Scrutinising COVIDSafe: Frameworks for evaluating digital contact tracing technologies

Adam Lodders and Jeannie Marie Paterson
Centre for AI and Digital Ethics, The University of Melbourne, Australia

Abstract
Digital technologies are being used to combat the coronavirus disease 2019 (COVID-19) pandemic through a variety of methods, including monitoring compliance with quarantine and contact tracing. These uses of technology are said to promote public health outcomes but risk undermining rights to privacy. In this article we focus on the use of digital technologies for contact tracing, such as the COVIDSafe app used in Australia. We explore the kind of framework that might be used for evaluating the design, deployment and governance of such technologies to ensure they operate in a manner that is proportionate to the ends to be achieved. We conclude that, in addition to issues of privacy, any use of contact tracing technology should address important considerations of efficacy, equity and accountability.

Keywords
COVID-19, contact tracing, digital surveillance, digital ethics, digital equity, artificial intelligence, digital design

Across the world new digital technologies are being presented as a key to controlling the spread of COVID-19 and promoting public health. These technology-based interventions vary in the degree to which they intrude on individual privacy and the extent to which they utilise sophisticated algorithms or artificial intelligence (AI). Current uses include mobile phone contact tracing apps that identify who people have come into contact with, CCTV cameras and facial recognition technology to monitor the location of people supposed to be in isolation, and GPS data to monitor large gatherings which may develop into virus hot spots. As we move through different stages of the pandemic, reliance on technologies for public health purposes is unlikely to wane. Indeed, the use of digital technologies for monitoring the health status of individuals is likely to be important in managing any return to ‘normal’ public life.

These uses of digital technologies for contact tracing, contagion tracking and other forms of COVID-19 monitoring are ostensibly focused on public health outcomes. However, they also raise concerns about the potential for such technologies to erode individuals’ rights to privacy.

Corresponding author:
Professor Jeannie Paterson, Melbourne Law School, The University of Melbourne, 185 Pelham Street, Parkville, VIC 3053, Australia.
Email: jeanniep@unimelb.edu.au

References:
1. Juliet Bedford et al, ‘COVID-19: Towards Controlling of a Pandemic’ (2020) 395 The Lancet 1015.
2. Chris Stokel-Walker, ‘Can mobile contact-tracing apps help lift lockdown?’, BBC Future, (online, 16 April 2020) https://www.bbc.com/future/article/20200415-covid-19-could-blue-tooth-contact-tracing-end-lockdown-early.
3. Arjun Kharpal, ‘Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends’, CNBC (online, 26 March 2020) https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html.
4. Josh Taylor, ‘Facebook data to show Australians’ movement as they emerge from coronavirus lockdown’, The Guardian (online, 3 June 2020) https://www.theguardian.com/australia-news/2020/jun/03/facebook-data-to-show-australians-movement-as-they-emerge-from-coronavirus-lockdown.
5. Sue Halpern, ‘Can we track COVID-19 and protect privacy at the same time’, The New Yorker (online, 27 April 2020) https://www.newyorker.com/tech/annals-of-technology/can-we-track-covid-19-and-protect-privacy-at-the-same-time.
privacy and expand the scope of surveillance by governments, technology companies. The combination of data collection and predictive analytics enabled by new digital technologies and advances in computing capacity offer a rich source of information that has hitherto been unimaginable. Equally, the complexity and relative novelty of these technologies make it both difficult to scrutinise and easy to extend their operation. It is, accordingly, important to think very carefully at the outset about the design, deployment and governance of any digital technologies used for contact tracing and other responses to COVID-19. The aim should be to ensure that technologies presented as being in the public interest are utilised in a manner that is proportionate to the threat to which they are responding and consistent with the values of the society in which they are operating.

This article considers these issues with reference to the COVIDSafe app being used in Australia. We do this by drawing on the Australian government’s AI Ethics Principles. These principles are reflective of a larger body of work being developed in many countries around the governance of new digital technologies, with the goal of ensuring their use is human centred, fair and accountable. The Australian government’s COVIDSafe app is primarily a data collection tool, which does not involve AI in the sense of complex machine learning. However, future iterations of contact tracing apps are predicted to use more sophisticated algorithms to identify those contacts who are at risk. This makes the principles a particularly pertinent framework for assessing the government’s own digital initiatives.

We begin our inquiry by noting the varied international uses of digital technologies in tracing and monitoring the COVID-19 pandemic. We then address the elements that the government’s AI principles suggest should be considered in evaluating such technologies: namely matters of privacy and public interest, consent, efficacy, equity, contestability, explainability, accountability and transparency. We do not resolve all the questions around how these elements might be reconciled in respect to the COVIDSafe app and similar technologies. Rather, we seek to draw attention to the importance of this complex suite of considerations and the way in which they may apply in this context.

