpetrator of domestic violence to deduce who the victim's close contacts are and when and for how long they have visited them'.

[68] 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

[69] See further section 5.1 below on the lack of restrictions based on proximity criteria.

of 1.5 metres distance or less for a period of at least 15 minutes.[70] When promoting the COVIDSafe app, the Government Services Minister repeatedly stated in the media – and the media and others have widely reported –[71] that COVIDSafe only records contacts with other app users which are within 1.5 metres of the user for at least 15 minutes.[72] 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.[73] 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.

According to the PIA:[74]

> '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:[75]

> 'A Digital Handshake will only include the following information (stored in an encrypted form on the User's device):

---

[70] 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>

[71] See, eg, Information Governance ANZ, 'COVIDSafe App: Are the risks work it for the recovery?' (4 May 2020) <COVIDSafe App – are the risks worth it for the recovery?>

[72] 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

[73] 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

[74] Maddocks PIA, p 19 para 8.21.

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

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.'

According to the PIA, the COVIDSafe app records all 'Digital Handshakes' between users' devices 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 NCSDS a log of all Digital Handshakes that user's device has recorded over the previous 21 days, regardless of duration or the distance between users.[76] When the log of encrypted user IDs is received at the NCSDS, all contacts' encrypted IDs are decrypted, regardless of duration or the distance between users.[77] At that point, the Department of Health since stated in its Response to the PIA 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,[78] although this restriction has not been incorporated in the Act.

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 NCSDS 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. In other words, 'contact events' are a much larger set than what are understood to be 'proximity events'.

This means that vastly more potentially revealing data concerning a person's movements, associations and interactions may be collected than accords with the popular understanding, while this data is irrelevant to contact tracing.[79] 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 unauthorised access to, and disclosure of data from, the NCSDS, as well as the risks of decryption of the data on the mobile device itself.

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

In the PIA, Maddocks recommended that the Department investigate whether it is technologically possible to:[80]

- 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

---

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

[77] Maddocks PIA, p 21 para 8.39.

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

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

[80] Maddocks PIA, p 13 Recommendation 18.

- 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:[81]

> '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 minimise the data collected, transferred and stored. The Department of Health only indicated it was opting for the alternative which maximises the personal information collected at the NCSDS. The government should investigate which of the first three options is technologically feasible, and implement that which minimises the data collected.

Even if none of the preferable options is technically feasible, the legislation should, at the very least, create a legal requirement which restricts the access of state and territory health officials to contacts which meet specific proximity criteria.

6. Storage and security

6.1. 'National COVIDSafe Data Store' (NCSDS), and shifting responsibility for it

The 'National COVIDSafe Data Store' (NCSDS) is defined in s. 6(1) as 'the database administered by or on behalf of the Commonwealth for the purpose of contact tracing', and is referred to frequently in the Act. Which Commonwealth agency 'administers' this entity, the NCSDS? It would make a great deal of difference to public trust if the answer – either now or in future – is the Department of Home Affairs, or some other law-enforcement or surveillance-oriented agency, rather than the Department of Health. It does not matter who the Explanatory Memorandum, the FAQs for the COVIDSafe system, or other explanatory material says it is, or who it actually is, at the moment. What matters is what the legislation provides. The Determination was silent.

The Act does not make an explicit statement as to which agency administers the NCSDS. Another s. 6(1) definition defines the 'data store administrator' as 'the Health Department', unless a notifiable Determination by the Secretary of the Health Department under section 94Z makes some other agency the administrator (but the extent of its role may be limited to only some of the provisions in Part VIIIA). The 'data store administrator' is referred to nine further times in the Act, and it seems that they administer the NCSDS. A change since the exposure draft Bill now adds s. 94Z(3) which provides that the Determination by the Secretary cannot make an 'enforcement body' (as defined in s. 6(1)), 'an intelligence agency', or two named intelligence bodies, the 'data store administrator'.[82] This is a valuable clarification.

The result, therefore, is that the government can move administrative control of the NCSDS from the Department of Health, for which there is already a very low level of public trust in relation to the operation of sensitive databases,[83] to any other agency (still including Home Affairs),[84] but not

---

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

[82] The Australian Geospatial Intelligence Organisation and the Defence Intelligence Organisation.

[83] See, eg, 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/

law enforcement or intelligence bodies, without obtaining prior Parliamentary approval. Such bureaucratic flexibility may be convenient in Canberra, but for many people it justifiably breeds suspicion, because of a perceived history of privacy abuses. To maximise public trust, the COVIDSafe Act should state who is the NCSDS data controller, and that this cannot be changed without further legislative amendment.

6.2. COVIDSafe app, and (lack of) responsibility for it

COVIDSafe is defined as 'an app that is made available or has been made available (including before the commencement of this Part), by or on behalf of the Commonwealth, for the purpose of facilitating contact tracing.' This definition does not specify which agency makes the app 'available'. The whole purpose of the app is to collect personal information (both registration data and, subsequently, COVID app data), and communicate it to the NCSDS under certain circumstances. The app may contain security flaws which allow personal data to be wrongly disclosed, or excess collection of personal information, or result in notifiable data breaches, or other interferences with privacy. Who is responsible for them, who should be prosecuted as a result, and who should be the respondent when individuals complain to the Privacy Commissioner?

