COVIDSafe App and human rights - Briefing Note

Executive Summary

1. The privacy concerns raised in the lead up to the release of the COVIDSafe App ('*the App*') in Australia on 26 April 2020 have largely fallen silent as the COVID-19 curve has been flattened, and the need for such tracing technology is no longer so urgent. In fact, its relevance has been called into question as the number of people traced through the App is so small.[1]

2. However, the concerns surrounding the App provide a useful case study for examining the existing Australian frameworks for protecting human rights and how these might be strengthened to avoid the human rights risks posed by the App, especially technology and data collection. It is important to consider how to address these risks before a future pandemic or crisis leads to renewed calls to use such measures.

3. Various human rights and privacy experts welcomed the App after reviewing its legislation, and concluded that it provided sufficient protections to address privacy concerns. These included the Australian Human Rights Commission,[2] the Law Council of Australia,[3] as well as law firm partners, global heads and specialists in technology and privacy law who co-signed an open letter encouraging people to download it.[4]

4. However, some of the broader risks to human rights posed by human tracing/tracking technology solutions include:

   4.1 Over-policing and targeting of certain groups with surveillance, including journalists;

   4.2 The unnecessary extension or permanent expansion of surveillance regimes; and

   4.3 The exclusion of vulnerable people from accessing the benefits.

5. In addition to the right to privacy, this technology has the potential to impact on freedom of association, facilitate discrimination against certain groups, and raises questions about the availability of effective remedies when these rights are breached, due to what a government could do with the data retained.

6. Australia relies on oversight and accountability mechanisms such as parliamentary processes for its human rights adherence, rather than entrenching human rights in a bill or charter of rights. Australia's current system means it is easier for legislative protections to be eroded, and fewer remedies are available.

---

[1] Josh Taylor, 'How did the Covidsafe App go from Being Vital to Almost Irrelevant?', *The Guardian* (online), 24 May 2020 <https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant>.

[2] Australian Human Rights Commission, *Commission Position on the Draft 'COVIDSafe App' Bill* (Web age, 8 May 2020) <https://humanrights.gov.au/about/news/commission-position-draft-covidsafe-app-bill>.

[3] Law Council of Australia, *Law Council President's Statement on the COVIDSafe Exposure Draft* (Web Page, 5 May 2020) <https://www.lawcouncil.asn.au/media/media-releases/law-council-presidents-statement-on-the-covidsafe-exposure-draft>.

[4] Naomi Neilson, '48 Lawyers Sign Open Letter Endorsing COVIDSafe App', *Lawyers Weekly* (online, 5 May 2020) <https://www.lawyersweekly.com.au/biglaw/28209-48-lawyers-sign-open-letter-endorsing-covidsafe-app>.

Level 26, 85 Castlereagh Street
Sydney NSW 2000 Australia
PO Box R235, Royal Exchange NSW 1225, Australia

AUCKLAND | BRISBANE | MELBOURNE | PERTH | **SYDNEY** | WELLINGTON
E: sydney@wottonkearney.com.au www.wottonkearney.com
T: + 61 2 8273 9900 **F:** + 61 2 8273 9901

Introduction

7. The App was released on 26 April 2020 and has since been downloaded by more than 6 million Australians, with strong encouragement by the government and business leaders that the benefits of the App as a public health response to the risk of the pandemic outweighs the risks to individuals' privacy. The Australian Government even described the App as "essential" in order to ease lockdown restrictions.[5]

8. On 14 May 2020, Parliament passed the *Privacy Amendment (Public Health Contact Information) Act* (Cth) ('*the Act*') to encourage uptake of the App. Some prominent human rights and privacy experts have welcomed the App, saying that the Act provides sufficient protections to address privacy concerns as articulated at [3].

9. However, there has been considerable controversy about the potential for the App and use of similar technology to constitute an unacceptable invasion of privacy and be misused in a manner which breaches human rights.

10. Given the likelihood of continuing and future health emergencies from this and other pandemics, this brief examines:

    10.1 the human rights standards applicable to the use of the App;

    10.2 the risks to human rights posed by health tracing/tracking technology solutions such as the App (including international case studies);

    10.3 how well the App and the Act in Australia addresses the human rights standards and risks; and

    10.4 recommendations for how an established human rights framework in Australia may offer greater protection of rights, thereby minimising existing risks and providing more reason for public confidence in the future.

