

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

IN REPLY: The coronavirus disease 2019 (COVID-19) pandemic has raised complex ethical questions, many of which focus on technology-based contact tracing. Commenting on our recent article,¹ Coghlan and colleagues observe that it may be “a moral requirement ... for citizens to support options to help protect the community”. We agree that there are strong individual and societal imperatives to support community protection, but we should also be aware of false dichotomies between embracing a single ad hoc solution and rejecting all technology outright. We believe that well implemented decentralised approaches and auditable open source codes reflect a better compromise, and that privacy and health are not in inherent tension.

Coghlan and colleagues note that potential improvements to health “benefit vulnerable and disadvantaged people who suffer disproportionate harms”. Similarly, potential privacy violations may disproportionately affect vulnerable groups.²

They also state that “providing individual app users with the discretion to act on notifications of potential exposure to COVID-19 may compromise disease control efforts”. However, COVIDSafe is not intended to be a tool of compliance, and as such, does not have the ability to enforce or monitor whether the recipient of an alert takes action. In COVIDSafe’s centralised design, enforcement is therefore equivalent to a decentralised approach. The risks that we have highlighted would be confirmed if COVIDSafe were to be used to monitor compliance. Such a change of function would be significant and would not be consistent with the statements and privacy impact assessment undertaken at its launch. For instance, users are currently permitted to use a pseudonym during registration, which implies that anonymity is allowed.

Coghlan and colleagues refer to the promotion of location tracking overseas “as necessary to understand community interactions and the effects of social distancing policies for current (and future) outbreaks”. The collection of citizens’ GPS data is a clear invasion of privacy; it is highly sensitive information that permits construction of detailed social graphs and reveals lifestyle attributes of users. The collection of location data should only ever be

voluntary, and should only occur where there is a compelling reason with known benefits. The risk is not only to individual human rights; such intimate data can be used to surveil individuals for other purposes (for example, at rallies or to track associations) at a scale that lacks available regulation, policy, technological safety or social understanding.

Much can be learned from using apps for contact tracing, based on the experience of COVIDSafe. Regulatory frameworks must be in place before any technical solutions are trialled, and systems must be technically sound. Alongside legal, policy, social and technical issues, ethical considerations should also be contemplated. This includes the longer term impact of the adoption of technologies on acceptance of technological solutionism, which may create more problems than it solves.

Christopher Culnane
Kobi Leins
Benjamin IP Rubinstein

University of Melbourne, Melbourne, VIC.

benjamin.rubinstein@unimelb.edu.au

Competing interests: No relevant disclosures. ■

doi: [10.5694/mja2.50683](https://doi.org/10.5694/mja2.50683)

© 2020 AMPCo Pty Ltd

References are available online.

- 1 Leins K, Culnane C, Rubinstein BI. Tracking, tracing, trust: contemplating mitigating the impact of COVID-19 through technological interventions. *Med J Aust* 2020; 213: 6–8.
- 2 Madden M, Gilman M, Levy K, Marwick A. Privacy, poverty, and Big Data: a matrix of vulnerabilities for poor Americans. *Washington University Law Rev* 2017; 95: 53–125. ■