Common sense says that the same agency as is responsible for the NCSDS – currently the Department of Health – should also be responsible for both the COVIDSafe app, and the whole COVIDSafe system for that matter. But there is nothing in the Act to clarify this, or even to state that a section 94Z Determination will change responsibility for the COVIDSafe app along with the NCSDS. In fact, common sense does not prevail at present, and the responsibility for the app rests with the Digital Transformation Agency,[85] which is not part of the Department of Health. Given the history of the Commonwealth government in denying responsibility for extremely cruel and damaging computing disasters such as RoboDebt, the appearance of obfuscation in who is legally responsible for the COVIDSafe system can and should create public mistrust.

7. Use and disclosure

7.1. User uploads of COVID app data

The Act makes it an offence to upload COVID app data from a communication device to the NCSDS without the consent of the 'COVIDSafe user' in relation to that device, or their parent, guardian or carer (s. 94E). The 'COVIDSafe user' is defined as 'the person whose registration data was uploaded from' that device 'when the user was registered through COVIDSafe' (s. 6(1)).

This is an improvement on the original Determination made with the release of the app, which only required consent to upload from 'the person who has possession or control of the device' (cl. 7(1)), which might have included a health official or police officer in possession or control of a user's mobile device.

7.2. Controlling dealing with 'COVID app data'

Under the Act, the general position is that it is an offence for any person to collect, use or disclose COVID app data (s. 94D(1)). The offence is punishable by imprisonment for 5 years or $63,000, or

---

[84] A recent example of perceived privacy abuse by Home Affairs is described in Paul Karp, 'Home affairs data breach may have exposed personal details of 700,000 migrants' (3 May 2020) < https://www.theguardian.com/technology/2020/may/03/home-affairs-data-breach-may-have-exposed-personal-details-of-700000-migrants>

[85] Digital Transformation Agency <https://www.dta.gov.au/>

both. The Act also provides a list of situations in which the collection, use or disclosure of COVID app data is permitted, which are the only exceptions to the general prohibition (s. 94D(2), (3)). It would be preferable for section 94D to refer to "access" in addition to "collection, use or disclosure", particularly since there is a line of case law in which Australian courts have held that "mere access" or "mere viewing" is not considered a "use" of data.[86]

In broad terms, the permitted collections, uses or disclosures are those which are for the purpose of, and only to the extent required for the purpose of:

- Contact tracing by a person employed, or in the service of, a state or territory health authority;
- The data store administrator's officers, employees or contractors enabling contact tracing by those authorities, or ensuring the functioning, integrity or security of the NCSDS;
- Transferring encrypted COVID app data between the communication devices of users, or between the device of a user and the NCSDS (collection and disclosure only);
- The Privacy Commissioner performing functions or exercising powers under Part VIIIA;
- Investigating whether the Part VIIIA has been contravened or prosecuting an offence under that Part;
- The data store administrator producing de-identified statistical information about the total number of registrations through COVIDSafe; or
- The data store administrator confirming that the correct data is being deleted in accordance with section 94L, which permits deletion of registration data at a user's request (s. 94D(2)).

There is a further exception where COVID app data is collected as part of, simultaneously with and incidental to, the collection of other non-COVID app data, where the collection of the non-COVID app data is permitted under an Australian law, so long as the COVID app data is deleted as soon as practicable after the person becomes aware that it had been collected; and is not otherwise accessed, used or disclosed by the person collecting it after it was collected (s. 94D(3)). This would appear to cover the situation where law enforcement officers lawfully access all of the data on a person's phone, and subsequently discover that data includes COVID app data.

It is also an offence for a person to decrypt encrypted COVID app data that is stored on a mobile device (s. 94G). Again, the offence is punishable by imprisonment for 5 years or $63,000, or both.

7.3. Stopping coerced use: Loopholes must be closed

There is a considerable risk that employers will insist that any employees coming back to work have the app installed on their phone, in order to protect co-workers or customers. Universities and schools might do likewise as a condition of attendance. Public events, and even restaurants, might make it a condition of entry. Minor changes to State and Territory regulations that require people to have 'a reasonable excuse'[87] or 'acceptable reason' to leave their homes (as in NSW,[88] Qld, Vic)[89]

---

[86] See Anna Johnston, extracts from 'PPIPA in Practice', Edition 14.1, May 2020; available at https://www.salingerprivacy.com.au/downloads/ppipa-in-practice/ , citing *JD v Department of Health* (GD) [2005] NSWADTAP 44 at [42]; *Director General, Department of Education and Training v MT* (GD) [2005] NSWADTAP 77 at [42], [44]; *Director General, Department of Education and Training v MT* (GD) [2005] NSWADTAP 77 at [45]); *SF v Shoalhaven City Council* [2013] NSWADT 94 at [181]).

[87] Explainer ''Stop looking for loopholes': What are the new COVID-19 social rules? Sydney Morning Herald, 18 April 2020 https://www.smh.com.au/national/stop-looking-for-loopholes-what-are-the-new-covid-19-social-rules-20200407-p54hyd.html

[88] Public Health (COVID-19 Restrictions on Gathering and Movement) Order 2020 (NSW) *Gazette*, 30 March 2020 https://gazette.legislation.nsw.gov.au/so/download.w3p?id=Gazette_2020_2020-65.pdf

could make it necessary to have the app installed in order to comply. Being required to take self-surveillance with you would give new meaning to the old Amex slogan 'don't leave home without it'. Those who don't like it would be told they can stay home. The use of the app is not 'voluntary' under these circumstances.

