The Medical Journal of Australia **– Preprint – 7 May 2020**

Tracking, Tracing, Trust: Contemplating Mitigating the Impact of COVID-19 through Technological Interventions

Kobi Leins
Research Fellow in Digital Ethics
University of Melbourne
Computing and Information Systems
Parkville, Victoria
Australia

Chris Culnane
Research Fellow
University of Melbourne
Computing and Information Systems
Parkville, Victoria
Australia

Benjamin I. P. Rubinstein
Senior Lecturer
University of Melbourne
Computing and Information Systems
Parkville, Victoria
Australia

Introduction

In the face of 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.

Increasingly, apps are being contemplated for tracking proximity of people to determine where transmission occurs. Much is being written about the different technological models, and whether they trace, track, comply with privacy and human rights frameworks, including whether this information can be anonymised. Anonymisation of individual information is challenging in general(1). Fully effective anonymisation is unlikely when collecting data as granular as regular interaction with others(2), and age, gender and postcode demographics. If further linked with other data sets, such as births in hospitals, or the public Myki data set(3), anonymity is virtually impossible to guarantee. Successful uptake of new technologies requires trust. Where adoption is insufficient, collective benefits are not guaranteed. New technologies can also undermine individual and collective privacy(4).

Technology Embeds Values

If it is decided that technology is useful, the history and context of the technology will affect its outcome.(5) A 'magical thinking' around technology has been observed widely(6). This week, the government messaged Australians' phones suggesting that downloading the COVIDSafe app would reduce restrictions, linking the two directly and potentially conflating the capability of COVIDSafe. Simplifying the function of technological solutions for mass communication risks overestimating or over promising technological capabilities. Contact tracing apps assist in manual tracing, in turn slowing the virus' spread, but usage of an app does not render the individual protected from infection. Yet statements made by those in authority have made strained assertions about COVIDSafe, likening the use of the app to the use of sunscreen(7), or a digital vaccine: 'You could think about contact tracing as a digital vaccine with our contact data being the virtual antibodies(8).' Such statements are incorrect representations of the app's capabilities. This may result in risk-taking and further spread of COVID-19 as people feel a false sense of security when using the app(9).

Introduction Centralised vs Decentralised Data Collection

The fundamental difference between centralised vs decentralised tracking is in who learns what. Decentralised systems are no more challenging to implement but better protect privacy. We focus here on collecting proximity data, as this is less sensitive than location data.

In the case of a centralised system, like TraceTogether (Singapore), 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. If a person tests positive, they report to the central authority all the identifiers they have received within a predetermined timeframe. 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(10). In a decentralised approach, like those proposed by DP-3T, Covid Watch, Apple, Google, devices generate random identifiers that are not linked to an individual. Bluetooth broadcast identifiers are again recorded by nearby devices. However, a user who tests positive publishes a list of the identifiers they have broadcast. All apps download such lists and check if they received positive identifiers, so as to identify likely contact. While there are variations in the details, the central authority does not map identifiers to individuals.

The distinction might seem small, and from a utility perspective they are largely identical, but from a privacy perspective there is a significant difference. In the centralised approach the central authority learns who an infected person has interacted with, whereas in the decentralised system they do not. Additionally, 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.

Bluetooth Risks in Centralised Data Collection

While Bluetooth avoids direct location tracking, 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.

Usage of the app may result in widespread behaviour change, with Bluetooth enabled beyond the present COVID-19 crisis. Unfortunately, Bluetooth has come to be used for invasive location tracking by commercial third parties. Given the requirement to enable Bluetooth, suitable legislative protections need to be included to prevent exposing app users to greater commercial location tracking. However, the Exposure Draft of the Privacy Amendment (Public Health Contact Information) Bill 2020(11) provides no such protections. In its current form, it provides an exemption to those accidentally collecting COVIDSafe data if it was collected as part of a wider collection of non-COVIDSafe data. This appears to be aimed at protecting commercial tracking, rather than protecting privacy. 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 de-centralised 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(12).

Even when consent for central data collection has been sought, it is unclear what users are consenting to in the absence of open code, a clear regulatory framework, and omissions such as COVIDSafe's Privacy Impact Assessment and Privacy Policy failing to mention collection of devices' make and model(13). In comparison, Singapore's TraceTogether is based on the same codebase and its FAQ notifies of such data collection(14).

