UNSW SYDNEY

THE ALLENS HUB
FOR TECHNOLOGY, LAW & INNOVATION

Australian Human Rights Institute

13 May 2020

Senator Katy Gallagher
Senate Select Committee on COVID-19
By email: covid.sen@aph.gov.au

Dear Senator Gallagher,

Privacy Amendment (Public Health Contact Information) Bill 2020

1. We write to you in relation to the *Privacy Amendment (Public Health Contact Information) Bill 2020*. The draft Bill, amending the *Privacy Act 1988* (Cth), sets out the conditions for operation of the COVIDSafe app scheme which the Commonwealth government has introduced. In this submission we set out our concerns about the extent of the privacy protections contained in the draft Bill. Our specific recommendations for amendments to the draft Bill to improve its compliance with human rights are set out at page 4 of this letter.

Compatibility of the COVID-19 app and scheme with the right to privacy: the availability of less restrictive alternatives

2. The introduction of the COVIDSafe app gives rise to issues of compatibility with the right to privacy contained in Article 17 of the International Covenant on Civil and Political Rights. Where the government urges the population to adopt technology (here, the COVIDSafe app) in response to a public health emergency, it is important to consider the impact on human rights. In this case, the relevant right is the right to privacy. The right to privacy is 'the right not to have one's privacy, family and home life or correspondence unlawfully or arbitrarily interfered with'.[1] It includes informational privacy, which requires effective measures 'to ensure unauthorised persons are not able to access personal information'.[2] Here, we are particularly concerned with the need to 'adopt legislative and other measures to protect people from arbitrary interference with their privacy' when using the COVIDSafe app.[3]

3. The right to privacy is addressed in the Explanatory Memorandum. The only question here is whether the rollout of COVIDSafe is proportionate to the legitimate objective to protect public health, given the relevant legal regime set out in the Bill.

---

[1] Parliamentary Joint Committee on Human Rights, *Guide to Human Rights* (June 2015) 1.108.
[2] Ibid 1.112-113.
[3] Ibid 1.110.

Within proportionality, the primary questions are whether there are ways to achieve the same aim with less impact on the right to privacy and whether the safeguards provided are effective.

4. We recognise that the COVIDSafe app scheme pursues a legitimate objective (the protection of public health and individuals' rights to health) and that the government has taken steps to provide significant privacy protections. However, we consider that its impact on the right to privacy of individuals is potentially greater than is required to achieve the purposes of the scheme. There are less intrusive alternatives which would provide more extensive protections, are practicable and will not impede the achievement of the overall goals of the scheme.

5. Issues surrounding the efficacy of the COVIDSafe app to function as proposed due to the technical difficulties of Bluetooth running as a background application may also have a bearing upon the proportionality of the response. iPhones are primarily affected and 'account for more than half the smartphones in Australia'.[4]

6. There are a range of practicable changes that would involve less intrusive measures and greater oversight and other protections that would still enable the government to attain the legitimate objective of protecting public health: these are set out in the attached table. The government should also be more transparent about the scheme. Following our recommendations may well encourage more Australians to download the app, thus increasing its chances of success.

Conclusion

7. We urge the government to ensure that the Bill is amended in the ways set out in the attached table.

8. We would be happy to provide further information if that were helpful. Please contact Lyria Bennett Moses at

[4] Max Koslowski, 'COVIDSafe downloads reach 5 million as experts question technical flaws', Sydney Morning Herald (online) 5 May 2020 <https://www.smh.com.au/politics/federal/covidsafe-downloads-reach-5-million-as-experts-question-technical-flaws-20200505-p54q2n.html>; see also Digital Transformation Agency evidence to the Senate Select Committee on Covid-19, 6 May 2020.

Yours sincerely,

Professor Lyria Bennett Moses, Ms Genna Churches, Dr Monika Zalnieriute
Allens Hub for Technology, Law and Innovation
UNSW Sydney

Professor Andrew Byrnes
Australian Human Rights Institute
UNSW Sydney

Professor Jackie Leach Scully
Disability Innovation Institute
UNSW Sydney

Dr Katharine Kemp
Lead, Grand Challenge on Trust
UNSW Sydney

Professor Graham Greenleaf
Faculty of Law
UNSW Sydney

CHANGES RECOMMENDED TO THE
PRIVACY AMENDMENT (PUBLIC HEALTH CONTACT INFORMATION) BILL 2020

Recommendation	**Explanation**
A simple amendment should be made to cl 94L(4) to correct an apparent oversight and ensure promised privacy protections are provided. Clause 94L(4) is an exception to the general obligation to delete registration data on the request of a COVIDSafe user. The current wording: 'This section does not apply to data that is de-identified.' should be replaced with: '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.'	The government has emphasised that it only intends that COVID app data should be de-identified for the narrow purpose described in cl 94D(2)(f). For this reason, the government amended the definition of 'COVID app data' in the draft Bill to clarify that the only de-identified data excluded from the definition of 'COVID app data' 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.' For the same reason, the exclusion of de-identified data from the general obligation to delete 'registration data' (which is part of the 'COVID app data') on request should be limited with the same wording.
States and territories should be encouraged to pass corresponding legislation	Although the Bill states that it applies to State and Territory health authorities (cl 94X), it would be preferable for equivalent provisions to be contained in state and territory law, particularly since (1) the application is limited to COVID app data, which is narrowly defined; and (2) cl 94X cannot directly override conflicting state and territory legislation. Agreements with the Commonwealth should not be used to determine the application of the *Privacy Amendment (Public Health Contact Information) Bill 2020*. Instead, legislation should be enacted. This is particularly relevant were States such as NSW have made Orders which broaden the existing data sharing