Digital technologies used for COVID-19 tracing, tracking and monitoring around the world

In Australia, the Commonwealth government launched COVIDSafe, a mobile phone app for contact tracing, in May 2020. Governments across the globe have also been utilising technology to assist in social distancing, quarantine and contact tracing in response to the COVID-19 pandemic. For example:

- In Russia the government is using Moscow’s CCTV network of 170,000 cameras to monitor people with facial-recognition software and punishing those not complying with quarantine and self-isolation.

See further Office of the Privacy Commission of New Zealand, ‘Overview of COVID-19 Contact Tracing Apps’ (12 May 2020) https://www.privacy.govt.nz/blog/the-app-race-to-contact-trace.
restrictions. This approach cannot be circumvented by citizens leaving their phone at home.

- China has used a similar approach to Russia, while also making use of a mobile phone app that provides colour-coded authorisation determining whether citizens are able to leave their homes or are at risk of virus infection.

- In South Korea, Taiwan and Poland governments are using mobile phones to monitor people in self-quarantine.

- Israel sought to repurpose location data collected from mobile phones for counterterrorism purposes to map the movements of people with COVID-19 and those they have encountered. Under this system the government’s counterintelligence agency, Shin Bet, would use phone metadata to identify individuals with the virus and their contacts, and then send an alert to those individuals’ contacts. The Supreme Court of Israel held this approach required legislation and oversight to continue operating.

- In Belgium, the government has been using the mobile phone data of 9 million people, out of a population of 11 million, to analyse movements to support social isolation policy settings and track inappropriate ‘lockdown parties’.  

- In Singapore a mobile phone application, TraceTogether, is being used to support the work of contact tracing. Australia’s app is based on this technology.

- Germany and Italy have launched contact tracing apps based on a model developed by Apple and Google.

- Authorities in England had been developing a contact tracing app but have now indicated support for the Apple/Google model.

As can be seen, these uses of technology in responding to the pandemic vary in the extent to which they are mandatory or consensual and the degree to which they intrude into citizens’ lives. In Australia and other comparable liberal democracies, greatest emphasis is being placed on phone apps to enable contact tracing. Tracking contacts of a person who is diagnosed with COVID-19 is a key public health tool that seeks to identify individuals who have come within a specific proximity of an infected person for a critical duration. In the absence of available smart phone apps, contact tracking relies on a person’s recollection of who they have come in contact with while infectious. The idea behind contact tracking apps is to improve the efficiency and accuracy of this process by allowing contact tracing through a digital record of proximate contacts recorded by an infected person’s phone. It is fair to say that as yet, if ever, the actuality of this technology has not lived up to its promise, and other concerns about its use have also been raised.

Digital ethics for COVID-19 tracing technologies

The use of innocuous technology in a phone for such important purposes as contact tracing is unprecedented in Australia, as elsewhere. As already noted, the use of this technology has potentially significant public health implications (improving contact tracing) but may also open the door to increased surveillance of individuals’ private lives. Thus, it is important to develop robust frameworks for the design, deployment and governance of such initiatives. One such framework is provided by work that has been done on ethical principles for new digital

---

13Ilya Khrennikov, ‘Moscow Deploys Facial Recognition to Spy on Citizens in Streets’, Bloomberg (online, 28 September 2017) https://www.bloomberg.com/news/articles/2017-09-28/moscow-deploys-facial-recognition-to-spy-on-citizens-in-streets; Mary Ilyushina, ‘How Russia is Using Authoritarian Tech to Curb Coronavirus’, The Verge (online, 15 April 2020) https://www.theverge.com/2020/4/15/21222161/apple-google-bluetooth-contact-tracing-system-coronavirus-health.

14Nicole Westman, ‘Google and Apple’s Covid-19 Tracking System Can’t Save Lives All on its own’, The Verge (online, 15 April 2020) https://www.theverge.com/2020/4/15/21222161/apple-google-bluetooth-contact-tracing-system-coronavirus-health.

15Chris Gillett, ‘Meet the Contact Tracers Fighting Coronavirus in Australia’, ABC News (online, 16 April 2020) https://www.abc.net.au/news/2020-04-16/meet-the-contact-tracers-fighting-coronavirus-in-australia/12151302.

16Paul Mozur, Raymond Zhong and Aaron Krolik, ‘In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags’, The New York Times (online, 1 March 2020) https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

17Lily Kuo, “The new normal”: China’s excessive coronavirus public monitoring could be here to stay’, The Guardian (online, 9 March 2020) https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.

18Simon Sharwood, ‘Pervasive digital surveillance of citizens deployed in COVID-19 fight, with rules that send genie back to bottle’, The Register (online, 16 March 2020) https://www.theregister.co.uk/2020/03/18/digital_surveillance_covid_19_coronavirus/;

19Ibid.