These are all examples of what is called 'pseudo-voluntary' compliance. By such means, a supposedly voluntary form of surveillance becomes *de facto* compulsory. Australia has previously rejected the pseudo-voluntary Australia Card (1987)[90] and the Health and Welfare Access Card[91] (2007). The US Electronic Frontier Foundation (EFF) warns against such dangers.[92] A draft *Coronavirus (Safeguards) Bill 2020* by UK academics[93] has as its first provision 'No sanctions for failing to carry personal device, install or run application'. We have warned about this problem from prior to the release of the app.[94]

In relation to the COVIDSafe system, the federal government has been attentive to this problem from the outset. The provisions of s. 9 of the Determination 'Coercing the use of COVIDSafe', are largely duplicated in s. 94H of the Act 'Requiring the use of COVIDSafe'. These provisions are a good start to dealing with the issue, but are not comprehensive enough, and have loopholes.

Section 94H(1), reproduced below, requires amendment by addition of the words in ***bold italics***:

> (1) A person commits an offence if the person requires another person to:
> (a) download COVIDSafe to a communication device; or
> (b) have COVIDSafe ***installed or*** in operation on a communication device; or
> (c) consent to uploading COVID app data from a communication device to the National COVIDSafe Data Store; ***or***
> (d) ***disclose or demonstrate that they have done any of (a)-(c)***.
> Penalty: Imprisonment for 5 years or 300 penalty units, or both.

The amendment to (b) is for the avoidance of doubt, and (d) is because third parties can achieve the same undesirable effect as requiring downloading simply by requiring a person to demonstrate that they have COVIDSafe installed, or abuse their honesty by requiring them to disclose whether they do.

Section 94H(2) is already in reasonably broad terms, but it is clear that it still has loopholes, from statements by chambers of commerce (recommending businesses require that customers install)[95]

---

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

[90] G. Greenleaf 'The Australia Card: Towards a National Surveillance System' *Law Society Journal* (NSW) Vol. 25, No. 9, October 1987, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2195493

[91] G. Greenleaf ''Access All Areas': Function Creep Guaranteed in Australia's ID Card Bill (No. 1)' Computer Law and Security Review, [GET CITATION] 2007 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=966710>

[92] A. Crocker, K. Opsahl and B. Cyphers 'The Challenge of Proximity Apps For COVID-19 Contact Tracing' Electronic Frontier Foundation (EFF) <https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing>

[93] 'The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates' <https://osf.io/preprints/lawarxiv/yc6xu/>

[94] 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

[95] L. Visentin ''Wimped out': COVIDSafe app should be compulsory, says local chamber of commerce' Sydney Morning Herald 28 April 2020 < https://www.smh.com.au/national/nsw/wimped-out-covidsafe-app-should-be-compulsory-says-local-chamber-of-commerce-20200428-p54o06.html>

local councils (requiring all employees to install)[96], articles by behavioural economists (recommending tax and utility fee discounts, among other 'nudges'),[97] and repeated comments in social media discussion to the effect that 'if an employer owns the phone, it can install whatever it likes on it'.[98]

Section 94H(2) is reproduced below:

> (2) A person commits an offence if the person:
> (a) refuses to enter into, or continue, a contract or arrangement with another person (including a contract of employment); or
> (b) takes adverse action (within the meaning of the *Fair Work Act 2009*) against another person; or
> (c) refuses to allow another person to enter:
> (i) premises that are otherwise accessible to the public; or
> (ii) premises that the other person has a right to enter; or
> (d) refuses to allow another person to participate in an activity; or
> (e) refuses to receive goods or services from another person, or insists on providing less monetary consideration for the goods or services; or
> (f) refuses to provide goods or services to another person, or insists on receiving more monetary consideration for the good or services;
> on the ground that, or on grounds that include the ground that, the other person: [*the provisions of s. 94H(1) are substantively reproduced here*]

Subsections (2)(e) and (2)(f) have been modified by the addition of the prohibition on offering less or requiring more financial incentives on the basis of use/non-use of the app.[99] Example are that a hairdresser will not be able to demand a higher payment from a non-app user, and a gym would not be able to offer a 10% discount on membership to those who had registered to use the app.

We have argued[100] that these prohibitions are not comprehensive enough of the coercive behaviour that needs to be prevented. The following should also be included in s. 94H(2):

- Where a person requires another person to accept discriminatory conditions as an alternative to the refusals, adverse actions or denials in (a)-(f) above. For example, if a restaurant, cinema or sporting venue can ask a person to disclose or demonstrate whether they have the app installed, they could (without requiring them to install it), set all those who do not in a segregated area (some have called it 'leper colony' seating). Alternatively, they could insist that such persons provide identification details, whereas this is not required of other patrons.[101]

---

[96] Strathfield Council proposed to do so until a NSW Minister made it clear this would be illegal.

[97] J. Hawkins and B. Freyens 'Contact tracing apps: a behavioural economist's guide to improving uptake' *The Conversation*, 30 April 2020; D. Byrne, R.Holden and J. Miller 'The big nudge: here's how the government could spread its coronavirus tracing app far, fast and wide' *Crikey* 27 April 2020 https://www.crikey.com.au/2020/04/27/covidsafe-public-nudge/

[98] See reader comments on K. Kemp and G. Greenleaf 'The COVIDSafe bill doesn't go far enough to protect our privacy. Here's what needs to change' *The Conversation*, 6 May 2020 < https://theconversation.com/the-covidsafe-bill-doesnt-go-far-enough-to-protect-our-privacy-heres-what-needs-to-change-137880#comment_2216305>

[99] This change was recommended in our 'Phase II' paper, where we said one ground should be that a person 'denies another person a discount, payment or any other financial incentive'.