Human Rights Standards applicable to the App

11. International human rights law holds that human rights may be restricted by states during public health emergencies, provided that the restrictions are lawful, necessary, and proportionate. Any restrictions imposed or limitations of rights must be limited in duration and must have regard to the potentially disproportionate impacts on specific populations or marginalised groups. Therefore, any attempt to track and monitor the spread of COVID-19 through the obtaining of data via Bluetooth will be subject to these rules.

12. The concern raised in respect of the App is that the collection of such data for public health purposes may also interfere with users' right to privacy by revealing their identities, and associations. The United Nations Human Rights Committee (UNHRC) has found that individuals' right to privacy must only be restricted "*in cases envisaged by the law*", and that such restrictions must be "*proportionate to the end sought*" and "*necessary in the circumstances*". Article 17 of the International Covenant on Civil and Political Rights (ICCPR), a derivation of Article 12 of the Universal Declaration of Human Rights (UDHR), holds that the law is to protect against "*arbitrary or unlawful influence*" with an individual's "*privacy, family, home or correspondence*".

13. Over 100 human rights organisations have encouraged governments to continue to uphold privacy rights through the COVID-19 crisis, particularly with regard to the use of digital technologies designed to contain the pandemic. Human Rights Watch have stated that, at minimum, technological measures should:

    - "*Be lawful, necessary, proportionate, transparent, and justified by legitimate public health objectives;*

[5] ABC News, 'The Main Points from Scott Morrison's Latest Coronavirus Update', *ABC News* (online, 2 May 2020) <https://www.abc.net.au/news/2020-05-01/scott-morrison-update-coronavirus-covidsafe-app-cohort-test/12206936>; Dinesh Kumar and Pj Radcliffe, 'False Positives, False Negatives: It's Hard to Say if the COVIDSafe App can Overcome its Shortcomings', *The Conversation* (online, 18 May 2020) <https://theconversation.com/false-positives-false-negatives-its-hard-to-say-if-the-covidsafe-app-can-overcome-its-shortcomings-138129>.

- *Be time-bound and only continue for as long as necessary to address the pandemic;*
- *Be limited in scope and purpose, used only for the purposes of responding to the pandemic;*
- *Ensure sufficient security of any personal data that is collected;*
- *Mitigate any risk of enabling discrimination or other rights abuses against marginalized populations;*
- *Be transparent about any data-sharing agreements with other public or private sector entities;*
- *Incorporate protections and safeguards against abusive surveillance and give people access to effective remedies; and*
- *Provide for free, active, and meaningful participation of relevant stakeholders in data collection efforts.*"[6]

14. Importantly, while international law is applicable, it is not necessarily enforceable in Australia unless it has been incorporated into domestic legislation. In the absence of such incorporation, it is merely aspirational at best, as it will lack the enforceability to be binding upon the operation of such an app.

15. In Australia, at a federal level, the privacy of Australians is protected by the *Privacy Act 1988* (Cth). The Australian Privacy Principles ('*APP*') constitute the cornerstone of the Privacy Act. The Act imposes obligations on 'APP entities' which are generally a federal government entity or office holder, or an organisation such as a body corporate.[7] Therefore, the company which oversees the storage of the data, Amazon Web Services in Australia, would be subject to the requirements of the Privacy Act. APP 6, for example, prohibits an APP entity from using or disclosing personal information for a purpose other than the purpose for which it was collected, unless a prescribed exception applies, such as where the person provides consent. It is noted that when people download the App, they do so voluntarily and thereby provide consent.