20Ibid.

21Lodders and Paterson

22Chris Gillett, ‘Meet the Contact Tracers Fighting Coronavirus in Australia’, ABC News (online, 16 April 2020) https://www.abc.net.au/news/2020-04-16/meet-the-contact-tracers-fighting-coronavirus-in-australia/12151302.

23Dan Sabbagh and Alex Hern, ‘UK Abandons Contact-Tracking App for Apple and Google model’ The Guardian (online, 19 June 2020) https://www.theguardian.com/world/2020/jun/18/uk-poised-to-abandon-coronavirus-app-in-favour-of-apple-and-google-models.

24Ibid.

25Ibid.

26Lodders and Paterson

---
technologies. In this article, we draw on the Australian government’s framework for ethical AI. In 2019, the Department of Industry, Science, Energy and Resources published a set of eight aspirational principles to inform the design, development and use of AI systems. The development of the principles was led by CSIRO’s Data 61 in consultation with stakeholders. Variations of these kinds of principles are also found in many other frameworks proposed for ethical AI and related digital technologies.

In many of the debates around the COVIDSafe app, concerns about privacy protection and human wellbeing/public health have been at the forefront. Considerations of these kinds are included in the government’s ethical AI principles. We also want to draw attention to the role of the other principles: autonomy (human centred values), reliability, fairness, accountability, contestability, explainability and transparency. These are important considerations in themselves. Moreover, these other principles for ethical AI and digital technologies are highly pertinent in assessing whether COVIDSafe and similar apps reach an appropriate balance between privacy and public health outcomes. In other words, they help illuminate the extent to which digital technologies represent a proportionate response to public interest goals.

Privacy and public health

In deploying contact tracing technologies, the goals of preserving privacy and advancing public wellbeing may appear to be in conflict, raising questions about the extent to which the need to reduce person-to-person transmission of COVID-19 should justify some loss of privacy and accompanying freedoms. On the one hand, the use of tracing technology aims to promote public health by allowing more effective identification of people who have come in contact with someone with the virus. It may also provide epidemiological evidence about the virus’s pattern of spread and the effectiveness of public health measures. On the other hand, the use of digital technologies for contact tracing, tracking or monitoring has the potential to threaten important and well-established rights to individual privacy. This is because tracing apps such as COVIDSafe collect data that would allow government agencies, and potentially also technology companies that develop or host the apps, to monitor people’s location and interactions.

Part of the solution to privacy concerns in contact tracing might be to try to avoid centralisation of the data collected. Apps relying on a centralised model, such as COVIDSafe, store encrypted user IDs in a centralised database and use the phone’s Bluetooth to identify other users that it comes into contact with. Should a user contract the virus, they will be asked to give consent for the encrypted data on their phone (the user IDs that they have been in contact with) to be shared with the relevant state or territory health authority. That agency will then use the data to determine which users require contact. These data are then held by that agency. While centralised data storage can create efficiencies for government and support research and other activities, it raises concerns about data potentially being stored for an indefinite time or repurposed for other uses – or, in other words, creeping surveillance.

At least in Australia, the Commonwealth government has put strict controls around the use of data collected by the COVIDSafe app. Nonetheless, privacy advocates have typically preferred a decentralised approach to data collection in contact tracing. However, this feature reduces the opportunity of health researchers and epidemiologists having easy access to the data to study the population in aggregate, although there may be other kinds of strategies that can deal with this issue. Thus, some health researchers have expressed concern about the UK government’s proposal to adopt the Apple/Google offering, on the ground that this approach reduces public health monitoring.

