Australia's 'COVIDSafe' experiment: A data privacy law for voluntary contact tracing

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

Draft 20 May 2020 for (2020) 165 *Privacy Laws & Business International Report* (3,800 words)

On 12 May 2020, the *Privacy Amendment (Public Health Contact Information) Bill 2020* ('the COVIDSafe Bill')[1] was introduced into the Australian Federal Parliament, and enacted unamended two days later, without the normal Committee deliberations. Two weeks earlier, on 26 April, Australian governments released a coronavirus contact tracing app for public download, marketed as 'COVIDSafe'. By the time the Bill reached Parliament, the app had been downloaded an estimated 5.5 million times, by approximately 25% of Australia's phone-owning population.

This article explains how the Australian contact tracing app works, and how the legislation governing it aims to encourage the public trust that is necessary for a voluntary app to be effective in improving contact tracing. It does not discuss the highly contentious issue of whether a much more decentralised app would be desirable.

How COVIDSafe works

When a person chooses to download the COVIDSafe app, they are able to upload their 'registration data' (name or pseudonym, phone number, age range and postcode) to the National COVIDSafe Data Store (NCSDS), operated for the federal Health Department. Once that data is uploaded, they become a 'COVIDSafe user'. 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 the time of contact is not recorded (GPS technology is not used). Claims by Ministers that the proximity required for recording of contacts is '1.5 metres for 15 minutes' have been misleading. Each contact event is stored on the mobile device for 21 days, then deleted.

Only when the user of one of the communication devices running the app (usually a mobile phone) 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.

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

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 event list that has been uploaded. They can then start the process of contact tracing.

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 applied to COVID app data (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 (IDs are centrally allocated, contact event data may be uploaded to the NCSDS in the event of a positive diagnosis, and the filtering of contact event into proximity event data is done at NCSDS).

An Australian experiment

There are no clearly successful examples of similar voluntary contact tracing apps implemented in any country as yet. Singapore's TraceTogether app (which influenced Australia's app), is reported to have obtained less than 25% take-up two months after its release.[2] Singapore now has a very significant 'second wave' of infections, and there are calls to make the app compulsory. 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), use apps which (variously) are compulsory to use, are used in combination with compulsory access to geolocation information, or are used in combination with compulsory privacy-invasive access to government registers, credit card information, and other contact-revealing data. They are not examples of the success of the COVIDSafe type of app. The voluntariness of the Australian example is therefore an experiment.

Two factors of the Australian context must also be borne in mind. First, Australia is unusual in having no fundamental privacy rights. It has no constitutional rights of privacy which must be complied with if contact tracing systems are introduced, and it is not a party to any enforceable international agreements protecting privacy (such as the *European Convention on Human Rights*, Article 8). 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.[3] Protections of privacy in Australia are essentially creatures of statute, particularly the *Privacy Act 1988* (Cth) (*Privacy Act*), and various state and territory Acts.

Second, an 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

---

[2] Navene Elangovan 'Covid-19: Governance expert says TraceTogether should be mandatory, but warns of potential 'slippery slope' of greater surveillance' *Today* 18 May 2020 https://www.todayonline.com/singapore/covid-19-governance-expert-says-tracetogether-should-be-mandatory-warns-potential-slippery

[3] 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*. Explanatory Memoranda to legislation require a Statement of Compatibility with Human Rights under the *Human Rights (Parliamentary Scrutiny) Act 2011*.

where reliable figures are available.[4] The numbers of new reported infections per day are also very low, with zero cases reported in all Australian states and territories on 11 May, except one cluster of cases in Victoria. This relative success might not be maintained: there may 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 set a very high initial benchmark against which the effectiveness (or lack of effectiveness) of the app must be measured. There are not as yet 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.

Key features of the legislation

The COVIDSafe Act is unusual in the strength of the privacy protections that it provides, but it does have some loopholes and weaknesses, and is not accompanied by sufficient transparency. The main features of the legislation are:

(i) Utilisation of the app is voluntary (opt-in), supported by the ability to opt-out.
(ii) Requiring use of the app, directly or indirectly, is illegal (anti-coercion provisions).
(iii) Individual enforcement of the anti-coercion provisions is provided, through complaints to the Privacy Commissioner.
(iv) The whole COVIDSafe system is to be disbanded, when it is no longer effective, and data collected is to be deleted.
(v) Permitted uses of COVID app data are narrowly defined, and all other uses illegal.