16. State and Territory legislation also has relevant application. For example, the *Privacy and Personal Information Protection Act 1998* (NSW) regulates the way NSW agencies collect and disclose personal information. The *Health Records Information Privacy Act 2002* (NSW) would also be relevant to the health information of individuals.[8] Health and other sensitive information will also be subject to the common law principles of confidentiality.[9]

Risks to human rights posed by health tracing/tracking technology solutions

Over-policing and targeting of certain groups and journalists with surveillance

17. The COVIDSafe App recognises other devices with the App installed and Bluetooth enabled. When the App recognises another user, it notes the date, time, distance and duration of the contact and the other user's reference code. The contact information stored on a person's mobile phone should be deleted on a 21-day rolling cycle, taking into account the COVID-19 incubation period and the time it takes to be tested for the virus.[10]

18. While the App does not collect the person's location, and personal details should be encrypted, it nevertheless tracks who people come into contact with. This proximity data will be of interest to law enforcement and intelligence agencies for use in crime investigation. In fact, former Federal Communications Minister, Stephen Conroy, has raised the concern that any app which records contact between different people, including when and how long for, is an alluring feature for security agencies, who may seek access to such data. He expressed a lack of confidence that any app issued by the government will not be compromised in this way.[11] Deputy chief medical officer, Nick Coatsworth, has revealed that multiple requests were made to include features in the App to assist

[6] Human Rights Watch, *Mobile Location Data and Covid-19: Q&A* (Web Page, 13 May 2020) <https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa>.
[7] Alison Baker and Oliver Jankowsky, *Overview of Privacy Law in Australia* (Web Page, 10 March 2017) <https://hallandwilcox.com.au/thinking/overview-of-privacy-law-in-australia/>.
[8] Information and Privacy Commission NSW, *Applying the Law* (Web Page) <https://www.ipc.nsw.gov.au/privacy/nsw-privacy-laws/applying-law>.
[9] Baker and Jankowsky (n 7).
[10] Department of Health, *COVIDSafe App* (Web Page, 13 May 2020) <https://www.health.gov.au/resources/apps-and-tools/covidsafe-app>.
[11] Digital Rights Watch, *The Government Covid-19 Contact Tracing Smartphone App* (Web Page, 24 April 2020) <https://digitalrightswatch.org.au/2020/04/24/covid-19-trace-app/>.

law enforcement agencies, however states that as of April 2020, the government has refused each request.[12]

19. Previous experience has shown that it is not uncommon for data to be misused beyond its intended purpose. For example, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* was used to gain access to the metadata of journalists in order to identify a confidential source, despite such legislation being created as a means of detecting and preventing terrorism, highlighting the ease with which the intended purpose of a law can be subverted.[13]

20. Australian metadata laws are a component of existing national security laws and are contained in the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, which caused public outcry when first enacted in May 2015. This act requires internet service providers to retain customers' metadata for two years, plus information about their telecommunications accounts and services. Metadata includes information on the people you have contacted, when and where such contact was made, how long for and the device that was used.[14]

Unnecessary extension or permanent expansion of surveillance regimes

21. The data collected by COVIDSafe should only be usable for the purpose of responding to the current pandemic, and its usage should cease once the pandemic has ended. The concern raised by the App is whether it will continue to linger after the current crisis, and whether it will be repurposed to make other use of the surveillance web that it has created.[15]

22. The history of emergency measures shows that when surveillance is introduced, it usually goes too far, fails to meet its objectives, and once approved, often outlives the event it was designed for. Without proper measures in place to limit the usage of such measures, technological preventive measures may become permanent features of an expanded surveillance regime.[16]

23. Dr Adam Fletcher, a human rights law expert in the Graduate School of Business at RMIT University notes that the privacy and human rights implications of the Bluetooth data collected are in question and the safe handling of any data eventually uploaded cannot yet be assessed. He also recognises that the government has a mixed track record on data privacy, as seen previously in their handling of Centrelink, medical records and census data. "*It also has a history of 'mission creep' regarding tracking mechanisms such as the metadata retention regime, where it allowed citizen's data to be accessed by all sorts of law enforcement mechanisms, contrary to initial intentions*."[17]

Exclusion of vulnerable people

24. If governments begin to develop an over-reliance on data obtained through mobile phones, this may have negative ramifications for marginalised groups who lack reliable access to internet services, putting their health and livelihoods at risk. There are more than 2.5 million Australians who are not online, while access to internet has become a necessity during these isolating times, particularly for older Australians.[18] Some older-model mobile phones, which may be more likely to be owned by those who are elderly or with less financial capacity, are not able to use the App. Further, some older Australians, most at risk from the virus due to their age, do not have access to technology at all. As at May 2020, the App conflicts with another essential monitoring app for those who have

[12] Paul Karp, 'Government Refuses Police Request for Access to Australian Coronavirus Contact Tracing App', *The Guardian* (online, 23 April 2020) <https://www.theguardian.com/australia-news/2020/apr/23/government-rules-out-police-having-any-access-to-australian-coronavirus-contact-tracing-app>.