27. AI Ethics Principles (n 8).
28. Developing the AI Framework and principles, Department of Industry, Science, Energy and Resources (Web Page) https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/developing-the-ai-framework-and-principles.
29. See Anna Jobin, Marcello Ienca and Effy Vayena, ‘The Global Landscape of AI Ethics Guidelines’ (2019) 1 Nature Machine Intelligence 389 https://doi.org/10.1038/s42256-019-0088-2.
30. See, eg, Graham Greenleaf and Katharine Kemp, ‘Australia’s COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing’ (2020) University of New South Wales Law Research Series http://dx.doi.org/10.2139/ssrn.3601730 and resources cited therein.
31. See Malcolm Farr and Daniel Hurst, ‘Australian Government plans to bring in mobile phone app to track people with coronavirus’, The Guardian (online, 14 April 2020) https://www.theguardian.com/australia-news/2020/apr/14/australian-government-plans-to-bring-in-mobile-phone-app-to-track-people-with-coronavirus.
32. Neil M Richards, ‘The Dangers of Surveillance’ (2013) 126 Harvard Law Review 1934.
33. Marcello Ienca and Effy Vayena, ‘On the responsible use of digital data to tackle the COVID-19 pandemic’ (2020) 26 Nature Medicine 458.
34. Privacy Policy for COVIDSafe app, Department of Health (Web Page, 27 May 2020) https://www.health.gov.au/using-our-websites/privacy/privacy-policy-for-covidsafe-app.
35. For example, contact data is deleted after 21 days. Privacy Amendment (Public Health Contact Information) Act 2020 s 94K.
36. Kobi Leins, Christopher Culnane and Benjamin IP Rubinstein, ‘Tracking, Tracing, Trust: Contemplating mitigating the impact of COVID-19 through technological interventions’, Medical Journal of Australia (online, 17 June 2020) https://www.mja.com.au/journal/2020/213/1/tracking-tracing-trust-con templating-mitigating-impact-covid-19-through; Morley et al (n 9) 29, 31.
37. Alex Hern, ‘What is happening with the UK’s contact-tracing app?’, The Guardian (online, 19 June 2020) https://www.theguardian.com/world/2020/jun/18/what-is-happening-with-the-uks-contact-tracing-app.
38. Goldenfein, Green and Viljoen (n 6).
39. Sabbagh and Hern (n 23).
and analysis. Another real concern is that reliance on Apple and Google for this technology clearly risks placing more opportunities for data mining and influence in public health within the hands of already dominant technology companies.

Consent

The Australian government’s ethical framework for AI and digital technologies also emphasises the importance of ‘human centred values’, including the autonomy of individuals. Respect for individual autonomy is often addressed in data driven uses of technology through seeking consent for the collection and processing of data. As with most other uses of phones to trace the spread of COVID-19, the COVIDSafe app relies on the consent of individuals to both download the app and to report their diagnosis through the app should they become infected. These kinds of consent-based models, in which people have the choice to participate in tracking and monitoring, may seem like the best compromise between the competing concerns of controlling the spread of the virus and respecting individual privacy.

A different perspective is that, given the high number of people in the community who need to download these apps to be effective, discussed further below, an opt-in model is not appropriate and that using existing datasets, such as mobile phone location data could be considered instead. When Australian citizens were initially surveyed about their acceptance of tracking, 78 per cent of respondents were supportive of mass surveillance derived from mobile phone data for contact tracing and surveillance of people in quarantine, compared to 72 per cent for an opt-in model. This differed from populations in the United Kingdom where the milder opt-in approach was preferred and the United States where no level of tracking was acceptable. But these findings might be questioned on the ground that people may not have understood the long-term implications of phone tracking on privacy rights, or the risk of the data being used for other purposes, such as by insurers.

Thus, we come back to consent as the most acceptable model for contact tracing technologies. Under this approach the risks associated with the technology should be explained in the terms and conditions of the app. Here it is important to be aware of insights from consumer protection law which suggest that the fine print of contract terms and consent provisions often operate to give a veneer of choice where it has not in fact been meaningfully exercised. This is because people may often fail to read fine print terms, lack the reading skills required to understand fine print terms, or be steered to certain less than welfare-enhancing choices by the form of the terms and the risks they allocate.

People also find making significant decisions concerning the future difficult, particularly when operating under considerable stress and involving technology about which they have little experience. These insights mean that consent should not be used to justify technological options that otherwise pose risks for individuals. Rather the app should be guaranteed to meet baseline