[100] In our 'Phase II' article.

[101] A similar point is made by Galloway and Castan: 'The nature of the COVIDSafe app and its purpose have created a novel type of status that lies beyond mere data protection, or privacy. In its desire to 'encourage public acceptance and uptake' of a data collection technology, the government is creating a new form of identifying feature to distinguish between individuals, based on their data choices or their ability to enter into the data arrangements. Despite criminal

- Where a person refuses to allow another person to benefit from an exception to 'stay at home' orders and similar orders by any government, including under any emergency legislation. Police are empowered to enforce compliance with exceptions to such orders, and it is conceivable that they would ask people in parks or on walks to display the app or move on or to go home.
- Where a person causes COVIDSafe to be installed on a device which is used by another person or persons, irrespective of who is the owner of the device. This problem may arise for those who have employer-owned phones on which the app is pre-installed in their names. The employee is not to be required to download the app or have it operational, but if they do nothing to turn it off, the effect is the same.

Without these changes, installation and use of the app will, as a result, become compulsory for many people. To be effective, the prohibitions must include all State and Territory government bodies and public corporations, and all local government entities.

8. Overseas transfers

8.1. Data localisation

The Act requires that COVID app data uploaded from a mobile device to the NCSDS must only be held on databases located in Australia and only disclosed for permitted purposes to persons physically located in Australia (s. 94F). This is a necessary instance of data localisation, but the effectiveness of this provision in the face of the US CLOUD Act must be established.

8.2. NCSDS and the US CLOUD Act

There are potentially circumstances in which US Stored Communications Act (1986), as amended by 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 would not be entitled to bring a motion to quash or modify that legal process in a US court under the CLOUD Act, on the basis that disclosure would contravene a law of Australia, since the Australian government is not a "qualifying foreign government" under the Act. Home Affairs Minister Dutton introduced a bill in March 2020[102] (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.

Outside the provisions of the CLOUD Act, there is an argument that AWS would be able to challenge any US legal process that would compel it to disclose COVID app data to US authorities, on the basis of common law defences which are not modified by the CLOUD Act.[103] In such a case, US courts would be required to apply 'comity principles' under US common law. It is not possible to say with any certainty what the outcome of such a challenge would be. It is also possible that the

---

sanctions against coercion, the Draft Bill has not afforded substantive rights concerning discrimination on the grounds of data status.' Kate Galloway and Melissa Castan, 'COVIDSafe and Identity: Governance Beyond Privacy' on AUSPUBLAW (11 May 2020) <https://auspublaw.org/2020/05/covidsafe-and-identity-governance-beyond-privacy>

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

[103] Parliamentary Library, Parliament of Australia, 'COVIDSafe app and Biosecurity Determination' (Client Advice to the Office of Senator Nick McKim, 1 May 2020) 23-25.

US would assert investigative powers in respect of data held by AWS even outside the CLOUD Act, on the basis of the Convention on Cybercrime ('the Budapest Convention'), which Australia ratified in 2012.[104]

An answer to the question whether data held by AWS as part of its COVIDSafe contract would be subject to the US CLOUD Act, the IPO Bill or the Budapest Convention 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 or the Budapest Convention should be made public; and

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

9. Deletion

The deletion provisions in the COVIDSafe Act are all important aspects of the voluntary nature of the COVIDSafe system, necessary to guarantee that users can opt out of the system, and that data obtained from them is not used beyond its intended purpose. There are four forms of deletion.

9.1. Automatic deletion from user devices after 21 days

Data about a user's contacts is only kept on their mobile device for 21 days after the occurrence of that contact. The Act requires the NCSDS administrator to 'take all reasonable steps to ensure that COVID app data is not retained on a communication device' for more than 21 days, or 'for longer than the shortest practicable period' if it is not possible to comply with that obligation (s. 94K). This is in keeping with the purpose of the app, since, based on our current understanding of the virus, contact data is most unlikely to be of any relevance for contact tracing if the contacts occurred more than 21 days before the user tests positive for COVID-19.

9.2. Deletion on request from the NCSDS of registration data (only)

A user can also have some of their data deleted on request. A registered user can request the NCSDS administrator to delete their registration data and the administrator must take all reasonable steps to delete the data as soon as practicable, and 'must not use or disclose the data for any purpose … if it is not practicable to delete the data immediately' (s. 94L(1)). However, upon such a request being made, the administrator is not required to delete:

- 'data relating to' the person making the deletion request that was uploaded from another COVIDSafe user's communication device to the NCSDS and was collected through that device interacting with the communication device of the person making the deletion request (s. 94L(3)); or
- 'data that is de-identified' (s. 94L(4)).

Section 94L(4) should be replaced by a provision that replicates the requirements of section 94D(2)(f), such as:

---

[104] US Department of Justice, 'Promoting public safety, privacy, and the rule of law around the world: the purpose and impact of the CLOUD Act' (White Paper, April 2019) pp. 6, 7, 11; Parliamentary Library, Parliament of Australia, 'COVIDSafe app and Biosecurity Determination' (Client Advice to the Office of Senator Nick McKim, 1 May 2020) 16.

> 'This section does not apply to data that is de-identified statistical information about the total number of registrations through COVIDSafe that is produced by:
>
> (i) an officer or employee of the data store administrator; or
>
> (ii) a contracted service provider for a government contract with the data store administrator.'

