Good legislation to make COVIDSafe trustworthy

These suggestions for drafting of good legislation to maximising uptake of the COVIDSafe app and ensuring success of COVIDSafe enabled contact tracing are made by the following data privacy professionals and academics:

Malcolm Crompton, Founder and Lead Privacy Adviser, Information Integrity Solutions, Privacy Commissioner of Australia 1999 - 2004

Anna Johnston, Principal, Salinger Privacy

Peter Leonard, Principal, Data Synergies; Professor of Practice (IT Systems and Management and Business Law), UNSW Business School; Consultant, Gilbert + Tobin Lawyers

Melanie Marks, Principal, elevenM; Advisory Board Member, International Association of Privacy Professionals

Rob Nicholls, Associate Professor, UNSW Business School; Director, UNSW Business School Cybersecurity and Data Governance Research Network

Nicole Stephensen, Principal, Ground Up Consulting and Executive Director (Privacy and Data Protection), Internet of Things Security Institute

Kimberlee Weatherall, Professor, The University of Sydney Law School

Why we are making these suggestions

Australian governments need to work together in order to address concerns of a significant number of citizens and persuade them to uptake the COVIDSafe app.

The protections written into the Determination are a good start. However, additional protections are necessary in order to build trust of Australian citizens to lift COVIDSafe app take-up to critical mass and ensure reliable and continuous use of the COVIDSafe app.

Nurturing digital trust of the segment of Australian citizens that remain reticent to take up the COVIDSafe app requires unprecedented cooperation and coordination by Australian government.

COVIDSafe app data (including associated metadata) potentially tells a revealing story of what each citizen using the app does, where and whenever they do it, and with whom.

To achieve critical mass in take-up (and in reliable use by most users without some users electing to ‘go dark’ from time to time), there must be only one conclusion reasonably open to Australian citizens: namely, that the COVIDSafe app is safe for all citizens to use for its stated purpose of contact tracing to control COVID-19.

All citizens need to know that they should make their decision to download and keep the COVIDSafe app active at all times free from any concern that COVIDSafe app data may flow out of the contact tracing system, anywhere.

Specifically, citizens must have legislated assurance, not just statements of reassurance, that COVIDSafe app data (including associated metadata) throughout the data lifecycle will not be potentially available to other government agencies, law enforcement agencies, security organisations, etc., or courts issuing subpoena and other legal process.

Citizens considering whether to self-report that they are COVID-19 positive should have no reason or incentive to pause and consider whether they wish to expose to scrutiny by Government agencies or other authorities or courts whatever they may have been doing, where and with whom.

Any citizen engaging in private activities, whether just personal and confidential or more dubious, including vulnerable and at-risk individuals concerned that others may find them, should have no incentive to consider 'going dark' and deactivating the app or turning off their mobile phone.

All citizens should know one fact that is clear and incontestable: COVIDSafe app data will only ever be made available for use for the one and only purpose for which citizens are asked to consent, that is, to enable contact tracing by a State or Territory contact tracing agency if a COVIDSafe 19 app user elects to report positive for COVID-19.

Achievement of this objective has been delegated by Australian governments to the Commonwealth Department of Health.

The Department stated the purpose of the COVIDSafe app to Australian citizens when seeking their informed consent.

The Department of Health's responsibilities should therefore include managing the shared risk[1] that other departments and agencies to whom the Department of Health entrusts COVIDSafe app data (and associated metadata) may not safely and securely manage that data.

[1] Shared risk was recently defined by the Dept of Finance as follows: "A shared risk extends beyond a single entity. It is a risk that emerges from a single source and impacts interrelated objectives of entities. A collaborative approach to managing shared risk is required to: identify accountability, nominate transparent roles and responsibilities, define risk appetite boundaries and seek agreement between all parties.": Department of Finance, Understanding and Managing Shared Risk, https://www.finance.gov.au/sites/default/files/2019-11/comcover-information-sheet-understanding-and-managing-shared-risk.pdf. The ANAO report on implementation of My Health Record applied this concept in evaluating responsibility for managing My Health Records data: see ANAO, Implementation of the My Health Record System: Australian Digital Health Agency and Department of Health, available at https://www.anao.gov.au/work/performance-audit/implementation-the-my-health-record-system. See further Office of the Australian information Commissioner, Privacy management framework: enabling compliance and encouraging good practice, available at https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice/, and paragraph 6.5 of the PIA for CovidSafe.