---

40Hern (n 37).
41Naomi Klein, ‘Screen New Deal’, The Intercept (online, 9 May 2020) https://theintercept.com/2020/05/08/andrew-cuomo-eric-schmidt-coronavirus-tech-shock-doctrine/.
42AI Ethics Principles (n 8).
43See, eg, the GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) O.J. L 119, 27.04.2016, 1–88. Also Damian Clifford and Jeannie Marie Paterson, ‘Consumer Privacy and Consent’, Australian Law Journal (forthcoming 2020).
44See further Ada Lovelace Institute, ‘Exit through the App Store!’ (20 April 2020) https://www.adalovelaceinstitute.org/our-work/covid-19/covid-19-exit-through-the-app-store/.
45‘Privacy policy for COVIDSafe app’ (n 34).
46Simon Dennis et al, A Representative Sample of Australian Participants’ Attitudes Towards Government Tracking during the COVID-19 Pandemic (Research Report, The University of Melbourne, 9 April 2020) https://psychologicalsociences.unimelb.edu.au/research/hubs/chdh/preliminary-results-covid-19-tracking-social-licence.
47Simon Dennis et al, Social Licensing of Privacy-Encroaching Policies to Address the COVID-19 Pandemic (Report, 6 July 2020) https://stephaniewandowsky.github.io/UKSocialLicence/index.html. This is a live, non peer-reviewed document with a number of surveys complete. United Kingdom (29 March 2020): https://stephaniewandowsky.github.io/UKSocialLicence/UKcov1.html and United States (4 April 2020): https://stephaniewandowsky.github.io/UKSocialLicence/UScov.html.
48On data collection see Dana McKay et al, State of the Art in Data Tracking Technology (Research Report, Consumer Policy Research Centre, November 2019) https://cprc.org.au/wp-content/uploads/State-of-the-Art-in-Data-Tracking-Technology_UeM_FINAL_01112019.pdf.
49David Berrey, ‘Click to agree with what? No one reads terms of service, studies confirm’, The Guardian (online, 4 March 2017) https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print.
50ACCC, Digital Platforms Inquiry Report (2019) 25; ForbrukerRadet, Deceived by design (Report, 27 June 2018) https://www.forbrukerradet.no/under-sokelse/no-undersokselseskategori/deceived-by-design/.
51Uri Benoliel and Shmuel I Becher, ‘The Duty to Read the Unreadable’ (2019) 60 Boston College Law Review 2255. https://lawdigitalcommons.bc.edu/bclr/vol60/iss8/2.
52Caroline Beaton, ‘Humans Are Bad at Predicting Futures That Don’t Benefit Them’, The Atlantic (online, 2 November 2017) https://www.theatlantic.com/science/archive/2017/11/humans-are-bad-at-predicting-futures-that-dont-benefit-them/544709/.
53Moira Paterson and Maeve McDonagh, ‘Data Protection in an Era of Big Data: The challenges posed by big personal data’ (2018) 44(1) Monash University Law Review 1, 30; Neil Richards and Woodrow Hartzog, ‘The Pathologies of Digital Consent’ (2019) 96 Washington University Law Review 1461; Genevieve Helleringer and Anne-Lise Sibony, ‘European Consumer Protection Through the Behavioral Lense’ (2017) 23(3) Columbia Journal of European Law 607.
standards of efficacy and safety before individuals are asked to choose to download it.

Reliability and efficacy

The governments’ principles for ethical AI state that such systems ‘should reliably operate in accordance with their intended purpose’. This is consistent with basic consumer protection principles, which, as manifested in the Australian Consumer Law, hold that goods and services must be reasonably fit for any disclosed or represented purpose. The COVIDSafe app is not a consumer good but there is merit in demanding a similar baseline standard of functionality from a technology citizens have been asked to download for their own welfare and that of the community. If the app is not effective in performing its promoted function, then it is harder to say it is a proportionate response to measures that pose a risk to individual rights of privacy.

Many of the concerns around the efficacy and reliability of the COVIDSafe app in Australia relate to the technology chosen to implement the government’s tracing strategy. These concerns include: operation of the app on certain phones, the unreliability of Bluetooth, risks of unmanageable numbers of false positives, flaws in the guarantee of anonymity and the possibility of third parties being able to track individual movements through Bluetooth. Even assuming technical flaws can be addressed, there also remains uncertainty about whether governments can galvanise enough public support for the strategy to make it effective. Only 12 per cent of Singaporeans downloaded the TraceTogether app after its launch in late March 2020. Experts in the UK have proposed that 60 per cent or 80 per cent uptake is required for any app to be effective, while in Australia the figure has been proposed to be at least 70 per cent. At the time of release, the Australian government indicated that at least a 40 per cent uptake was required. At the time of writing, the number of Australians who have downloaded the COVIDSafe app has been well below these figures. Government reports suggest that about 5.6 million people had downloaded the app within days of its release. Since that time, the numbers have risen only to around six million and it has been reported that the app has not found a useful number of cases, with only six unique connections found in New South Wales and none in Victoria that were not already known to contact tracers.

We do not know the reason for this apparently stalled uptake but suggest that it may be influenced by a range of factors. These include low levels of trust in government, community concern about the effectiveness of the Commonwealth to deliver digital services, mission creep, concerns about personal privacy and standards of efficacy and safety before individuals are asked to choose to download it.