[13] 'Is COVIDSafe Safe?', *The Signal* (ABC Radio, 2020).

[14] Wes Mountain, 'Four Laws that Need Urgent Reform to Protect both National Security and Press Freedom', *The Conversation* (online, 19 June 2019) <https://theconversation.com/four-laws-that-need-urgent-reform-to-protect-both-national-security-and-press-freedom-118994>.

[15] Maria O'Sullivan, *Coronavirus: The COVIDSafe Tracing App, Your Privacy, and the Role of Law* (Web Page, 29 April 2020) <https://lens.monash.edu/@politics-society/2020/04/29/1380222/coronavirus-the-covidsafe-tracing-app-your-privacy-and-the-role-of-law>.

[16] Human Rights Watch, *Covid-19 Apps Pose Serious Human Rights Risks* (Web Page, 13 May 2020) <https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks>.

[17] Diana Robertson, *Transparency Key to Uptake of Coronavirus Tracing App* (Web Page, 27 April 2020) <https://www.rmit.edu.au/news/all-news/2020/april/transparency-key-to-uptake-of-coronavirus-tracing-app>.

[18] Committee for Economic Development of Australia, *How COVID-19 is worsening digital inequality* (Web Page, 27 April 2020 <https://www.ceda.com.au/Digital-hub/Blogs/CEDA-Blog/April-2020/How-COVID-19-is-worsening-digital-inequality >.

diabetes.[19] People who suffer from diabetes have been recognised as an at-risk group when concerning the virus. Unfortunately, the only solution is to uninstall the App, which means that a vulnerable group is not able to enjoy its benefits.

25. The pandemic has made it more evident that the technological revolution cannot leave behind those most vulnerable, particularly when not having access to technology means missing out on protection from a deadly virus.

International comparison

26. Human rights have been a casualty of curbing the spread of coronavirus in countries such as China, where the use of technology to monitor the spread of coronavirus has been profound and controls many, if not all, aspects of daily life.

27. Chinese digital surveillance by mobile apps may have helped China to quickly stop the spread of the virus, with the combination of rigorous quarantining of infected people and accurate tracking of contacts proving to be very effective in containing the spread of COVID-19.[20]

28. However, as the experiences of countries such as China and Russia show, the initial minor undermining of privacy of citizens can pave the way for a limiting of freedom of movement, expression and association.[21] While these are countries with a history of implementing surveillance regimes, there are others such as South Korea and Israel which have also rapidly increased measures which impact freedoms. South Korea has additionally used credit card transaction histories in conjunction with CCTV footage evidence to monitor the movement of its citizens, while Israel's security agency actively tracks the location of its citizens and has the ability to order mandatory quarantine based on the collected data.[22]

How well does the App and the Act address the human rights standards and risks?

Privacy, freedom of movement and association

29. On 14 May 2020, Parliament passed *the Privacy Amendment (Public Health Contact Information) Act* (Cth) ('*the Act*') to encourage the uptake of the COVIDSafe app. This new legislation amended the *Privacy Act 1988* and repealed the Health Minister's determination under the *Biosecurity Act 2015* (Cth). There are proponents of the new Act who have summarised it as having sufficient privacy protections.[23]

30. The main protection for the right to privacy in the legislation is that a breach of a requirement under the legislation will constitute an interference with the privacy of an individual (s 94R) for the purposes of section 13 of the Privacy Act. The requirements mainly relate to the handling of the data, making decryption of its data a crime and coercing people into downloading the App.[24] However, the new legislation still leaves some concerns unanswered. For example, some have questioned whether data that is *derived* from COVIDSafe data will be subject to the same protections as COVIDSafe data itself.[25]

---

[19] Tim Biggs, 'COVIDSafe May Interfere with Diabetes-Monitoring Apps', *Sydney Morning Herald* (online, 1 May 2020) <https://www.smh.com.au/technology/covidsafe-may-interfere-with-diabetes-monitoring-apps-20200501-p54oyd.html>.

