Tracking, tracing, trust: contemplating mitigating the impact of COVID-19 with technological interventions

A false impression of technological panacea may see much needed interventions overlooked and may introduce unintended consequences and risks

Kobi Leins

Christopher Culnane

Benjamin IP Rubinstein

University of Melbourne, Melbourne, VIC.

benjamin.rubinstein@unimelb.edu.au

doi: 10.5694/mja2.50669

The unedited version of this article was published as a preprint on mja.com.au 7 May 2020.

In the face of coronavirus disease 2019 (COVID-19) limiting free movement, experts are scrambling to mitigate the profound impact that the disease is having on our lives. For many countries, this approach involves increased testing, isolation, and education about hygiene practices until a vaccine is found. To varying degrees, without much evidence as to their efficacy, countries are turning to technology to solve some of the current challenges.[1] Increasingly, smartphone applications (apps) are being contemplated for tracking proximity of people to determine possible sources of transmission, with elements of technological solutionism. Such technical solutions require trust, and without honest and clear information about the possibilities and limitations of technologies, an app's benefits may be undermined by low adoption, or conversely a false impression of a technological panacea may see much needed interventions overlooked. For example, the Australian Government's target of a 40% uptake of the COVIDSafe app may or may not be effective in helping to control the disease, while 60% uptake is supported by independent modelling from the United Kingdom.[2] Furthermore, such summary statistics do not clarify to the public the wide range of other factors and assumptions that must be considered in predicting the app's efficacy.

Much is being written about the different technological models and whether they trace, track and comply with privacy and human rights frameworks, including whether this information can, in fact, ever be anonymised.[3] Fully effective anonymisation is unlikely when collecting data as granular as regular interaction with others in addition to age, gender and postcode demographics, as has been demonstrated by previous attempts to de-anonymise data.[4] If these data are accidentally or deliberately linked with other datasets, such as births in hospitals or the public Myki public transport dataset,[5] anonymity is virtually impossible to guarantee. Successful uptake of new technologies requires trust. When adoption is insufficient, collective benefits are not guaranteed. Civil society in the United Kingdom called for clear and comprehensive primary legislation to regulate data processing in symptom tracking and digital contact tracing applications, including with a strict purpose, access and time limitations.[6] Such regulation may improve trust.

Technology embeds values

Even when people are told of the limitations of technology, they may have magical thinking about its capabilities.[7,8] In early May 2020, the Australian Government furthered this magical thinking by direct messaging Australians that downloading the COVIDSafe app would help to keep people safe and ease restrictions, linking the two directly and potentially conflating the capability of COVIDSafe.

Contact tracing apps may assist in manual tracing, in turn slowing the virus' spread, but usage of an app does not render the individual protected from infection nor does it guarantee successful tracking without intensive manual efforts. Yet statements by those in authority have made strained assertions about COVIDSafe, likening the use of the app to the use of sunscreen[9] or a digital vaccine: "You could think about contact tracing as a digital vaccine with our contact data being the virtual antibodies".[10] Such statements are incorrect representations of the app's capabilities.[11]

Even the technical details of the app are not immune from false messaging. For example, the app records all Bluetooth contacts, not just those that last 15 minutes or that are within 1.5 m. The filtering occurs after contacts are uploaded. Furthermore, there are some inaccurate statements on the official COVIDSafe website; for example, the frequently asked questions section states that "all information that is stored on the phone is digitally encrypted;" however, metadata, such as the device make and model for each contact, are stored unencrypted.[12]

Communication must be fact-based, transparent and consultative, any short term gains in support from the use of emotive and persuasive messaging may be undone when they are ultimately demonstrated to be false.