54 AI Ethics Principles (n 8).
55 Competition and Consumer Law Act 2010 (Cth) sch 2 (Australian Consumer Law) ss 55 and 61.
56 See also ‘Show evidence that apps for COVID-19 contact-tracing are secure and effective’, Nature (online, 29 April 2020) https://www.nature.com/articles/d41586-020-01264-1.
57 Rachel Riga, ‘How do you download the COVIDSafe app’ ABC News (online, 27 April 2020) https://www.abc.net.au/news/2020-04-27/how-to-download-the-covidsafe-app-and-the-issues-you-can-expect/12188156.
58 Alex Hern, (n 37).
59 ‘Experts examine the COVID-19 tracing app’, The University of Sydney (Web Page, 28 April 2020) https://www.sydney.edu.au/news-opinion/news/2020/04/28/experts-examine-the-covid-19-tracing-app.html.
60 Chris Culnane et al, ‘Tracing the challenges of COVIDSafe’ (Blog Post, 27 April 2020) https://github.com/vteague/contactT racking/blob/master/blog/2020-04-27T rackingTheChallenges.md; Leins, Culnane and Rubinstein (n 36).
61 James Jin Kang and Paul Haskell-Dowland, ‘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; Jim Mussared, ‘Privacy issues discovered in the BLE implementation of the COVIDSafe Android app’ (updated 15 May 2020) https://docs.google.com/document/d/1u5a5ersKBH6eG362atALrzuXo3zuZ70qrGomWVEC27U/preview.
62 Leo Kelion, ‘Coronavirus: NHS contact tracing app to target 80% of smartphone users’, BBC News (online, 16 April 2020) https://www.bbc.com/news/technology-52294696.
63 ‘Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown’, University of Oxford (Web Page, 16 April 2020) https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.
64 Kelion (n 62).
65 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.
66 Josh Taylor, ‘Australia’s coronavirus tracing app. What we know so far’, The Guardian (online, 19 April 2020) https://www.theguardian.com/world/2020/apr/17/australias-coronavirus-contact-tracing-app-what-we-know-so-far.
67 Georgia Hitch, ‘Coronavirus tracing app COVIDSafe now fully functional, Deputy Chief Medical Officer confirms’, ABC News (online, 13 May 2020) https://www.abc.net.au/news/2020-05-13/coronavirus-tracing-app-covidsafe-now-fully-functional/12244616.
68 Sophie Meixner, ‘How many people have downloaded the COVIDSafe app and how central has it been to Australia’s coronavirus response?’, ABC News (online, 2 June 2020) https://www.abc.net.au/news/2020-06-02-coronavirus-covid19-covidsafe-app-how-many-downloads-greg-hunt/12295130; Ben Grubb, ‘Dishonest’: COVIDSafe app has not detected a case despite 6 million downloads’, The Sydney Morning Herald (online, 28 June 2020) https://www.smh.com.au/politics/federal/dishonest-covidsafe-app-has-not-detected-a-case-despite-6-million-downloads-20200627-p55ks7.html.
69 Peter Lewis, ‘Trust in the government is rising – but will Australians accept the coronavirus tracing app?’, The Guardian (online, 21 April 2020) https://www.theguardian.com.australia-news/commentisfree/2020/apr/20/trust-in-the-government-is-rising-but-will-australians-accept-the-coronavirus-tracing-app.
70 Nicholas Biddle and Matthew Gray, ‘Australians want to support government use and sharing of data, but don’t trust their data will be safe’, The Conversation (online, 28 February 2019) https://theconversation.com/australians-want-to-support-government-use-and-sharing-of-data-but-dont-trust-their-data-will-be-safe-111610.
government surveillance, and the fact that a very high proportion of people need to opt-in to make it effective.\textsuperscript{72} It is possible that a perception that COVID-19 is under control in some communities has led people to disregard the app. However, further outbreaks may lead the government to conclude it is worth continuing to improve the effectiveness of the app. If so, we suggest that it is necessary to be absolutely clear regarding issues around the app’s workings and to engage with the community to allow improvements. It may be that contact tracing apps in many countries, including Australia, will inevitably devolve to the Apple/Google model. But, as noted above, this is not without democratic and commercial risks in having already monolithic technology companies dominating the public health responses to the pandemic.\textsuperscript{73}

**Fairness and equity**

Under the Australian government’s principles for ethical AI, ‘fairness’ means that AI and related digital systems should not result in ‘unfair discrimination against individuals, communities or groups’.\textsuperscript{74} Any digital tracing or tracking technology should not be used to perpetuate or amplify unlawful discrimination.\textsuperscript{75} Good processes around accountability and explainability will be crucial in this regard. Equally critical is for the experiences and the perspectives of all users to be included in the very design of the technologies.\textsuperscript{76}

Fairness, or what we might term ‘equity’, also requires that technologies be ‘inclusive and accessible’. In the case of contact tracing apps, concerns have been raised that the benefits of the technology may be out of reach of some people because of embedded social inequalities.\textsuperscript{77} Contact tracing apps rely on smartphones, which many people do not have.\textsuperscript{78} The contact tracing solution proposed by Apple and Google is dependent on a specific piece of hardware within the devices. Many people do not have such up-to-date devices, including those experiencing poverty, and the elderly.\textsuperscript{79} Additionally, some people may not know how to download or use the app, or afford the connectivity required to run it.

