COUNCILS FOR CIVIL LIBERTIES PUBLIC STATEMENT

PARLIAMENT MUST STRENGTHEN PROTECTIONS IN COVID APP BILL

9 May 2020

The Australian Government has released the *Privacy Amendment (Public Health Contact Information) Bill 2020 (COVIDSafe Bill)* which will be considered by Parliament next week. The COVIDSafe Bill largely reproduces the biosecurity orders which made it possible to begin to download and operate the COVIDSafe App (*App)*.

The NSW, Queensland and South Australian Councils for Civil Liberties support the introduction of effective digital contact tracing if it has robust privacy and transparency legislation underpinning it.

The stated object of this Bill is to provide stronger privacy protections for the collected data to encourage public acceptance and uptake of the App and to enable faster and more effective contact tracing. (s94B)

Unless the legislation provides Australians with certainty that their legitimate privacy and data security concerns have been fully addressed, it is not likely the Government will achieve the needed take-up level for effective tracking.

It is our hope the Government will use this crisis context to set a new high standard in privacy rights in Australia.

Numbers of the community's privacy and data security concerns have been addressed in the bio-security order and in this Bill. For example, we support s94H which protects persons against being coerced into using the App by making such coercion an offence. This protection is broad based but is particularly important in relation to workers returning to employment and young people to schools.

There are however outstanding issues the Government should address before this Bill is passed.

Major issues

There is no express provision ensuring that the use of the App is voluntary. Also, while it is specified as 'opt-in', there is no provision which prohibits a switch to an 'opt-out' option if there is insufficient uptake - as was tried with **My Health Record**.

More needs to be done to ensure that the App does not compromise data protection and thereby increase the risk of illegal and inappropriate use of data or surveillance of Australians.

We welcomed the Government's decision to commission a Privacy Impact Statement but it is disappointing that its scope was limited to compliance with the Privacy Act 1988 and the privacy principles, rather than a wide-ranging review of the most appropriate options for this particular context.

It is also disappointing that the Government has opted for centralized data storage in a new National COVIDSafe Data Store rather than adopting the widely supported and more privacy-friendly decentralised option .

The COVIDSafe Data Store will hold registration information, encrypted information from users' devices and sensitive information about a user's positive COVID-19 infection status.

Cyber-attacks and accidental and illegal data breaches will continue to occur on Australian Government databases. This storage choice creates a real risk of such breaches and will undermine users' confidence as to the safety of their private data.

Mobile device contact tracing can be decentralized, with contacts registered in encrypted form on the local mobile device, and not identifiable to others or the government. Such measures reduce the fallout should a data breach occur. The Government should reassess its decision on this aspect.

Apart from the content of the Bill we have concerns about aspects of the Government's information campaign which has included misleading advertising and spruiking of the App. This is not appropriate when informed consent relies on the provision of clear, accurate and relevant information – including information as to risks as well as benefits.

More openness as to potential problems with the App might have allowed Australians to be less perturbed by the technological flaws that immediately emerged - most seriously with the iPhone Bluetooth operation [1]- or the fact that contact tracing is not actually functional until the States and Territories get onboard.[2]

If an individual registers COVID-19 positive status, that information is sent to the National Database and then on to State health agencies to notify the individual's contacts. The COVIDSafe Bill applies to State and Territory health authorities in relation to the COVID app data (s94X). There is some uncertainty as to achievement of the application of the COVIDSafe Bill in every jurisdiction. The Australian government needs to do everything necessary to ensure this is achieved as the States will be handling the bulk of the unencrypted information.

Australians' greater freedom of movement should not be predicated on the downloading of the App, particularly given that the COVIDSafe Privacy Policy states that no user should feel pressured to install or continue to use it. Contrary to at least some people's understanding, COVIDSafe does not confer protection from COVID-19 on the individual user.

Recommendations

We recommend that the following issues should be considered by Parliament for incorporation into the Bill – or for Government action - to more adequately protect the privacy of Australian citizens who have voluntarily participated in this tracking exercise for the public good.

i) The legislation must have a defined end date. The Bill states this will be 90 days after the Minister determines a day from which he is satisfied that the App is no longer required or effective (s94Y). This means that the date for ending use of the App relies on the subjective belief of the Health Minister.