There is therefore a simple and clear purpose for COVIDSafe, as has already been stated to Australian citizens when seeking their fully informed consent, and a simple objective for Australian governments: make COVIDSafe safe for all at all times because COVIDSafe app data (including metadata) is locked-down.

Australian governments need to come together to ensure they achieve that objective through demonstrated good implementation.

Although the purpose and objective are clear and simple, giving effect to them requires unprecedented action.

State and Territory agencies are generally not regulated by the Privacy Act 1988 (Cth).

Some States and Territories do not have data privacy statutes.

“Agreement from States and Territories to ensure that information they receive will not be used for any other purpose than contact tracing” is not an adequate safeguard.

The national enabling legislation for COVIDSafe needs to expressly cover all relevant agencies, regardless of whether those agencies are:

- entities regulated by the Privacy Act 1988 (Cth),
- entities regulated by State and Territory data privacy or health data privacy statutes,
- regulated only by their own enabling statutes or not subject to any current data privacy statute.

There is a risk that any gaps in coverage of data privacy regulation to regulate all agencies in the national COVIDSafe data ecosystem might be seen by some civil society organisations and parts of the Australian community as leaving a ‘backdoor of vulnerability’ to data leakage or misuse, or other use that is contrary to the interests of the COVIDSafe app user.

Providing assurance to the critical segment of Australian citizens that remain reticent to take-up the COVIDSafe app requires passage of a Commonwealth statute that, within the time limited window of the COVID-19 emergency, governs activities of all Federal, State and Territory departments and agencies that are involved in handling of COVIDSafe app data, as that data passes through and is transformed end-to-end within the COVIDSafe app data (including metadata) ecosystem.

This data ecosystem starts on a citizen’s smartphone, involves each department and agency in the chain, and potentially ends at a contact tracer’s file in a State or Territory contact tracing agency.

The purpose and objective can only be urgently given effect by a Commonwealth statute.

The Commonwealth stature must regulate all handling of COVIDSafe app data within the COVIDSafe app data ecosystem, regardless of whether the handling agency is a Federal, State or Territory agency.

No Commonwealth law that 'covers the field' in this way has ever been more urgently required.

No Commonwealth law has ever been passed on the basis of such urgency, or with an objective of persuading most Australians to voluntarily give up their individual right of freedom from surveillance.

The required levels of digital trust across a broad and diverse community, that COVIDSafe will only be used in control and management of COVID-19, cannot be built only upon statements of good intent and pointing to legislated constraints.

Reassurance of good intent and legislated constraints are necessary but insufficient steps to demonstrate safe and secure management of COVIDSafe app data by all agencies operating within the COVIDSafe app data ecosystem.

Assurance to build citizen trust requires full separation of COVIDSafe app data (and related metadata) from all other operations of Governments and their departments and agencies, including law enforcement agencies, security organisations, commissions and statutory authorities, and courts issuing subpoena and other legal process.

The government agencies and instrumentalities that are precluded from accessing COVIDSafe app data (and related metadata) must include all other Federal, State or Territory agencies and instrumentalities including law enforcement agencies, security organisations, commissions and statutory authorities, and courts issuing subpoena and other legal process.

Providing assurance to the critical segment of Australian citizens also requires the Commonwealth law to:

- mandate functional separation of the operation of handling COVIDSafe app data in each department and agency from all other operations, activities and responsibilities of that department or agency, and
- mandate accountability of each department and agency to ensure that these controls and safeguards will be implemented and will reliably work,
- empower a properly resourced oversight authority that is independent of each department and agency to verify that these controls and safeguards are working and publish reports that provide this assurance.

Legislating-in additional protections will provide assurance to the critical segment of Australian citizens that are reticent to take up the COVIDSafe app, and the civil society organisations that inform the views of these citizens, that:

- controls and safeguards will be reliably implemented by all Federal, State and Territory agencies that will have access to COVIDSafe app data, and
- this reliable implementation across Australia will be overseen and will be verified by an appropriate independent oversight authority.

The clear and simple purpose for which citizens are asked to consent, being to enable contact tracing by a State or Territory contact tracing agency if a COVIDSafe 19 app user elects to report positive for COVID-19, can be entirely fulfilled without sacrificing reasonable, appropriate and proportionate privacy and security controls and safeguards.

Legislating-in additional protections can be done without delaying drafting and introduction for passage of the Commonwealth legislation.