There are other hurdles to the effective utilisation of contact tracing apps that go beyond access to the devices needed to run the technology. Cathy O’Neil draws attention to the need to have access to adequate healthcare for those who are infected.\textsuperscript{80} Landau, Lopez and Moy forcefully describe how COVID-19 tracing technologies may perpetuate disadvantage because some communities may be distrustful of the authorities’ use of the data collected, risk higher numbers of false positives due to crowded living conditions and are vulnerable to more significant economic impact should they test positive.\textsuperscript{81} A technological response to COVID-19 that does not account for these systemic issues of disadvantage and exclusion will be unfair and should not be tolerated.

**Contestability**

Contestability under the Australian government’s principles for ethical AI requires that when an AI system ‘significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or output’ of that system.\textsuperscript{82} Currently, the use of the COVIDSafe app is consensual and there are rules against requiring a person to download the app.\textsuperscript{83} It will be interesting to see whether the COVIDSafe app or other variations become mandatory or amplify unlawful discrimination.\textsuperscript{85} Good processes around accountability and explainability will be crucial in this regard. Equally critical is for the experiences and the perspectives of all users to be included in the very design of the technologies.\textsuperscript{76} Fairness, or what we might term ‘equity’, also requires that technologies be ‘inclusive and accessible’. In the case of contact tracing apps, concerns have been raised that the benefits of the technology may be out of reach of some people because of embedded social inequalities.\textsuperscript{77} Contact tracing apps rely on smartphones, which many people do not have.\textsuperscript{78} The contact tracing solution proposed by Apple and Google is dependent on a specific piece of hardware within the devices. Many people do not have such up-to-date devices, including those experiencing poverty, and the elderly.\textsuperscript{79} Additionally, some people may not know how to download or use the app, or afford the connectivity required to run it.

There are other hurdles to the effective utilisation of contact tracing apps that go beyond access to the devices needed to run the technology. Cathy O’Neil draws attention to the need to have access to adequate healthcare for those who are infected.\textsuperscript{80} Landau, Lopez and Moy forcefully describe how COVID-19 tracing technologies may perpetuate disadvantage because some communities may be distrustful of the authorities’ use of the data collected, risk higher numbers of false positives due to crowded living conditions and are vulnerable to more significant economic impact should they test positive.\textsuperscript{81} A technological response to COVID-19 that does not account for these systemic issues of disadvantage and exclusion will be unfair and should not be tolerated.

**Contestability**

Contestability under the Australian government’s principles for ethical AI requires that when an AI system ‘significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or output’ of that system.\textsuperscript{82} Currently, the use of the COVIDSafe app is consensual and there are rules against requiring a person to download the app.\textsuperscript{83} It will be interesting to see whether the COVIDSafe app or other variations become mandatory or amplify unlawful discrimination.\textsuperscript{85} Good processes around accountability and explainability will be crucial in this regard. Equally critical is for the experiences and the perspectives of all users to be included in the very design of the technologies.\textsuperscript{76} Fairness, or what we might term ‘equity’, also requires that technologies be ‘inclusive and accessible’. In the case of contact tracing apps, concerns have been raised that the benefits of the technology may be out of reach of some people because of embedded social inequalities.\textsuperscript{77} Contact tracing apps rely on smartphones, which many people do not have.\textsuperscript{78} The contact tracing solution proposed by Apple and Google is dependent on a specific piece of hardware within the devices. Many people do not have such up-to-date devices, including those experiencing poverty, and the elderly.\textsuperscript{79} Additionally, some people may not know how to download or use the app, or afford the connectivity required to run it.

There are other hurdles to the effective utilisation of contact tracing apps that go beyond access to the devices needed to run the technology. Cathy O’Neil draws attention to the need to have access to adequate healthcare for those who are infected.\textsuperscript{80} Landau, Lopez and Moy forcefully describe how COVID-19 tracing technologies may perpetuate disadvantage because some communities may be distrustful of the authorities’ use of the data collected, risk higher numbers of false positives due to crowded living conditions and are vulnerable to more significant economic impact should they test positive.\textsuperscript{81} A technological response to COVID-19 that does not account for these systemic issues of disadvantage and exclusion will be unfair and should not be tolerated.
Accountability

Accountability relates to ensuring there is human oversight of an AI system or digital technology and that there are clear processes in place to ensure accountability for the operation of that system.\textsuperscript{85} Mello and Wang note that the pandemic has meant ‘technological solutions are being pursued by small groups of officials and tech company leaders working outside ordinary channels and public view’.\textsuperscript{86} There is a risk that, once technologies developed with minimal oversight with the potential for mass surveillance are enabled, they are unlikely to be watered down because they will have been legitimised as socially useful.\textsuperscript{87} It is therefore important that appropriate governance and regulatory safeguards are in place to guard against unscrutinised surveillance creep through technologies.\textsuperscript{88} These might include mechanisms for regular evaluation along with an explicit time limitation on usage. The Department of Health states that at the end of the pandemic users will be notified to delete the app and the government will destroy all data obtained.\textsuperscript{89} Currently, however, there is uncertainty around the nature of the review process and the discretion over how long the app will be in use.\textsuperscript{90} This is understandable given the uncertainties around the progress of the virus. But from a civil liberties perspective it would be preferable to have an automatic sunset clause that could be extended by the government if a demonstrated need was shown.