However, this structure has weaknesses: the anti-coercion provisions have some weaknesses; contact event data is collected too broadly, and how it is transformed into 'proximity event data' for tracing use is not defined in law; the law does not require automatic regular deletion of contact data from the national data store after any fixed period; and there is no provision for independent periodic assessments of the effectiveness of the COVIDSafe system or even objective criteria laid down for the government to report on its effectiveness.

We have published a detailed critique of the legislation, and of its transparency deficiencies,[5] where the statutory and other references supporting this summary paper may be found.

Voluntary use

The positive starting point of the COVIDSafe Act is that there are at least five ways in which use of the app (and inclusion in the NCSDS system) is voluntary, not compulsory: (i) downloading the app is voluntary (as is uploading 'registration data' to the NCSDS); (ii) the COVIDSafe user can enable or disable the operation of the app from time to time using their device settings, operation is not automatic; (iii) a person tested positive for coronavirus, who is running the app, must consent (again) 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 thus opt-out from future data collection); and (v) users can require their registration data to be deleted from the NCSDS (but not any contact logs they have already uploaded).

---

[4] 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.

[5] G. Greenleaf, and K. Kemp 'Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing' (May 15, 2020). (2020) University of New South Wales Law Research Series. https://ssrn.com/abstract=3601730

Restrictions on use of COVID app data

It is an offence for any person (including governments) to collect, use or disclose COVID app data (registration data and contact logs), punishable by imprisonment for 5 years or AUD $63,000 or both (s. 94D). The only exceptions to this general prohibition are collections, uses or disclosures insofar as they are for these purposes:

- For contact tracing by employees/contractors of a state or territory health authority (Australia's federal government does not have this role);
- By the NCSDS administrator to ensure the NCSDS functions properly to enabling this contact tracing;
- By the NCSDS administrator to produce de-identified statistical information about the total number of registrations through COVIDSafe (but only these statistics);
- To transfer encrypted COVID app data between devices of users, or between a user and the NCSDS;
- By the Privacy Commissioner performing functions or exercising powers under Part VIIIA;
- By Police authorities investigating or prosecuting contraventions of Part VIIIA; or
- By the NCSDS administrator to confirm that the correct registration data is being deleted at a user's request.

This is an extremely limited set of permissible uses. There are other restrictions in relation to COVID app data. It is an offence for anyone to decrypt it. NCSDS data cannot be held on a database located outside Australia, or disclosed to anyone outside Australia.

There is an ongoing dispute concerning whether storage on an Amazon Web Services (AWS) server located in Canberra places the data at undue risk of access required under the US CLOUD Act.

Part VIIIA (the COVIDSafe Act) overrides other laws

Reinforcing these restrictions, 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 (including under s. 94D, as above). It also 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,[6] of which there are many.

The only exception to this cancellation is that it 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.

Anti-coercion offences

Misuse of COVID app data is not the only risk. Australian governments have already been advertising downloading of the app as 'the quickest way that Australian life can get back to normal', or words to that effect. There is a considerable danger that employers will insist that

[6] 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.

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. State and Territory regulations that require people to have 'a reasonable excuse'[7] for some outdoor activities could be changed to make it necessary to have the app installed in order to comply. Those who don't like it could be told they can stay home. The use of the app would not be 'voluntary' under these circumstances of 'pseudo-voluntary' compliance.

The Australian federal government recognised this issue from the outset. It addresses it in section 94H, 'Requiring the use of COVIDSafe', which provides that a person commits an offence (with the penalties abovementioned) if they require another person to download the app, or have it in operation, or consent to upload data to the NCSDC (s. 94H(1)). This otherwise comprehensive provision needs to have added 'disclose or demonstrate that they have done any' of these three things. Requiring disclosure opens up the potential for discrimination.

Section 94H(2) provides another set of offences, wherever a person is required to do any of the three compliance steps listed in section 94H(1), failing which the other person:

(a) refuses to enter into, or continue, a contract (including of employment) with them;
(b) takes 'adverse action' (within the meaning of the *Fair Work Act 2009*) against them;
(c) refuses to allow them to enter premises that are otherwise accessible to the public; or premises that they have a right to enter;
(d) refuses to allow another person to participate in an activity;
(e) refuses to receive goods or services from them, or insists on paying less for them; or
(f) refuses to provide goods or services to them, or insists on receiving more monetary consideration for them.

These prohibitions against direct or indirect coercion are already very broad, particularly the reference to 'activity' in (d). Examples under (e) and (f) 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.

However, there are still loopholes which need closing. Discriminatory conditions need to be prevented, such as seating all those who do not have the app installed in a segregated area, or requiring abnormal provision of identity details. Other problems may arise for those who have employer-owned phones on which the app is pre-installed in their name or the employer's name. If the app is already running, the employee is not required to do anything, but their interactions would be tracked.

