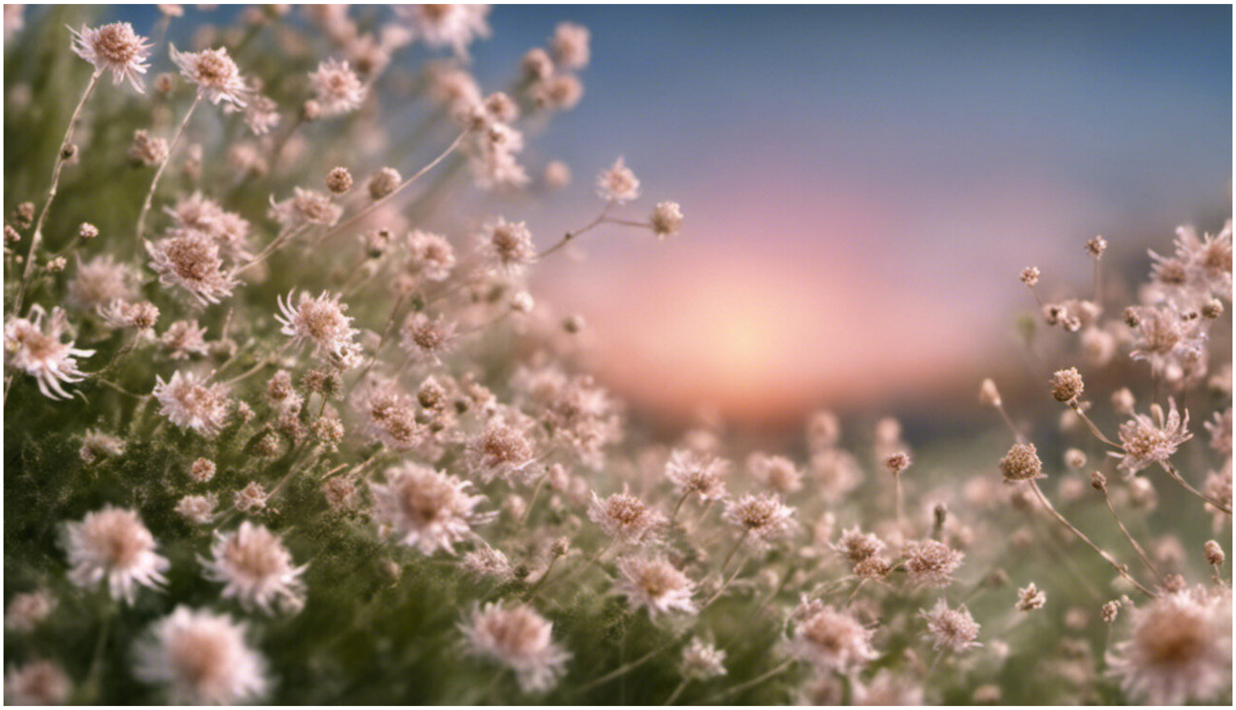
Is the Australian government's coronavirus app a risk to privacy?

April 21 2020, by Rick Sarre



Credit: AI-generated image (disclaimer)

Few people can fault the government's zeal in staring down the coronavirus and steering a path for Australia to emerge on the other side ready to do business again.

Unlike the crowds amassing in some US cities to declare their scorn for "stay at home" rules, Australians, generally speaking, have been supportive of federal and state government strategies to tackle the pandemic.

Prime Minister Scott Morrison has added a potential new weapon to his armoury—a COVID-19 tracing app. Government Services Minister Stuart Robert has been spruiking the plan to introduce the app, which is based on technology in use in Singapore.

But the idea of a government potentially monitoring our daily travels and interactions has drawn suspicion or even scorn. Nationals MP Barnaby Joyce says he won't be downloading the app.

Robert has since gone on the offensive, explaining the process and playing down any concerns.

"So if your app has been within 15 minutes' duration of someone within 1.5 metres proximity, there'll be a ping or swapping of phone numbers, and that'll stay on your phone. And then of course if you test positive … you'll give consent and those numbers will be provided securely to health professionals, and they'll be able to call people you've been in contact with … Those numbers will be on your phone, nowhere else, encrypted. You can't access them, no one else can."

Downloading the app is to be voluntary. But its effectiveness would be enhanced, Robert says, if a significant proportion of the population embraced the idea.

On ABC Radio National Breakfast this week he backed away from a previously mentioned minimum 40% community commitment. Instead, Robert said: "Any digital take-up … is of great value."

He has strong support from other quarters. Epidemiologist Marion

Kainer said the adoption of such an app would allow contact tracing to occur much more quickly.

"Having the rapid contact tracing is essential in controlling this, so having an app may allow us to open up society to a much greater extent than if we didn't have an app."

This all sounds well and good. But there are potential problems. Our starting point is that governments must ensure no policy sacrifices our democratic liberties in the pursuit of a goal that could be attained by other, less intrusive, schemes.

The immediate concern comes down to the age-old (and important) debate about how much freedom we are prepared to give up in fighting an existential threat, be it a virus, terrorism, or crime more generally.

Law academic Katharine Kemp last week highlighted her concerns about the dangers of adopting a poorly thought-through strategy before safeguards are in place.

The app, she said:

"will require a clear and accurate privacy policy; strict limits on the data collected and the purposes for which it can be used; strict limits on data sharing; and clear rules about when the data will be deleted."

Other commentators have warned more broadly against "mission creep": that is, with the tool in place, what's to stop a government insisting upon an expanded surveillance tool down the track?

True, downloading the app is voluntary, but the government has threatened that the price of not volunteering is a longer time-frame for the current restrictions. That threat fails any "pub" test of voluntariness.

On the other hand, there is a privacy trade-off that most people are willing to make if the benefits are manifestly clear. For example, our in-car mapping devices are clever enough (based on the speed of other road users with similar devices) to warn us of traffic problems ahead.

Remember, too, that Australians have had a 20-year love affair with smart technologies. We're a generation away from the naysayers who argued successfully against the Hawke government's failed Australia Card in the mid-1980s.

By the same token, the Coalition does not have a strong record of inspiring confidence in large-scale data collection and retrieval. One need only recall the lack of enthusiasm healthcare provider organisations showed for the My Health Record system. In 2019, the National Audit Office found the system had failed to manage its cybersecurity risks adequately.

So where do we go from here? The government sought to allay public concerns about the metadata retention scheme, a program introduced in 2015 to amass private telecommunications data, by giving a role to the Commonwealth Ombudsman to assess police agencies' compliance with their legislated powers. In the case of the COVID-19 tracing app, the government has, appropriately, enlisted the support of the Office of the Australian Information Commissioner. Robert has said:

"Right now a privacy impact assessment is being conducted, the Privacy Commissioner is involved, and all of that will be made public."

While that is an admirable sentiment, one would hope the government would put specific legislation in place to set out all of the conditions of use, and that the commissioner would not be asked for her view unless and until that legislation is in order. The Law Council of Australia has today joined this chorus.

Once the commissioner gives the "all clear," I will be happy to download the app. Let's hope it then works as intended.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Is the Australian government's coronavirus app a risk to privacy? (2020, April 21) retrieved 25 April 2024 from https://techxplore.com/news/2020-04-australian-coronavirus-app-privacy.html