[20] Josh Taylor, 'Coronavirus Apps: How Australia's Covidsafe Compares to Other Countries' Contact Tracing Technology', *The Guardian* (online, 3 May 2020) <https://www.theguardian.com/australia-news/2020/may/03/coronavirus-apps-how-australias-covidsafe-compares-to-other-countries-contact-tracing-technology>.

[21] Human Rights Watch, *Covid-19 Apps Pose Serious Human Rights Risks* (Web Page, 13 May 2020) <https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks>.

[22] Arjun Kharpal, 'Use of Surveillance to Fight Coronavirus Raises Concerns about Government Power after Pandemic Ends' *CNBC* (online, 26 Mach 2020) <https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html>.

[23] Law Council of Australia (n 3); Australian Human Rights Commission (n 2).

[24] *Privacy Act 1988* (Cth) ss 8-9.

[25] Gavin Smith, Phil O'Sullivan and Claudia Hall, *The COVIDSafe Bill – Good Progress, But There's More to Do* (Web Page, 6 May 2020) <https://www.allens.com.au/insights-news/insights/2020/05/the-covidsafe-bill-good-progress-but-theres-more-to-do/>.

31. Section 94D of the Act contains a wide variety of purposes for which the collection, use or disclosure of app data can be valid. These can effectively restrict unauthorised purposes because the legislation is drafted with specific reference to authorised purposes. However, this may also be seen as exhaustive and would thus leave room for unauthorised purposes to not be technically illegal under the legislation. There are also unfortunately many instances in the Act where deletion of data becomes a live issue for privacy rights. It seems promising that data can also be deleted upon a request being made to the data store administrator from the user or former user of the COVIDSafe app. However, section 94L(1)(a) leaves open when deletion of the data can occur on request, saying that it can occur 'as soon as practicable', so long as 'all reasonable steps' are taken. The protections for deleting data of a user on request under s 94L also contains a carve-out for data that is de-identified. Some commentators have suggested the need for the Act to protect data once re-identification occurs.[26]

32. The Australian Prime Minister, Scott Morrison, has said that while the data will be held by the federal government, only state health authorities charged with contact tracing will be able to access it. Federal agencies such as Centrelink and the Department of Home Affairs will not be able to gain access to it. The government has said police will not be able to get the data, even with a warrant, and court orders will not be able to force the government to hand over the data.[27] However, the *Privacy Act 1988* (Cth), which protects privacy rights on a federal level, does not regulate state government agencies. Further, protections for the data from court orders or warrants are not explicitly laid out in the legislation.

33. Upon reviewing the legislation, the Australian Human Rights Commission and the Australian Law Council acknowledged that it contained several important protections, but warned of the need to do more.[28] There remains a risk that the ambiguities in the legislation allow for both unintended and intended breaches of privacy.

34. These risks need to be considered in light of the Australian Government's track record when it comes to looking after Australians' private data.[29] For example, in a review by the Australian National Audit Office (ANAO), the Government has been criticised for failing to manage cybersecurity and privacy risks in relation to My Health Record, a centralised system for patient records. The most recent privacy impact assessment conducted by the Australian Digital Health Agency was in 2017, and the four privacy reviews between October 2017 and June 2019, which cost $3.6 million dollars, have not been completed. The ANAO has stated that 'management of shared cybersecurity risks was not appropriate and should be improved with respect to those risks that are shared with third-party software vendors and healthcare provider organisations'.[30]

<u>Unnecessary extension or permanent expansion of surveillance regimes</u>

35. There is some ambiguity as to how long the App's data can be retained on a mobile phone. Although section 94K(a) states that it cannot be for more than 21 days, in the alternative, it cannot be *"…in any case in which it is not possible to comply with paragraph (a)… for longer than the shortest practicable period*". Therefore, there is no clear date at which the data can be taken off a mobile phone. Section 94Y(1) deals with determining the end of the "COVIDSafe data period". It is only at the end of this period that all data can be deleted from the server and the COVIDSafe app can be made "out of operation". This is left up to the Minister's discretion (with some consultation from the Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee). Therefore, there is no actual sunset period to this legislation.

