The COVIDSafe app was just one contact tracing option. These alternatives guarantee more privacy

30 April 2020, by Kelsie Nabben

Credit: CC0 Public Domain

Since its release on Sunday, experts and members of the public alike have raised privacy concerns with the federal government's COVIDSafe mobile app.

The contact tracing app aims to stop COVID-19's spread by "tracing" interactions between users via Bluetooth, and alerting those who may have been in proximity with a confirmed case.

According to a recent poll commissioned by The Guardian, out of 1054 respondents, 57% said they were "concerned about the security of personal information collected" through COVIDSafe.

In its coronavirus response, the government has a golden opportunity to build public trust. There are other ways to build a digital contact tracing system, some of which would arguably raise fewer doubts about data security than the app.

All eyes on encryption

Incorporating advanced cryptography into COVIDSafe could have given Australian citizens a mathematical guarantee of their privacy, rather than a legal one.

A team at Canada's McGill University is working on a solution that uses "mix networks" to send cryptographically "hashed" contact tracing location data through multiple, decentralised servers. This process hides the location and time stamps of users, sharing only necessary data.

This would let the government alert those who have been near a diagnosed person, without revealing other identifiers that could be used to trace back to them.

It's currently unclear what encryption standards COVIDSafe is using, as the app's source code has not been publicly released, and the government has been widely criticised for this. Once the code is available, researchers will be able to review and assess how safe users' data is.

COVIDSafe is based on Singapore's TraceTogether mobile app. Cybersecurity experts Chris Culnane, Eleanor McMurtry, Robert Merkel and Vanessa Teague have raised concerns over the app's encryption standards.

If COVIDSafe has similar encryption standards—which we can't know without the source code—it would be wrong to say the app's data are encrypted. According to the experts, COVIDSafe shares a phone's exact model number in plaintext with other users, whose phones store this detail alongside the original user's corresponding unique ID.

Tough tech techniques for privacy

US-based advocacy group The Open Technology Institute has argued in favour of a "differential

privacy" method for encrypting contact tracing data. This involves injecting statistical "noise" into datasets, giving individuals plausible deniability if their data are leaked for purposes other than contact tracing.

Zero-knowledge proof is another option. In this computation technique, one party (the prover) proves to another party (the verifier) they know the value of a specific piece of information, without conveying any other information. Thus, it would "prove" necessary information such as who a user has been in proximity with, without revealing details such as their name, phone number, postcode, age, or other apps running on their phone.

Not on the cloud, but still an effective device

Some approaches to contact tracing involve specialised hardware. Simmel is a wearable pen-like contact tracing device. It's being designed by a Singapore-based team, supported by the European Commission's Next Generation Internet program. All data are stored in the device itself, so the user has full control of their trace history until they share it.

This provides citizens a tracing beacon they can give to health officials if diagnosed, but is otherwise not linked to them through phone data or personal identifiers.

Missed opportunity

The response to COVIDSafe has been varied. While the number of downloads has been promising since its release, iPhone users have faced a range of functionality issues. Federal police are also investigating a series of text message scams allegedly aiming to dupe users.

The federal government has not chosen a decentralised, open-source, privacy-first approach. A better response to contact tracing would have been to establish clearer user information requirements and interoperability specifications (standards allowing different technologies and data to interact).

Also, inviting the private sector to help develop solutions (backed by peer review) could have encouraged innovation and provided economic opportunities.

How do we define privacy?

Personal information collected via COVIDSafe is governed under the Privacy Act 1988 and the Biosecurity Determination 2020.

These legal regimes reveal a gap between the public's and the government's conceptions of "privacy".

You may think privacy means the government won't share your private information. But judging by its general approach, the government thinks privacy means it will only share your information if it has authorised itself to do so.

Fundamentally, once you've told the government something, it has broad latitude to share that information using legislative exemptions and permissions built up over decades. This is why, when it comes to data security, mathematical guarantees trump legal "guarantees".

For example, data collected by COVIDSafe may be accessible to various government departments through the recent anti-encryption legislation, the Assistance and Access Act. And you could be prosecuted for not properly self-isolating, based on your COVIDSafe data.

A right to feel secure

Moving forward, we may see more iterations of contact tracing technology in Australia and around the world.

The World Health Organisation is advocating for interoperability between contact tracing apps as part of the global virus response. And reports from Apple and Google indicate contact tracing will soon be built into your phone's operating system.

As our government considers what to do next, it must balance privacy considerations with public health. We shouldn't be forced to choose one over another.