

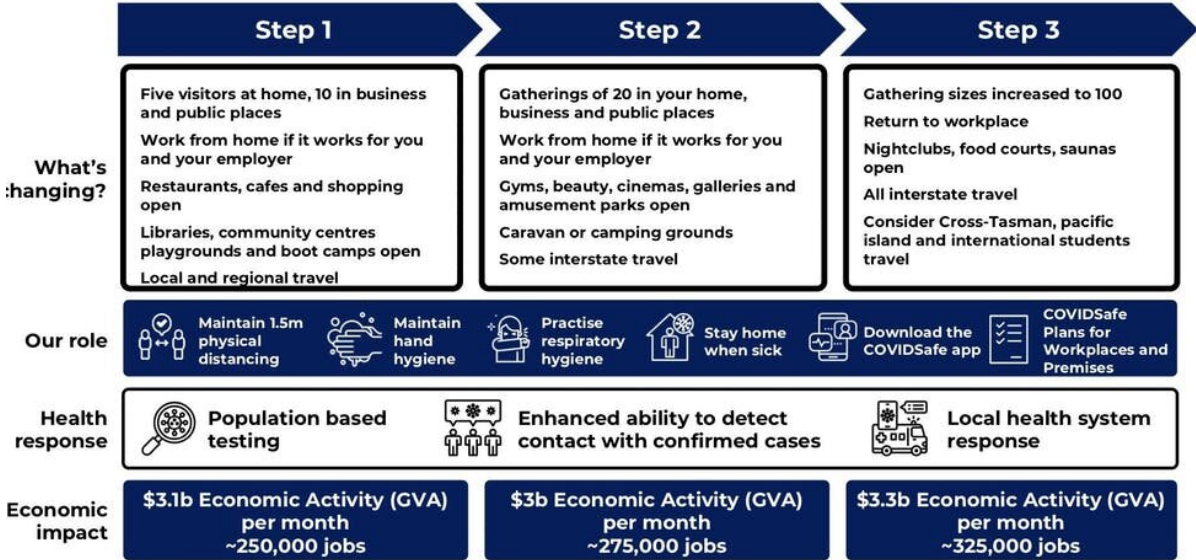
The trade-offs 'smart city' apps like COVIDSafe ask us to make go well beyond privacy

May 18 2020, by Kurt Iveson

Roadmap to a COVIDSafe Australia

COVIDSAFE

States and territories will move at different times based on local conditions



Australian government messaging is framing use of the COVIDSafe app, while voluntary, as being imperative in the public interest. Credit: Australian government/AAP

The Commonwealth government says if enough of us download its COVIDSafe app, restrictions on our movements and activities can be lifted more quickly and life can return to normal. As important as it is to

contain the spread of coronavirus, no government decision about how to do that is beyond question. For those of us concerned about the social and political life of our increasingly "smart" cities, the thinking behind the COVIDSafe app and other "smart city" technology must be open to challenge.

The public focus has been on the app's privacy implications, but other important issues warrant critical scrutiny too. Indeed, the app could help to entrench problematic forms of social and corporate power over our lives.

Social control

As research on the [politics of smart technologies in our cities insists](#), while [personal privacy](#) is important, it's not the only issue here. Apps like this have implications for the forms of social control that operate in dense urban environments—where use of a digital technology is technically "voluntary," but ends up being required if people want access to urban spaces and infrastructures.

Some protections are being promised in the case of the COVIDSafe app. These include a prohibition on employers, [government](#) authorities and others requiring any individual to install the app. The law still might not stop this in practice. Some [business groups](#) have [lobbied government](#) to enable employers to require employees to use the app.

Even if this legal prohibition holds, Prime Minister Scott Morrison has been making thinly veiled threats about more people needing to download the app before he lifts restrictions. App uptake is being demanded in the name of a public interest (in this case, public health).

There's also significant risk of mission creep here. What other "public interests" might be used to justify contact tracing based on this

precedent? It's easy to imagine [government agencies](#) and authorities desiring contact tracing in the service of a range of interests that could be discriminatory and oppressive—the policing of immigrants, welfare recipients and activists, for example.

We must guard against such surveillance creep.

Privacy protections

Compared to other government and corporate apps, the COVIDSafe app now has relatively strong privacy protections. It keeps information about who you share space or associate with, but not where you go. It does this by storing encrypted data on the user's phone about any other phones in range of a Bluetooth "handshake" that are also running the app.

Data will be automatically deleted after 21 days. Data will only be shared after a user has tested positive for COVID-19 and agreed to share the data. Only state health authorities may request and access data for contact tracing.

The [legislated protections](#) represent a big advance on some other government apps. For instance, [over 100 government authorities have access](#) to the data the New South Wales government collects from its public transport Opal smartcard.

It may be that neither governments nor corporations can assume people will continue to uncritically accept "[trade-offs](#)" of public goods like personal privacy and autonomy for the convenience and benefits of digital technology.

However, [some important privacy issues](#) remain unresolved, including:

- the amount of data stored, which is [about all devices in range](#), not

- just those in range for more than 15 minutes
- whether data stored on Amazon servers will [potentially be accessible for US law enforcement agencies](#),
- when and how the data and app will finally be deleted.

Questions of power and profit

It's also important to ask who benefits from the mass uptake of this app.

A government agency developed the app, drawing in part on an open-source app made available by the Singapore government. But even when an app is "free" and no one profits from its sale, remember that smartphones and data are not free.

Data storage has been contracted out to Amazon Web Services. It was the only company asked to tender for this lucrative government contract. That has [raised both security concerns and questions](#) about why locally owned, security-accredited providers were not invited.

Like so many instances of "smart" technology being offered as the solution to pressing problems, the profits of big tech and big telcos who sell us devices, connectivity and data storage are being presented as natural and aligned with public good. It is clear tech corporations see the coronavirus crisis as an [opportunity to consolidate and expand their profits and their power](#). Every problem [looks like a nail to the folks who have hammers to sell](#).

Will it work?

Given these concerns, will the COVIDSafe app even perform as promised? Here, the jury is still out.

Much discussion has focused on the minimum number of app users required for its coverage to be effective. But the app has other limitations too. It doesn't yet work properly on iPhones, for a start.

Most importantly, the app treats Bluetooth handshakes as a proxy for spatial proximity of devices, it treats this spatial proximity as a proxy for contact between people, and it treats prolonged contact between people as a proxy for viral transmission. Each step in this chain is [prone to significant failures and error](#).

Fortunately, then, the government is not proposing to replace contact tracing performed by human health professionals. Data from the app will be used to support that process.

It's vital we expand the scope of public discussion about this app and others in our increasingly "smart" cities and societies. Otherwise, we risk embracing "smart" solutions that create new surveillance infrastructures that further concentrate state and corporate power at the expense of our autonomy and alternative solutions to pressing societal problems.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: The trade-offs 'smart city' apps like COVIDSafe ask us to make go well beyond privacy (2020, May 18) retrieved 19 April 2024 from <https://techxplore.com/news/2020-05-trade-offs-smart-city-apps-covidsafe.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.