---

[26] Ibid; Law Council of Australia (n 3).

[27] Josh Taylor, 'Covidsafe App: How Australia's Coronavirus Contact Tracing App Works, What it Does, Downloads and Problems', *The Guardian* (online, 15 May 2020) <https://www.theguardian.com/australia-news/2020/may/15/covid-safe-app-australia-how-download-does-it-work-australian-government-covidsafe-covid19-tracking-downloads>.

[28] Paul Farrell, 'Experts Raise Concerns About Security of Coronavirus Tracing App COVIDSafe' *ABC News* (online, 14 May 2020) <https://www.abc.net.au/news/2020-05-14/experts-concerned-about-coronavirus-tracing-covidsafe-security/12245122>.

[29] James Jin Kang, 'How Safe is COVIDSafe? What you Should Know About the App's Issues, and Bluetooth-related Risks', *The Conversation* (online, 7 May 2020) <https://theconversation.com/how-safe-is-covidsafe-what-you-should-know-about-the-apps-issues-and-bluetooth-related-risks-137894>.

[30] Australian National Audit Office, *Implementation of the My Health Record System* (Auditor-General Report No. 13 2019-20, 25 November 2019) 8.

36. There has also been confusion regarding where user data is sent, how it's stored, and who can access it.[31] If a user tests positive for COVID-19 and consents to their data being uploaded, the information is then held by the federal government on an Amazon Web Services (AWS) server in Australia.[32] The Amazon data centre has achieved a very high level of security as verified by the Australian Cyber Security Centre.[33] Someone who downloads the App has their data collected from the App which is stored on the user's device and transmitted in an encrypted form to the server. When this is done by other apps, data held within servers is then often used for marketing purposes.[34] While contact information stored on user devices is apparently deleted on a 21-day rolling basis, the Department of Health has said data sent to Amazon's server will "*be destroyed at the end of the pandemic*". It's unclear how such a date would be determined.[35] It's also likely that COVIDSafe isn't the only app that uses Bluetooth on a person's phone. Once Bluetooth is enabled, other apps may start using the COVIDSafe App to collect information without the person's knowledge as an incidental breach of privacy.[36]

37. The data must be properly and safely stored. There have been concerns around how the Australian government will protect data privacy, particularly given that the App's data is being stored by Amazon, a third party and US-based company.

38. US law requires that American corporations give the US government access to their data when so required, regardless of where the data is stored. The concern that arises is that the US government can access the COVIDSafe data, and they cannot be held accountable by the Australian public.[37]

39. The code for Australia's COVIDSafe App was based on Singapore's app 'TraceTogether', which the Singapore Government released both the source and server code for. The Australian Government has released the source code for the App, which allows for public scrutiny and allows the public to search for any vulnerabilities. However, the server code was omitted which could have allowed further scrutiny of how data is stored and encrypted.

Exclusion of vulnerable people

40. While the app raises valid questions with respect to users' privacy and data storage, it offers benefits in addressing COVID-19. However, certain vulnerable groups in society are faced with higher barriers to entry and are more likely to be excluded from accessing the app as a result of their circumstances. These groups may include the elderly, the homeless, some Aboriginal and Torres Strait Islander people and those experiencing financial disadvantage.

41. We currently lack data on whether the App is being downloaded by specific groups to identify how effective it is, such as frontline and essential service workers, people with underlying medical conditions and those with less access to healthcare and COVID-19 information generally.[38]

Remedies for breaches

42. International human rights law requires that people have access to effective remedies when their right to privacy is breached. The Australian Human Rights Commission has stated that the legal protections in the Act, including criminal offences for misuse of data, are effective remedies.[39] However, it has also recommended amendments to ensure that anyone who suffers loss as a consequence of a breach can seek compensation or other relevant remedies in respect of the losses, noting that the legislation emphasises criminal prosecutions over other existing remedies.