This would ensure that only data de-identified in accordance with the permitted purpose in section 94D(2)(f) is exempt from deletion on request.

The right to request deletion only relates to a user's registration data (that is, the name, mobile number, age range and postcode provided upon registration), and does not apply to the COVID app data collected by the Bluetooth contact tracking facility of the app (the 'contact log'). If the user has previously tested positive for COVID-19 and consented to upload their contact log to the NCSDS, that contact log and any data derived or transformed from it, will not be deleted upon request (discussed further below).

A user can put an end to the future collection of their COVID app data by deleting the app from their device. If a user deletes the COVIDSafe app from a device (and has not downloaded the app again), the NCSDS administrator must not collect COVID app data relating to that person from that mobile device (s. 94N). This would not, however, automatically result in the user's registration data being deleted from the central data store. The user would need to request such deletion as a separate step under s. 94 L. The wording of the draft Bill does not appear to preclude a user making such a request after deleting the app from their mobile device, but it is likely to be logistically more convenient to request deletion of registration data via the app prior to deleting the app. As an element of 'privacy by design' the app should contain a simple-to-use facility by which users can delete their registration data from the NCSDS.

The Act also provides that a person 'who receives COVID app data in error must, as soon as practicable, … delete the data; and … notify the data store administrator that the person received the data' (s. 94M).

The next three sub-parts concern deficiencies in the provisions for retention and deletion of COVID app data.

9.3. Deletion of COVID app data from NCSDS

Retaining COVID app data in the NCSDS until the end of the pandemic, and not allowing users to have it deleted on request, does not sit well with the objectives of the Act, namely 'to assist in preventing and controlling the entry, emergence, establishment or spread of' COVID-19 in Australia 'by providing stronger privacy protections for COVID app data and COVIDSafe users in order to … encourage public acceptance and uptake of COVIDSafe; and … enable faster and more effective contact tracing' (s. 94B). Retaining COVID app data for potentially many months after any contact tracing has or could effectively take place will neither increase public confidence nor enable faster or more effective contact tracing.

On the other hand, there are good reasons why COVID app data (contact logs) voluntarily uploaded to the NCSDS by a user may need to be retained longer than some users might prefer:

- Contact tracing by state and territory health officials may be taking longer than expected, and the data has not yet been downloaded by them; or
- Health officials, and independent assessors, may need to use the data in order to periodically assess the effectiveness of the COVIDSafe system (see part 2.1), which might only occur quarterly (or at some other interval).

We do not know how many months or years it will be necessary to keep the COVIDSafe system operational (or before the pandemic is over), but it may be far longer than these two reasons for retention. There is no justification for the COVID app data to be kept in the NCSDS indefinitely.

In our view, the legislation should require the NCSDS administrator to delete any uploaded contact logs within a period which is specified (on expert advice) to be sufficient for the two situations described above to be accommodated.[105] This will ensure that data is only retained only for so long as it is necessary to fulfil the objectives of COVIDSafe. This will also reduce considerably the significance of the determination of the 'end date' when the COVIDSafe system is no longer needed, or the pandemic is over, discussed next.

9.4. Deletion of COVID app data once pandemic is over

As the Act stands, in the absence of a request from a user to delete their registration data under section 94L, the user's registration data will be kept in the NCSDS until 'the end of the COVIDSafe data period', a date that is to be determined by the Health Minister under section 94Y(1). Any COVID app data uploaded from a user's mobile device to the NCSDS with the user's consent after a positive COVID-19 test, or from any other user's mobile device with their consent after a positive COVID-19 test, will also be kept on the NCSDS until the end of the 'COVIDSafe data period', since this data cannot be deleted at the user's request.

The data store administrator must delete all COVID app data from the NCSDS '[a]s soon as reasonably practicable after the end of the day' determined to be the end of the COVIDSafe data period (s. 94P). The data store administrator must also inform all COVIDSafe users, the Health Minister and the Privacy Commissioner of this deletion (s. 94P(3)). The latter would permit the Privacy Commissioner to conduct a review to ensure compliance with s. 94P (s. 94T, EM [39], [138]-[141]).

The mechanism for determining the end of the pandemic under the Act should ensure that the end date is based on the objective advice of independent health experts, rather than political advice. The Act provides that the Health Minister must determine a day by which 'use of COVIDSafe … is no longer required to prevent or control; or … is no longer likely to be effective in preventing or controlling; the entry, emergence, establishment or spread' of COVID-19 into Australia or any part of Australia (s. 94Y(1)). The Act currently provides that the Health Minister must not make this determination 'unless the Health Minister has consulted, or considered recommendations from, the Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee' (s. 94Y(2)), and that either of those entities 'may recommend to the Health Minister that the Health Minister' make the determination of the COVIDSafe end date (s. 94Y(3)). The legislation should include an obligation on the Health Minister to make public any such recommendation from the CMO or the Committee.

One weakness with this provision is that it does not state that the AHPPC or CMO is entitled to give such advice unsolicited by the Health Minister. Both may be reluctant to do so, and the Minister may prefer to keep the surveillance system in place longer than is necessary, so s/he will not request advice on the question. One solution to this is to allow either the federal Privacy Commissioner or the Australian privacy commissioners acting collectively, to request the AHPPC or CMO to give advice to the Minister on this question. Since they have a specific interest in the protection of privacy, including termination of the COVIDSafe system, that may overcome the problem.