Implementation of functional separation and technical, operational and legal controls and safeguards is not a process which is novel or unchartered or which will be cumbersome, slow, contentious or expensive. The Australian Privacy Commissioner has well established and documented data privacy management frameworks and deidentified guidelines which will assist rapid implementation. The Office of the Interim National Data Commissioner has relevant knowledge and expertise. Specialist data analytics service providers in the business sector already stand up complex technical data linkage environments, and implement associated operational and legal controls and safeguards, within a matter of days.

Our specific suggestions for additional protections follow.

1. Definition of COVIDSafe app data and new clarity as to prohibitions on disclosure

A new definition of COVIDSafe app data should make it clear that data that originates as COVIDSafe app data:

- includes all associated metadata, and
- retains its character as COVIDSafe app data through transformations (e.g. by linking to other data) from first capture on a citizen's smartphone through each department and agency in the chain potentially ending at a contact tracer's file in a State or Territory contact tracing agency.

The only exception should be reliably and pervasively deidentified data.

2. Deidentified data

The definition of "de-identified" data, as taken from the Privacy Act 1988, has been rightly criticised as leaving open the question of whether data is reliably and pervasively deidentified in the hands of any entity and all entities that may at any time have access to the relevant data, taking into account all other data that this entity may access.

Reidentification (that is, loss of deidentification) may be through mosaic effects or other data recombination, so it is important to expressly reference this possibility.

There is a real risk that some civil society organisations may see any ambiguity as to deidentification as a possible 'backdoor'.

This is not a debate which should be left open at a time when citizen trust as to legislated safeguards is critical to achieve high uptake of the COVIDSafe app.

It should be made clear that the only purpose for which deidentified data may be used is aggregations that enable statistical aggregated analytics to generate insights as to activations, periods of use and unavailability, and like analytics which assist government efforts to promote effective take-up and use of the COVIDSafe app.

3. Functional separation and organisational accountability

The Determination does not recognise the key role that functional separation and organisational accountability should play in building trust of citizens as to how (derived) COVIDSafe app data (including metadata) is handled (and might be accidentally mishandled).

For example, there is left open a legal question as to whether (derived) COVIDSafe app data is 'disclosed' if it can be viewed within an agency by any individual within an agency where that individual is not someone who is directly involved in the handling of that data and who requires access to that data on a need to know basis.

There should be no room left for debate as to whether appropriate technical, operational and legal controls and safeguards (developed applying the Five Safes Framework, as adopted by the Interim National Data Commission team in development of the draft Federal data sharing bill) will be applied within each agency handling (derived) COVIDSafe app data, so that functional separation within each agency is demonstrably ensured through reliable and verifiable processes, practices and procedures.

Each Commonwealth, State and Territory department and agency that handles derived COVIDSafe app data should be required to design, implement and maintain technical, operational and legal controls and safeguards as reasonable and appropriate to ensure safe and secure handling of COVIDSafe app data reliably and verifiably separated from other activities and functions of that department or agency.

Either the Office of the Interim National Data Commissioner, or the Australian Privacy Commissioner and/or State and Territory Privacy Commissioners, or both, should be empowered to consult with each agency, and each agency should be required to consult with either or both Commissioners, in design and implementation of such controls and safeguards.

4. Encryption

Electronic derived COVIDSafe app data should be required to be encrypted both in transit and at rest.

This is particularly important given outsourcing of data warehousing.

5. Reporting and independent oversight

Empowered, effective and real-time independent oversight and verification, and prompt and public reporting as to oversight and verification is an important plank in nurturing trust.

Independence requires the oversight authority to have clear separation from executive government and like powers to a Commissioner, Ombudsman, or the Independent National Security Monitor.

It is a choice for the Parliament as to which independent body should be empowered to oversight practical implementation of this legalisation and the operation of the national COVIDSafe app data ecosystem.

It should not be a question whether effective and empowered independent oversight is necessary or desirable.

6. Sunset at the end of the pandemic

The COVID-19 pandemic will definitely end. So should the need for, and operation of, this unusual legislation.

The statute should have a set sunset date on which the statute ends.

The statute should also be stated to end earlier if the pandemic bioemergency is declared by Australian governments to be over.

There could be a power for extension by determination for an additional period if contact tracing continues to be reasonably necessary to address a tail of COVID-19 cases and the Minister determines that the COVIDSafe app continues to be of substantial benefit in assisting contact tracing of this tail of COVID-19 cases.

Of course, all COVIDSafe app data (and associated metadata and records in any form of that data and metadata) should then be required to be deleted, the app taken down, and secondary uses of deidentified COVIDSafe app data should then crease to be permitted.

And also of course, 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.

1 May 2020