---

[31] Ibid.
[32] Dylan Welch and Linton Besser, 'Experts Warn There are Still Legal Ways the US could Obtain COVIDSafe Data', *ABC News* (online, 28 April 2020) <https://www.abc.net.au/news/2020-04-28/covidsafe-tracing-app-data-may-not-be-protected-from-usa/12189372>.
[33] Kang (n 29).
[34] Ibid.
[35] Ibid.
[36] Ibid.
[37] O'Sullivan (n 15).
[38] Kate Benson, 'How do you Download COVID-19 Apps if you don't Own a Device?', '*The Canberra Times* (online, 2 May 2020) <https://www.canberratimes.com.au/story/6742254/how-do-you-download-covid-19-apps-if-you-dont-own-a-device/>.
[39] Australian Human Rights Commission (n 2).

Criminal prosecutions require a higher standard of proof than civil suits, and this will make it more burdensome for applicants to succeed in a claim.

43. Barriers to accessing remedies need to be lowered, making them easier to obtain and less financially imposing upon applicants. Access to effective remedies should be provided in respect of both the actions of private individuals and in response to government actions while administering the App.

Recommendations for greater protection of rights through human rights frameworks

Recommendations

44. The effectiveness of the COVIDSafe App for the purpose of stopping coronavirus outbreaks in Australia is yet to be determined, but is looking questionable given the App has been identifying close contacts of people who have tested positive with coronavirus who have not already been found through manual contact tracing.[40] International experience has shown that there is the potential for such technology to be a powerful tool in a health crisis such as the current pandemic, but also for serious breaches of human rights to flow from the misuse of the health and proximity data in the immediate and longer term.

45. Immediate risks to privacy have been well considered and to a significant extent addressed in the legislation passed to accompany the release of the App. Further protections which have been recommended include:

45.1 Providing a review of the App's operation and data storage centre within six months of the Act coming into force, and periodic reporting obligations following this initial review, conducted by a parliamentary committee or an independent body, such as the Office of the Australian Information Commissioner.[41]

45.2 Clarifying the more ambiguous aspects of the handling of data, including the storage of the data in the COVIDSafe Data Store being for the minimum period necessary to complete contact tracing, a mandatory termination date for all data obtained through the App which is held on mobile phones, and a clear sunset clause in the legislation.

46. Less obvious is the risk of "mission creep" – that the government of the day will use the App for Covid-19 purposes, however will also continue to access the data after the pandemic,[42] and there will be unnecessary extension or permanent expansion of surveillance regimes well into the future. Australia's current reliance on parliamentary oversight and accountability mechanisms for its human rights adherence are more vulnerable to the politics of the day.

47. Protection from these longer-term, more insidious human rights risks, and prevention of the erosion of existing protections over time, is more likely to be assured if Australia strengthens its human rights frameworks in the form of a Bill or Charter of Rights. This would not only set a benchmark for human rights in Australia but also help to entrench human rights by creating a strong foundation for human rights in Australia.

48. It is for these reasons this brief not only highlights but recommends a greater entrenchment of rights via a Bill or Charter of Rights, and more specifically, to enact a statutory cause of action for serious invasion of privacy. This has been a longstanding policy of organisations like the NSW Council for Civil Liberties,[43] and the Covid-19 outbreak has further highlighted the need.

---

[40] Ben Grubb, ''Dishonest': COVIDSafe app has not detected a case despite 6 million downloads', *Sydney Morning Herald* (online), 21 June 2020 < https://www.smh.com.au/politics/federal/dishonest-covidsafe-app-has-not-detected-a-case-despite-6-million-downloads-20200627-p556s7.html>.

[41] Anthony Hallal, 'International Human Rights Law and Australia's COVIDSafe App', *Inernational Law Association* (online, May 2020) <http://ilareporter.org.au/2020/05/international-human-rights-law-and-australias-covidsafe-app-anthony-hallal/>.

[42] O'Sullivan (n 15).

[43] Nicholas Cowdery AO QC (President NSW Council for Civil Liberties), *Privacy and digital COVID-19 contact tracing* (online, 31 August 2020) <https://www.nswccl.org.au/privacy_and_digital_covid_19_contact_tracing >.