Legal and Social Implications are as Important as the Technical

Given these potential risks, the contemplation of any technological solutions to alleviate the impacts of COVID-19 need to be not only technical, but also legal and social. Providing open code for audit provides some technical safety, much as providing open and transparent proof of test results ensures that no risks are overseen. But beyond technical questions are also legal questions, including with whom the data may be shared. Watts refers to the multiple legal regimes potentially applicable to the app in Australia, as experts scrambled to review the legal protections for those using COVIDSafe(15).

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 is effectively 'in the wild' where it can be accessed and misused. Protections and limits for this data and its providers need to be contemplated before use, not only to protect individuals but also for group privacy. Increasingly, as States intervene in others sovereign affairs, national security may also be at risk by such personal data being collected and stored, even briefly.

It is vital that the technical, legal, and social challenges are addressed in co-ordination. 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 protections are maintained, including protections to privacy. Without sound legal protections and safeguards, tracing apps will not only fail, but embed values that may not be those that represent the society we wish to be.

Acknowledgements: With enormous thanks to Professor David Watts and Associate Professor Vanessa Teague for their helpful comments.

References

1. Chris Culnane and Kobi Leins, Misconceptions in Privacy Protection and Regulation. LiC [Internet]. 2020Apr.16 [cited 2020May4];36(2):1-12. Available from: https://journals.latrobe.edu.au/index.php/law-in-context/article/view/110
2. Arvind Narayanan, Elaine Shi and Benjamin I. P. Rubinstein, Link prediction by de-anonymization: How we won the Kaggle social network challenge. International Joint Conference on Neural Networks, IEEE Press (2011), pp. 1825-1834
3. Chris Culnane, Benjamin I. P. Rubinstein and Vanessa Teague, Stop the Open Data Bus, We Want to Get Off. (2019) arXiv: 1908.05004 [cs.CR]
4. Kobi Leins, Do We Really Need a Tracking App and Can We Trust It? (2020) *Pursuit* https://pursuit.unimelb.edu.au/articles/do-we-really-need-a-tracking-app-and-can-we-trust-it
5. Sheila Jasanoff, 'Science Will not Come on a White Horse' (6 April 2020) https://www.thenation.com/article/society/sheila-jasanoff-interview-coronavirus/
6. Josef Weizenbaum J (1976). Computer Power and Human Reason cited in Kobi Leins, AI for Better or for Worse, Or AI at all? (2019) Future Leaders, https://www.futureleaders.com.au/book_chapters/Artificial-Intelligence/Kobi-Leins.php
7. Robert Hillard, Chair of the Australian Information Industry Association, in Prime Minister Scott Morrison, Transcript of Press Conference given on 29 Apr 2020, https://www.pm.gov.au/media/press-conference-australian-parliament-house-act-290420
8. https://www.zdnet.com/article/australias-covidsafe-contact-tracing-story-is-full-of-holes-and-we-should-worry/
9. https://policyoptions.irpp.org/magazines/april-2020/five-ways-a-covid-19-contact-tracing-app-could-make-things-worse/

10. Chris Culnane, Eleanor McMurtry, Robert Merkel and Vanessa Teague. ‘Tracing the challenges of COVIDSafe,‘ (4th May 2020) https://github.com/vteague/contactTracing/
11. https://www.ag.gov.au/RightsAndProtections/Privacy/Documents/exposure-draft-privacy-amendment-public-health-contact-information.pdf
12. https://www.matrixlaw.co.uk/news/legal-advice-on-smartphone-contact-tracing-published/
13. Australian Government Department of Health, Privacy policy for COVIDSafe app, (accessed 6 May 2020) https://www.health.gov.au/using-our-websites/privacy/privacy-policy-for-covidsafe-app
14. TraceTogether ‘What data is collected? Are you able to see my personal data?’, (accessed 6 May 2020) https://tracetogether.zendesk.com/hc/en-sg/articles/360043735693-What-data-is-collected-Are-you-able-to-see-my-personal-data-
15. David Watts, ‘COVIDSafe, Australia’s Digital Contact Tracing App: The Legal Issues’ (3 May 2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3591622