[1] Rollins, A (5 May 2020) Coronavirus: federal government faces criticism over bugs and flaws in COVIDSafe app *Canberra Times* https://www.canberratimes.com.au/story/6745024/govt-under-pressure-over-app-bugs-and-flaws/

[2] Taylor, J. (5 May 2020) COVIDSafe app: how Australia's coronavirus contact tracing app works, what it does, downloads and problems *The Guardian* <https://www.theguardian.com/australia-news/2020/may/05/covid-safe-app-downloads-ios-android-iphone-australian-government-covidsafe-tracking-how-to-download-install-works-working-problems-australia-coronavirus-contact-tracing>

Given the sensitivity in relation to the App this decision should be made by the parliament. The legislation should specify that parliament will review the necessity for the continuation of the Act no later than 6 months after its commencement and, if renewed, at 6 monthly intervals.

ii) The legislation must mandate voluntary adoption of the App and exclude a future move to an opt-out mode if there is insufficient take up.

iii) The Bill provides that application must be made to the Australian Government to have data on the National Database removed. This does not apply to that user's data collected from the devices of others (s94L).

The legislation must specify all data, including that held by States and Territories and any transformation of data, should be deleted when the user decides that they do not wish to use that App any more.

There should be specified time limits on the destruction of that information, not just "as soon as practicable".

iv) There must be explicit restriction of access by law enforcement, including the national intelligence services, other government agencies and State and Territory government agencies (other than the health agencies permitted).

It follows that there must be no ability to subpoena data through court proceedings or obtain a warrant to gain access to the data.

The previously introduced encryption laws give the intelligence services access to information on a person's phone and this alternative authorization of access must be prohibited.

v) Further to iv): there is doubt as to whether the protections in the *Biosecurity Act 2015* are sufficient to prevent App data from being accessed by US law enforcement agencies via the US CLOUD Act. Although, the data will remain in Australia, it is held by US-based company Amazon Web Services, which can be compelled to provide that data to US law enforcement unless Australia is designated a qualifying foreign government.[3]

vi) The COVIDSafe Bill is limited to contact tracing. The legislation should specify that there must be no secondary use of, or disclosure of the data. Personal data should not be retained for any new purpose.

vii) Collection of incidental COVIDapp data is not an offence (94D(3)). It should, therefore, not be available to other agencies, used in any other proceedings and should be destroyed when collected, not just when the person affected becomes aware of its collection.

[3] Pauline Wright, Law Council in Welch, D & Besser, L. (28 April 2020) Experts warn there are still legal ways the US could obtain COVIDSafe data *ABC NEWS* <https://www.abc.net.au/news/2020-04-28/covidsafe-tracing-app-data-may-not-be-protected-from-usa/12189372>

viii) The COVIDSafe Bill includes an independent oversight role for the Office of the Australian Information Commissioner to conduct assessment of the system and investigate complaints (ss94T, 94U, 94V). The OAIC and State and Territory Commissioners should also be required to provide regular public reporting of data collected by the technology, including how de-identified research data is being used, and be well resourced to cope with the increased workload.

ix) There may be constitutional difficulties with proposed section 94X in so far as it relates to the States. The need for complementary state/territory legislation should be investigated.

x) Further, both the Commonwealth and State Privacy Commissioners should be authorised to conduct on the spot audits, without notice, of the use and safety of the data.

xi) Ideally there should be independent judicial oversight of the COVIDSafe legislation and an obligation by that body and the Privacy Commissioners to report to Parliament on COVIDSafe operations.

xii) The definition of *COVID App Data* excludes information that is de-identified. Given that it is in fact relatively easy to de-anonymize data, this exclusion should be removed.

xiii) There should be no delegation of the primary legislation enacted and no ministerial discretion, particularly relating to the sunset period.

xiv) There must be informed consent by users of the App which means the Government must provide accurate and complete information about its use and its effectiveness, risks and limitations set out in a short and clear privacy policy and updated as necessary.

Contacts:

NSW Council for Civil Liberties: Michelle Falstein email: michelle.Falstein@nswccl.org.au; mob: 0412980540
Queensland Council for Civil Liberties: Michael Cope mob: 0432847154
SA Council for Civil Liberties: Claire O'Connor mob: 0434103394