---

[105] See further Malcolm Crompton, Anna Johnston, Peter Leonard et al, 'Good legislation to make COVIDSafe trustworthy' (1 May 2020) < https://www.gtlaw.com.au/insights/good-legislation-make-covidsafe-trustworthy>, arguing that 'COVIDSafe app data (and associated metadata and records in any form of that data and metadata) should be scheduled for deletion and reliably deleted during the life of the pandemic as that COVIDSafe app data ceases to be current for contact tracing'.

9.5. Deletion of COVID app data held outside the NCSDS

The Act does not address the need to delete 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, but only individuals who have been identified as potentially relevant contacts to trace (and who have registered with the NCSDS). Given the importance placed on the voluntary nature of the app, there should be effective deletion requirements for this data, if the public is to trust government assurances that this is temporary collection and use of data. The Commonwealth claims to have sufficient constitutional powers (see part 4.1 above) for legislation to govern the actions of state and territory health officials for this purpose. There are no such obligations in the Act at present.

9.6. Repeal of all legislative provisions

Schedule 2 of the Act provides for the automatic repeal of Part VIIIA, and the definitions added to the *Privacy Act* by the Act, such repeals to commence at the end of 90 days after the day determined under section 94Y(1) discussed above. The Act clarifies that, notwithstanding this repeal of Part VIIIA, the powers of the Privacy Commissioner under or in relation to PartVIIIA 'continue to apply in relation to matters that arose under or in relation to that Part before that commencement' as if the repeal had not been made (Sched. 2, Item 4).

The period of 90 days before the automatic repeal should be sufficient for the NCSDS administrator to shut the system down, and delete data, as well as for privacy authorities to complete exchanges of data and other cooperation on outstanding issues and investigations.

This provision for automatic repeal is a significant privacy protection, but one that should not be exaggerated. The COVIDSafe system will not sit in 'legislative mothballs', needing only bureaucratic activity to make it operative again. New legislation – even if only a Determination under an emergency – would be needed to start it again. But we now know from experience that extraordinary surveillance systems can be built, made operative, and legitimated, in a very short period of time, and before Parliamentary consideration.

10. Enforcement

10.1. Criminal penalties

The Determination's only means of enforcement were through the criminal law. Superficially, the Act takes a similar approach, with various the provisions in Division 2 (s. 94D – s. 94H) stating that 'a person' (Commonwealth official, private sector party, and at least in some cases, State or Territory officials) 'commits an offence' if they do various things. Maximum penalties are the same as under the Determination: $63,000 (300 penalty units) or 5 years imprisonment or both.

The provisions in Division 3 (s. 94K – s. 94P) are mainly concerned with specifying the obligations of the data store administrator, and failure to observe these provisions does not constitute a criminal offence carrying specific penalties.

10.2. Individual enforcement and remedies

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 the 'coercion' provisions (s. 94H) will be sporadic, if it ever occurs. If criminal penalties were the only means of enforcement of protections in relation to the COVIDSafe app, there would be no reason why the

public should have any confidence at all in them. It is likely that many civil society organisations would argue that they are largely worthless protections, and should not be trusted.

We previously argued[106] that the COVIDSafe Act must provide remedies that individuals affected by breaches of the law can initiate for their own protection, and to obtain compensation for harms.[107] Such remedies must include both injunctive relief and compensation. We expressed the view that 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*, 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).[108]

This approach has been taken in the Act, and is one of its best aspects. An act or practice in breach of requirements in Part VIIIA 'in relation to an individual constitutes an interference with the privacy of the individual for the purposes of s. 13' (s. 94R(1)), and thus gives rise to a right to complain to the Privacy Commissioner under s. 36. This applies to breaches of both Division 2 and Division 3 discussed above. Exemptions for security agencies are removed (s. 94R(2)). A similar approach to creating rights to complain to the Privacy Commissioner is taken in relation to data breaches (and resulting obligations to give data breach notifications) concerning COVID app data, whether by the NCSDS administrator or a state or territory health authority (s. 94S).

The addition of a provision requiring the Privacy Commissioner to provide regular reporting on the number of enforcement activities undertaken under the Act (s. 94ZB) is useful, but not explicit enough. It needs to state that it requires:

(i) Details of prosecutions and their results, not only complaints;
(ii) Details of State and Territory prosecutions, and complaints, and their results; and
(iii) Details of all complaints received, how they were disposed of, and the remedies that resulted. Complaints which do not result in prosecutions or remedies are just as important as those that do.

This is a national scheme, and there needs to be one consolidated national report, or the public will never be able to work out how much enforcement occurs.

We also argued previously that, because dissatisfaction with the Privacy Commissioner being the sole source of remedies for breaches of data privacy rights is common, there is a need for the COVIDSafe Act, in order to encourage public trust, to be seen as going beyond the (ineffective) norm. It should include two additional avenues through which such remedies should be able to be obtained:

(i) The Australian Competition and Consumer Commission has recommended that individuals should be able to seek the same remedies from a court as are available from

---

[106] G. Greenleaf and K. Kemp 'Australia's 'COVIDSafe App': An experiment in surveillance, trust and law', 1 May 2020, Work-in-Progress draft at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589317> See further See Letter from ACCAN and other NGOs to the Hon Greg Hunt MP, Minister for Health (11 May 2020) 4, emphasising the need for 'personal action for misuse of data and any other breaches [to] be included in the Bill to allow those affected not only to complain to the [OAIC], but also have legal access to compensation and to take out injunctions if needed'.

[107] 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.