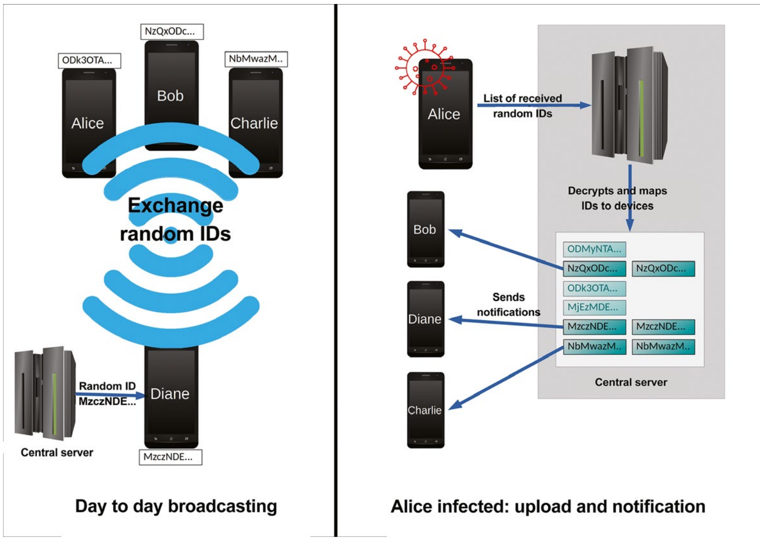
Centralised versus decentralised data collection

The fundamental difference between centralised versus decentralised tracking is in who learns what. In the centralised approach, the central authority learns who an infected person has interacted with, whereas this does not occur in the decentralised system. Decentralised systems are no more challenging to implement but they better protect privacy.

In a centralised approach (Box 1), such as TraceTogether (Singapore) or COVIDSafe (Australia):

- encrypted identifiers are issued by the central authority to each device;
- devices broadcast the encrypted identifiers via Bluetooth, and nearby devices listen for such broadcasts and record any that they receive;

1 The centralised approach of contact tracing wherein the central server learns user contact details



- if a person tests positive, they report to the central authority all the identifiers they have received within a predetermined timeframe; and
- the central authority decrypts the identifiers and maps them to the individuals they were issued to and duly notifies them if they are deemed to be at risk.

The above is a very high level description and there are many technical challenges in implementing such a system securely.[13]

In a decentralised approach (Box 2), as proposed by decentralised privacy-preserving proximity tracing (DP-3T), Covid Watch, Apple and Google:

- devices generate random identifiers that are not linked to an individual;
- identifiers are broadcast via Bluetooth and recorded by nearby devices;
- a person who tests positive publishes a list of the identifiers they have broadcast; and
- all apps on user devices download such lists and check if they received positive identifiers so as to identify likely contacts.

While there are variations in the details, in the decentralised approach, the central authority does not map identifiers to individuals.

Although the distinction between centralised versus decentralised tracking may seem small, from a privacy perspective, there is a significant difference. In the case of COVIDSafe, the identifiers are generated and provided to the phone individually rather than as a daily batch: the central authority can monitor whether the app is being used in at least 2-hourly increments, and possibly as frequently as every 9 minutes, due to regular checks for new identifiers.

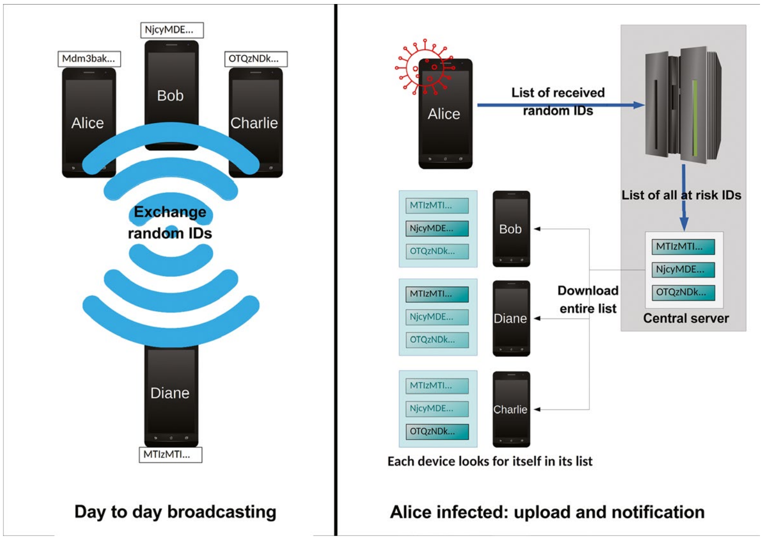
Models reflect differing societal priorities. In Germany, where there are legal protections for both individual and group privacy, the decentralised app has been chosen. In fact, it has been suggested that a decentralised smartphone contact tracing system — as contemplated by DP-3T, Apple, Google, and governments across Europe — would be likely to comply with human rights and data protection laws. In contrast, a centralised smartphone system would pose a greater risk to fundamental rights and would require significantly greater justification to be lawful.[6]