	capabilities of departments, increasing the likelihood of data sharing beyond the confines of the *Privacy Amendment (Public Health Contact Information) Bill 2020*.[5]
The following should be made publicly available:[6] - Source code for the National COVIDSafe data store; - Advice referred to in the Explanatory Statement for the Determination from the Digital Transformation Agency, the Acting Secretary of the Health Department and the Commonwealth Chief Medical Officer. - Evaluations of the COVIDSafe app over time. - Clear statements as to the data collected by the app (which, contrary to some statements to date, is not limited to information about users who come within 1.5 metres for at least 15 minutes). The federal Privacy Commissioner should be requested to state and justify an opinion on whether the COVIDSafe app and its operation is a necessary and	This will enhance transparency and allow the public to evaluate the security, effectiveness, necessity and proportionality of the app. Current Bluetooth technology does not have the precision to only collect information of those phones within 1.5m, meaning that a broader range of contact, including those in separate rooms or even apartments, may be collected.[7] Signal strength can be influenced by a number of factors, some of which are unrelated to distance, making it difficult to distinguish a close contact from other contacts.[8] The effectiveness of the app is likely to depend on technical issues (some of which have been identified), the role of the app in Australia's overall COVID-19 response, and assumptions about the natural history of COVID-19.

[5] *Public Health Act 2010 (NSW)*, Public Health (COVID-19 Restrictions on Gathering and Movement) Order 2020 amended 9 May 2020 Part 6.
[6] Graham Greenleaf and Katharine Kemp, Australia's 'COVIDSafe App': An Experiment in Surveillance, Trust and Law (April 30, 2020). (2020) University of New South Wales Law Research Series 999. Available at SSRN: https://ssrn.com/abstract=3589317.
[7] Ariel Bogle and Olivia Willis, 'Can Australia's coronavirus contact tracing app COVIDSafe lift the country out of lockdown?' ABC News (online) 6 May 2020 <https://www.abc.net.au/news/science/2020-05-06/coronavirus-contact-tracing-app-covid-safe-lockdown-lift/12217146>.
[8] Sam Biddle, 'The inventors of Bluetooth say there could be problems using their tech for coronavirus tracing', The Intercept, 5 May 2020 <https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing/>

proportionate response given the risks to privacy.	
The processes used to de-identify data for statistical purposes should be made public.	As in the *Privacy Act 1988* (Cth) more broadly, de-identified data is treated as a category rather than as a scale of risk despite the fact that all data derived from personal information can be re-identified in at least some circumstances (such as by a person with existing knowledge derived from other data). Transparency would be improved by making explicit the processes used to render negligible the risk of re-identification.
For clarity, the Bill should amend not only the *Privacy Act*, but also federal laws concerning court and agency powers to obtain or use COVID app data.	Although cl 94ZD of the Bill ensures it overrides other laws, there may be loopholes, for example where Part 15 of the *Telecommunications Act* is used to seek assistance in decrypting data not on a device (but, perhaps, backed up in the cloud). Clear statements contained within the operating Act/s that powers do not apply to COVID app data are preferable.
Clause 94F of the Bill should be amended to provide that no data from the app can be taken out of Australia, with the exception of the situation contemplated in s cl 94F(2)(c).	On current drafting, it is possible that a person could get data about individuals while in Australia and take that to a foreign country provided they never 'retained' it on 'a database outside Australia'. This loophole should be closed.
Clause 94K of the Bill should be amended to provide that data relating to individuals' COVID-19 status and contacts be deleted from the data store and by state and territory health authorities after 21 days.	While information is deleted from a device after 21 days, there is no similar provision that it be deleted from the data store or by health authorities. After 21 days, data will no longer be useful for contact tracing. De-identified data within in the meaning of s 94D(2)(f) is already exempted.

The government should introduce amendments into the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (IPO Bill) and related agreements with the US to specifically exclude COVID app data. Note that the IPO Bill will make it possible for Australia to enter into an agreement with the US that would enable cooperation in accessing data stored in the other country.	Given the data will be held by a US company, there is also the possibility that US agencies may seek to access the data under US law, in particular, the *Clarifying Lawful Overseas Use of Data Act* ('US CLOUD Act'). This possibility has been rejected by the Secretary of Home Affairs, based on discussions with the US Department of Justice.[9] This relies on diplomatic assurances, that should be confirmed in due course through any forthcoming agreement between the US and Australia.
Clause 94ZC in the Bill should be amended to replace the reference to "property of the Commonwealth" with a more explicit statement of the rights and powers retained by the Commonwealth.	The Bill (cl 94ZC) provides that "COVID App data is the property of the Commonwealth" even after it is disclosed to or used by others including state and territory health authorities. This is a strange proposition given that data is not an object of property rights under Australian law.[10] If this provision is to protect the data from uses by other actors, it should be redrafted.
Clause 94H of the Bill and s 9 of the Determination should be amended to state that it is prohibited to make any of the enumerated activities a condition of exceptions to stay at home orders issued by any government, and to make it unlawful for an employer to install the app on a phone used by an employee.	These recommendations originate from Graham Greenleaf and Katharine Kemp, 'Australia's 'COVIDSafe 1App': An experiment in surveillance, trust and law' (above n 5)
A COVIDSafe Privacy Advisory Committee should be created in the Bill.	

[9] The Guardian reporting on Digital Transformation Agency evidence to the Senate Select Committee on Covid-19, 6 May 2020.
[10] Lyria Bennett Moses, 'Who Owns Information? Law Enforcement Information Sharing as a Case Study in Conceptual Confusion' (2020) *UNSW Law Journal*, forthcoming.