[108] *Privacy Act*, 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.

the Privacy Commissioner under the *Privacy Act*.[109] For the same reasons, such an avenue of redress should be available here.

(ii) For enforcement of provisions in some sectors, such as employers, or businesses illegally requiring downloading and use of the app, more effective and trusted enforcement could be obtained through other legal avenues (eg, the *Fair Work Act* for s. 94H(2)(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 used where there is some special reason to choose that route.

10.3. Other relevant powers of federal Privacy Commissioner

Some other powers of the federal Privacy Commissioner are expressly retained in relation to matters under Part VIIIA. The Commissioner may conduct an assessment under *Privacy Act* s. 33 (similar to an audit of privacy practices) relating to COVID app data, including an audit of a state or territory authority (s. 94T).

Where the federal Privacy Commissioner is investigating a complaint under s. 40, s/he must inform the Commissioner of Police or the Director of Public Prosecutions if s/he forms the opinion that an offence may have been committed under Division 2 of Part VIIIA, or certain other offences (s. 94U(1),(2)). Upon forming this opinion, the Privacy Commissioner must 'discontinue the investigation except to the extent that it concerns matters unconnected with the offence that the Commissioner believes may have been committed' (s. 94U(2)(c)). The Privacy Commissioner may also continue the investigation in respect of matters connected with the potential offence if the Commissioner of Police or the DPP notifies the Privacy Commissioner that s/he is satisfied that their investigation 'will not be jeopardised, or otherwise affected, by continuation of the Commissioner's investigation' (s. 94U(4),(5)). Section 94U is a valuable provision because it means that the function of investigation of civil law complaints by the Privacy Commissioner can result in independent assessments and referrals concerning possible criminal offences, making that aspect of the enforcement structure more likely to be used.

10.4. Independent oversight: A National Privacy Advisory Council

The COVIDSafe system is a joint scheme authorising and requiring collaborative actions by officials from all Australian jurisdictions, particularly health officials and privacy officials. 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'.[110] 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. Irrespective of what their individual Acts seem to authorise them to speak out about, it is rare for the public to ever hear them speak about privacy issues that are of great concern to the community.

---

[109] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (June 2019) 473.

[110] LCA *Principles*, principle 7.

One reason for this is that each Commissioner is likely to be subject to intense political pressure within their own jurisdiction if they air views publicly that are not to the government's liking.

One partial approach to dealing with this problem is to give Australia's privacy authorities a collective voice, together with responsibilities defined by statute, including but not limited to, advising both governments and the public. A collective voice helps provide some protection against a privacy official being 'singled out' for unpopular views, but it is not enough. Statutory responsibilities to speak or act are essential, so that privacy officials can say that they could not choose to stay silent or do nothing.

The effectiveness of a collective privacy voice is most clearly seen in the history of the 'Article 29 Working Party' of 28 EU Data Protection Commissioners which from 1995 had statutory responsibilities under the EU's Data Protection Directive, and became the most vocal and most influential 'privacy voice' in the world. Its role has now been taken over, with much expanded responsibilities, by the European Data Protection Board (EDPB) of 27 data protection authorities (plus the EU's own Commissioner), which speaks collectively and independently on issues such as COVID-19. In contrast, one major reason why the 'Asia Pacific Privacy Authorities' (APPA) has done relatively little over a couple of decades is because it has no authority from any external source, such as a treaty, to speak collectively, and certainly no obligation to do so.

In our view, a National Privacy Advisory Council (or 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.[111] 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).

The Act has already gone a considerable distance in requiring greater cooperation between privacy authorities, through provisions such as s. 94V ('Referring COVID data matters to State or Territory privacy authorities') and s. 94W ('Commissioner may share information with State or Territory privacy authorities'). The Commissioners from the various jurisdictions have already established an informal coordinating committee. It would be a logical and valuable step to take this greater cooperation one step further through statutory recognition.

11. Conclusions: Some foundations for trust, with serious deficiencies

The Act is a significant improvement on the Determination that preceded it. The most significant improvements are tightening of the prohibitions against coercion and the inclusion of an individual right of enforcement action before the Privacy Commissioner for most breaches of the COVIDSafe requirements. This is particularly important as a means of stopping attempts to make use of the app *de facto* compulsory. The Act also adds valuable provisions concerning deletion of data, extension of Commonwealth jurisdiction to cover state and territory authorities, and sharing of information between privacy authorities in all jurisdictions. These changes are additional to elements of the Act

[111] As part of the COVIDSafe legislation, s. 6(1) of the *Privacy Act* states '***State or Territory privacy authority*** means a State or Territory authority that has functions to protect the privacy of individuals (whether or not the authority has other functions)'. In Western Australia and South Australia, the Ombudsman or some similar statutory officer could fulfil this role.

which already contributed to trustworthiness: use of the app is voluntary (opt in); uploading contact data is a second stage of voluntariness; and users can opt out from further use of the app, and from future NCSDS storage of their registration data (but not previously loaded contact data).

Nevertheless, there are still many shortcomings in matters which would help justify sufficient public trust for the Australian public to opt in voluntarily to the installation and use of the COVIDSafe app, and then to not opt out. The main deficiencies we identify in this article still are remediable by disclosures and by further amendments: six deficiencies in transparency of how the COVIDSafe system operates and its efficacy; and eleven improvements to the Act. While there are reasons not to give up on attempting to achieve these changes, there is no guarantee that any will be achieved.