Even when consent for central data collection has been sought, it is unclear what users are consenting to in the absence of fully open code that includes server-side code, a clear regulatory framework, and with omissions, such as the COVIDSafe's Privacy Impact Assessment and Privacy Policy failing to mention the collection of the devices' make and model.[14] In comparison, Singapore's TraceTogether is based on the same codebase and its frequently asked questions section notifies of such data collection.[15]

Efficacy and risks of using Bluetooth

Bluetooth Low Energy (BLE) is designed to be a low power communication technology, it was

2 The decentralised approach to contact tracing wherein no central authority learns user contact details



not designed to facilitate range finding. Accurately measuring the distance between two devices based only on the received signal strength is a challenge, with error margins often in the metres.[16] The signal strength is relative not absolute, and thus, the scale of the reported values differ by manufacturer. Furthermore, the signal strength is influenced by many external factors, including the angle at which the device is held, whether it is in a pocket or a bag and any objects around or between it and the other device. Whether BLE can deliver the necessary accuracy remains an open question.

While the use of Bluetooth avoids direct location tracking, many other risks remain. There are vast networks of Bluetooth beacons distributed around cities, which facilitate location tracking. Security advice is to disable Bluetooth when not in use. While the public might be expected to compromise for the common good, legislation could also move to limit Bluetooth beacons during the crisis.

However, the *Privacy Amendment (Public Health Contact Information) Act* 2020[17] passed on 14 May provides no such protections.[18] It provides an exemption to those accidentally collecting COVIDSafe data as part of a wider collection of non-COVIDSafe data. This appears to be aimed at protecting commercial tracking, rather than protecting privacy.

Legal and social implications are as important as the technical ones

Given the many risks of using technology, the contemplation of any technological solutions to alleviate the impacts of COVID-19 needs to be not only technical but also legal and social. Making the code open for audit provides some technical guard rails, much as providing open and transparent proof of test results ensures that no risks are overseen. But beyond technical questions there are also legal questions, including with whom the data may be shared. A recently published article refers to the multiple legal regimes potentially applicable to the app in Australia, as experts scramble to review the legal protections for individuals using COVIDSafe.[19]

Enacting emergency measures in the face of catastrophes is easy. Rolling back changes to technology, habits and even culture is far more difficult. If they are to be used, technological tracking solutions must have sunset clauses to ensure that human rights are protected. But even with sunset clauses, the large quantity of data collected are effectively out in the world, where they can be accessed and misused. Protections and limits for these data and their providers need to be contemplated before use, not only to protect individuals but also for group privacy. Increasingly, there is a risk of data being accessed by overseas agencies, which could have an impact on national security.

It is vital that the technical, legal and social challenges are addressed in coordination. Any new legislation must be written within the context of existing technological practices, particularly around Bluetooth tracking. Likewise, where technical compromises are made, they must be justified to the public with clear, concise explanations, in a manner that is transparent and open to scrutiny.

While many liberties have been curtailed during COVID-19, all modifications to existing rights are required, under law, to be legal, necessary and proportionate. These same standards apply to the use of technology. Legal protections need to be in place to ensure that rights are protected, including the right to privacy. Without sound legal protections and safeguards, tracing apps will not only fail but will embed values that may not be those that represent the society we wish to be.

Acknowledgements: We thank David Watts and Vanessa Teague for their helpful comments.

Competing interests: No relevant disclosures.

Provenance: Commissioned; externally peer reviewed. ■

References are available online.