Transparency

Transparency means allowing people to understand the salient features of a system that affects them.\textsuperscript{92} Criticism has been made of the lack of transparency in the way the COVIDSafe app was initially promoted. The app was compared to ‘sunscreen style protection against COVID-19’, when it does nothing of the kind.\textsuperscript{93} Initial statements from the government also wrongly suggested that the key criteria for data collection were being within 1.5 metres and 15 minutes of close contact.\textsuperscript{94} Over promotion of the benefits of the app may create a false sense of security, undermining other public health efforts.\textsuperscript{95} By contrast accurate information provided to citizens about the process involved in collecting, storing and using the data as part of the broader contact tracing effort is essential in building public trust and allowing the kinds of debate that will improve the functionality and accountability of the app.

Technical transparency would come in providing software as open source, allowing inspection of the code.\textsuperscript{96} Such an approach would improve the app by providing opportunities for robust review and feedback by those with technical expertise within the community. As Greenleaf and Kemp detail, the source code for the COVIDSafe app was eventually released on 8 May 2020, but not the server code which contains critical information about the management and use of uploaded data.\textsuperscript{97}

Conclusion

There are unlikely to be any easy answers in determining the ideal strategy for digital technologies used in the fight against COVID-19. This article has focused on contact tracing apps such as Australia’s COVIDSafe. The future of this app is uncertain. It is possible it will be replaced with the decentralised Apple/Google approach that, at the time of writing, was gaining support as a more privacy preserving alternative, yet is not without its own concerns. Our overall objective has been to highlight the need for a robust framework for evaluating any contact tracing app. This scrutiny is essential in ensuring that

\begin{itemize}
  \item \textsuperscript{85}AI Ethics Principles (n 8).
  \item \textsuperscript{86}Michelle M Mello and C Jason Wang, ‘Ethics and governance for digital disease surveillance’ (2020) 10 Science 1126.
  \item \textsuperscript{87}O’Shea (n 7).
  \item \textsuperscript{88}Yuval Noah Harari, ‘The World After Coronavirus’, Financial Times (online, 20 March 2020) https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.
  \item \textsuperscript{89}Michelle M Mello and C Jason Wang, ‘Ethics and governance for digital disease surveillance’ (2020) 10 Science 1126.
  \item \textsuperscript{90}See, discussing the Privacy Amendment (Public Health Contact Information) Act 2020, Greenleaf and Kemp (n 30).
  \item \textsuperscript{91}Tim Miller, ‘What were you thinking’, Pursuit (online, 18 August 2018) https://pursuit.unimelb.edu.au/articles/what-were-you-thinking.
  \item \textsuperscript{92}AI Ethics Principles (n 8).
  \item \textsuperscript{93}Bernard Keane, ‘Download if you will’, Crikey (online, 5 May 2020) https://www.crikey.com.au/2020/05/05/covidsafe-app-misinformation-risks/.
  \item \textsuperscript{94}Maddocks, Privacy Impact Assessment (PIA) Report, 24 April 2020, recommendation 18 https://www.health.gov.au/resources/publications/covidsafe-application-privacy-impact-assessment; Greenleaf and Kemp (n 30).
  \item \textsuperscript{95}Landau, Lopez and May (n 81).
  \item \textsuperscript{96}A total of 653 scientists and researchers signed a statement including the recommendation that any solution be transparent, Dali Kaafar et al, Contact Tracing Joint Statement (Web Page, 3 July 2020) https://www.esac.kuleuven.be/cosis/sites/contact-tracing-joint-statement/.
  \item \textsuperscript{97}Greenleaf and Kemp (n 30).
\end{itemize}
public interest uses of digital technology are implemented in ways that actually accord with civic values.

Acknowledgments
The authors would like to acknowledge the valuable contributions made by Tim Miller, Gabby Bush and Calvin Collins. This article extends upon ideas first identified in a piece published by *Pursuit* at the University of Melbourne.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs
Adam Lodders https://orcid.org/0000-0003-2469-3924
Jeannie Marie Paterson https://orcid.org/0000-0002-2649-7591

Adam Lodders is Academic & Research Programs Manager at the Centre for AI and Digital Ethics, The University of Melbourne.

Jeannie Marie Paterson is a Professor at the Melbourne Law School and Co-Director of the Centre for AI and Digital Ethics, The University of Melbourne.