Given that the Bill was debated and enacted in a three day Parliamentary sitting, it is not very surprising that no amendments were made to the Bill as introduced. However, that is not the end of the matter, because opportunities for further amendments when Parliament resumes (probably in August) should be pursued, including before two Parliamentary Committees considering the app and the Act.

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, but the extent of privacy protections that have been enacted, and their deficiencies, are now clear.

Overall, our conclusion is that the likely operation of the app, and the provisions of the Act, together provide a sufficient basis for it to be rational to trust what the government is doing, but there are also significant serious deficiencies in both transparency and legislative protections which make a continuation of distrust reasonable. As we say in our concluding paragraphs, it is appropriate that use of the app is voluntary, because reasonable disagreement is inevitable.

We explain the details of these conclusions in the following paragraphs.

11.1. Continuing lack of transparency, and misinformation, detract from trust

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 trust in the COVIDSafe system. A new contributor to this lack of trust is the 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. The Act should provide that independent experts will be provided with access to such information as is necessary for them to make periodic assessments of the extent to which the COVIDSafe system is achieving its objectives, and to make such assessments public. A six-monthly report by the Minister, without even requiring the advice of the CMO, is insufficient.
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 whole COVIDSafe system should be made public. This requires publication of the server-side code and not just that for the two apps, unless the government can provide a convincing explanation as to why this cannot be provided. The government should also promptly announce whether, and if so how, it is addressing technical flaws users and developers have identified in the app.

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 she considers necessary. State and Territory privacy commissioners should be requested by their respective governments (and by Federal Parliament, if possible) 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.
6. The Agreements between the Commonwealth and States/Territories should be made public because they include essential information on the extent of use of surveillance data collected by the COVIDSafe app.

11.2. Legislation needs stronger protections than the Act provides

The COVIDSafe Act has been passed during a three day sitting of Parliament, without the lengthy Committee consideration it would normally receive. Given this haste, the appropriate response is for it now to receive that deliberation, post-enactment, and for an amending Bill to incorporate further improvements. The most important further amendments which should be made to it, in something like their order of importance, are (as explained more fully in this article):

1. The prohibitions against any persons coercing the use of COVIDSafe app, good though they are, need to be made even stronger by closing loopholes. We have recommended additional prohibitions on making the download or use of the app a condition of (i) exemptions from 'stay at home' orders; (ii) discriminatory alternative offers; as well as prohibiting (iii) requirements to disclose or demonstrate whether the app has been downloaded; and (iv) employers installing the app on 'work-owned' phones.
2. The collection of data by the app should be minimised, in line with the recommendations made in the PIA, recommendation 18. It is not sufficient protection simply to contractually oblige State and Territory health officials not to access decrypted data which they have no need to receive in the first place.
3. The Act should require regular automatic deletion of COVID app data from the NCSDS, after a reasonable period allowing for contact tracing, and for periodic independent assessments of the effectiveness of the COVIDSafe system.
4. The conditions for termination of the operation of the app and deletion of all data collected are determined by the Minister based on advice from the Australian Health Protection Principals Committee or the Commonwealth Chief Medical Officer. The federal Priacy Commissioner, or the Australian privacy authorities acting collectively, should be able to request the AHPPC or the CMO to give of such advice. The Act should include an obligation on the Minister to make public any such recommendation from the Committee or the CMO.
5. Methods should be found to ensure deletion of COVID app data held outside the NCSDS by state and territory health authorities.
6. Section 94D should refer to 'access' in addition to 'collection, use or disclosure', particularly since there is a line of case law in which Australian courts have held that 'mere access' or 'mere viewing' is not considered a 'use' of data.
7. 'Proximity' must be defined in legislation, even if the definition is capable of being changed.
8. There should be definitions stating that the controller of both the COVIDSafe app and the 'National COVIDSafe Data Store', is the Department of Health, and that this cannot be changed without a further Act of Parliament.
9. 'COVID app data', 'registration data', and 'information about whether a person has downloaded or installed COVIDSafe' should all be classified as 'sensitive information'.

10. 'COVID app data' should not be declared to be 'property' of the Commonwealth, given that data is not recognised as an object of property rights under Australian law. Copyright or breach of confidence could be utilised instead.
11. A National Privacy Advisory Council should be created to exercise independent oversight and advise both the public and the National Cabinet.

11.3. 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 legislative amendments addressing some or all of the above concerns may eventually be enacted, but for the present, incomplete information and somewhat deficient legislation is the result of the completed Parliamentary process. Individual circumstances may now require decisions whether to install COVIDSafe despite this result. 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 over 100 lives in this country. On the other hand, the numbers of new infections, and of deaths, is at present relatively low, but with no certainty that will continue.

At the same time, many in the media and government, as well as high-profile figures in business and tech, have openly exerted moral pressure in favour of using the COVIDSafe app, even shaming those who don't, characterising them as putting trivial privacy concerns ahead of the interests of the nation. A more balanced approach is required, one that recognises there should be no requirement for Australians to give up more privacy than is necessary and proportionate, and that the need for privacy has even greater immediacy for some, including journalists; victims of stalking and domestic violence; and those out of favour with state powers at home or abroad. Individual decisions about whether to install and run this app are best made after obtaining as much information as can reasonably be obtained and put in the balance. This should not require a binary choice between health and privacy. With the right rules and design, the government can support both.

The position in which Australians are put, of needing to make complex choices based on limited information, does at least have the virtue that serious efforts have been made, via legislation, to ensure that the choice of whether to participate is voluntary, both the choices to opt in and opt out. This allows us to respect the decisions made by others.