1 Parker J. Efficacy, ideology, and COVIDSafe. *Pursuit* (Melbourne) 2020, 11 May. https://pursuit.unimelb.edu.au/articles/efficacy-ideology-and-covidsafe (viewed May 2020).

2 Hinch R, Probert W, Nurtay A, et al. Effective configurations of a digital contact tracing app: a report to NHSX. https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf (viewed May 2020).

3 Culnane C, Leins K. Misconceptions in privacy protection and regulation. *Law in Cont* 2020; 36: 1–12. https://journals.latrobe.edu.au/index.php/law-in-context/article/view/110.

4 Narayanan A, Shi E, Rubinstein BIP. Link prediction by de-anonymization: how we won the Kaggle social network challenge. International Joint Conference on Neural Networks; San Jose (USA), 31 July – 5 Aug 2011. IEEE Press, 2011; pp. 1825–1834.

5 Culnane C, Rubinstein BIP, Teague V. Stop the open data bus, we want to get off. *arXiv* 2019; 1908.05004 [cs.CR]: https://arxiv.org/abs/1908.05004.

6 Matrix Chambers. Legal advice on smartphone contract tracing published [website]. London: Matrix Chambers, 2020. https://www.matrixlaw.co.uk/news/legal-advice-on-smartphone-contact-tracing-published/ (viewed May 2020).

7 Leins K. AI for better or for worse, or AI at all? Future Leaders, 2019. https://www.futureleaders.com.au/book_chapters/Artificial-Intelligence/Kobi-Leins.php (viewed May 2020).

8 Weizenbaum J. Computer power and human reason. New York: WH Freeman, 1976.

9 Prime Minister of Australia. Transcript of press conference — 29 Apr 2020. https://www.pm.gov.au/media/press-conference-australian-parliament-house-act-290420 (viewed May 2020).

10 Gauci R. AIIA supports government's COVID-19 tracing app after receiving detailed briefing from government. Melbourne: Australian Information Industry Association, 2020. https://mailchi.mp/aiia/aiia-supports-governments-covid-19-tracing-app?e=544bc002db (viewed May 2020).

11 Taylor J, Murphy-Oates L. Does the COVIDSafe app work? [podcast]. *The Guardian* 2020, 27 May. https://www.theguardian.com/australia-news/audio/2020/may/27/does-the-covidsafe-app-work-podcast

12 Australian Government, Department of Health. COVIDSafe app FAQs. https://www.health.gov.au/resources/publications/covidsafe-app-faqs (viewed May 2020).

13 Levy I. NHS COVID-19 app security: two weeks on. London: National Cyber Security Centre, 2020. https://www.ncsc.gov.uk/blog-post/nhs-covid-19-app-security-two-weeks-on (viewed May 2020).

14 Department of Health. Privacy policy for COVIDSafe app. Canberra: Commonwealth of Australia, 2020. https://www.health.gov.au/using-our-websites/privacy/privacy-policy-for-covidsafe-app (viewed May 2020).

15 TraceTogether. What data is collected? Are you able to see my personal data? Government of Singapore, 2020. https://tracetogether.zendesk.com/hc/en-sg/articles/360043735693-What-data-is-collected-Are-you-able-to-see-my-personal-data (viewed May 2020).

16 Huang B, Liu J, Sun W, Yang F. A robust indoor positioning method based on Bluetooth Low Energy with separate channel information. *Sensors* 2019; 19: 3487.

17 Privacy Amendment (Public Health Contact Information) Act 2020. https://www.legislation.gov.au/Details/C2020A00044 (viewed May 2020).

18 Taylor J. Questions remain over whether data collected by COVIDSafe app could be accessed by US law enforcement. *The Guardian* 2020, 14 May. https://www.theguardian.com/law/2020/may/14/questions-remain-over-whether-data-collected-by-covidsafe-app-could-be-accessed-by-us-law-enforcement (viewed May 2020).

19 Watts D. COVIDSafe, Australia's digital contact tracing app: the legal issues. SSRN 2020, 2 May. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3591622 (viewed May 2020). ■