Individual enforcement provisions

The criminal penalties for breaches of Division 2 of Part VIIIA are very desirable, but 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 would be sporadic, if it ever occurs.

To overcome this, we argued that the COVIDSafe Act needed to provide remedies that individuals affected by breaches of the law can initiate for their own protection, and to obtain

[7] 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

compensation for harms or injunctive relief.[8] This approach has been taken, and is one of the Act's 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' of the *Privacy Act*, and thus gives rise to a right to complain to the Privacy Commissioner under section 36 (s. 94R). This also applies to breaches of both Division 2 and Division 3, so is comprehensive of all obligations in Part VIIIA, and there are no exemptions. Similarly, there is a right to complain to the Privacy Commissioner in relation to any data breaches (and resulting obligations to give data breach notifications) concerning COVID app data, applying to both the NCSDS administrator and state or territory health authorities (s. 94S).

It is a defect in Australia's Privacy Act that individuals cannot go directly to the courts to take actions for breaches, and this general problem has not been resolved by this Act.

De-commissioning of the COVIDSafe system

Privacy advocates argue, with many precedents on their side, that surveillance systems introduced for 'temporary' or 'emergency' purposes always end up being permanent. The COVIDSafe Act provides a number of means by which individuals can disengage from its surveillance. First, data on an app user's 'contact events' are deleted from their mobile after 21 days. An app user can delete the app from their device at any time, and the NCSDS administrator must not from that point collect any contact event data from their device (s. 94N). However, deletion of the app does not result in user data being removed from the NCSDS. The user can request that their registration data be removed from the NCSDS (s. 94L), but there is no provision for requests to be made to remove any contact event data they have previously uploaded to the NCSDS (because of a COVID19 diagnosis). Nor can they request removal of any references to their IDs in the contact logs uploaded by other users.

There are no provisions for periodic purging of contact logs from the NCSDS once their practical utility (for contact tracing or statistical reporting) has expired. This is a deficiency, because we have no way of telling how long the pandemic will last and NCSDS will operate, so a large body of sensitive data may accumulate and not be deleted after its utility has expired.

In the absence of a request from a user to delete their registration data under section 94L, the user's registration data will also be kept in the NCSDS until 'the end of the COVIDSafe data period', at which point the NCSDS administrator must delete all COVID app data from the NCSDS, and inform all COVIDSafe users (s. 94P). The Health Minister must determine the 'end' 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). The Minister must not make this determination unless s/he has 'consulted, or considered recommendations from, the Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee' of all such CMOs. One flaw is that unless the medical experts volunteer this advice, there is no way to require the Minister to ask for it: so COVIDSafe and the NCSDS could go on for an unnecessarily long time, perhaps indefinitely. Further flaws, just as serious, are that no objective measure of the effectiveness of the app is specified, and the CMOs are not independent and unbiased. They have 'skin in the game' as some of the main promoters of uploading of the app.

[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>

Operational issues with COVIDSafe data minimisation

Despite the Act appearing to deal comprehensively with the COVIDSafe system, there are obscure aspects of its operation. As explained under 'How COVIDSafe works', the app collects details of every 'contact event' that occurs within the variable 'Bluetooth range' of another device with the app. It is only when data is uploaded to the NCSDS by a user with a positive COVID19 diagnosis that 'contact events' may be filtered in some way to produce 'proximity events' (which are popularly understood as '1.5 metres for 15 minutes'). But the measure of proximity is not defined in the Act. It may be found in the server-side source code, but this has not been made public, or it may be in the agreements the Commonwealth has reached with each of the States and Territories, but these are not public either. Transparency is undesirably low.

Conclusions: Results from an experiment

There are many identifiable deficiencies with this legislation, and with the transparency of the operation of the app.[9] Many will also argue that a more centralised tracing system like this presents unnecessary risks compared with a radically decentralised system. Some governments, and others, will argue in return that a system like COVIDSafe is more likely to be effective. 'Effectiveness' is a matter of guesswork at this stage, but it needs to be measured by objective and unbiased means, otherwise the experiment will not have an honest result. The Australian governments have also taken a gamble (another experiment) that they can win sufficient public confidence in the app that the number of downloads will be high enough to make it work. For this reason, the COVIDSafe Act contains stronger privacy protections than previous examples of Australian data privacy legislation, and may be of interest as a model (somewhat flawed) for other countries that want to take a similar approach.

[9] See Greenleaf and Kemp 'Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing', Part 11, for six deficiencies in transparency, and eleven aspects of the Act that need improvement.