Written by Patrick Fair, Adjunct Professor, School of Information Technology, Deakin University

Borders, beaches, pubs and churches are closed, large events are cancelled, and travellers are subject to 14 days' isolation – all at significant cost to taxpayers and the economy. But could telecommunications technology offer a more targeted approach to controlling the spread of the COVID-19 coronavirus?

One possibility is to use location history data from the mobile phones of confirmed cases, to help track and trace the spread of infection.

Some people can be contagious without knowing, either because they have not yet developed symptoms, or because their symptoms are mild. These individuals cannot be identified until they become sufficiently unwell to seek medical assistance. Finding them more quickly could help curb the spread of the disease.

This suggestion clearly raises complex privacy issues.

Read more: ***Explainer: what is contact tracing and how does it help limit the coronavirus spread?***

All mobile service providers in Australia are required to hold two years of data relating to the use of each mobile phone on their network, including location information.

For anyone who tests positive with COVID-19, this data could be used to list every location where they (or, more accurately, their phone) had been over the preceding few weeks. Using that list, it would then be possible to identify every phone that had been in close proximity to the person's phone during that time. The owners of those phones could then be tested, even though they may not necessarily have developed symptoms or suspected that they had come into contact with the coronavirus.

The government could do this in a systematic way. It could assemble everyone's location history into a single, searchable database that could then be cross-referenced against the locations of known clusters of infection. This would allow contact tracing throughout the entire population, creating a more proactive way to track down suspected cases.

The privacy problem

You may well ask: do we want the government to assemble a searchable database showing the locations of almost every person over 16 in Australia over the past month?

Some people will undoubtedly find it a confronting prospect to be contacted by the government and told that surveillance analysis suggests they need to be isolated or tested. Others will be concerned that such a database, or the broad surveillance capability that underpins it, could be used to intrude on our privacy in other ways.

Several countries are already using mobile phone data in the fight against the coronavirus. The UK government is reportedly in talks with major mobile phone operators to use location data to analyse the outbreak's spread.

India, Hong Kong, Israel, Austria, Belgium, Germany are also among the list of countries taking advantage of mobile data to tackle the pandemic.

The Singapore government has launched an app called Trace Together , which allows mobile users to voluntarily share their location data. Iran's leaders have been accused of being rather less transparent, amid
reports
that its coronavirus "diagnosis" app also logs people's whereabouts.

Is it legal anyway?

We may well take the view that the privacy risks are justified in the circumstances. But does the Australian government actually have the power to use our data for this purpose?

The Telecommunications Act requires carriers to keep telecommunications data secure, but also allows federal, state and territory governments to request access to it for purposes including law enforcement, national security, and protecting public revenue.

Being infected with COVID-19 is not a crime, and while a pandemic is arguably a threat to national security, it is not specifically listed under the Act. Limiting the outbreak would undoubtedly benefit public revenue, but clearly the primary intent of contact tracing is as a public health measure.

There is another law that could also compel mobile carriers to hand over users' data. During a "human biosecurity emergency period", the Biosecurity Act 2015 allows the federal health minister to take any action necessary to prevent or control the "emergence, establishment or spread" of the declared emergency disease. A human biosecurity emergency period was declared on Sunday 23 March.

Read more: Explainer: what are the laws mandating self-isolation and how will they be enforced?

In recent years there has been a great deal of debate over the use of telecommunications data for surveillance purposes. The introduction of the mandatory data retention regime was contentious, as was the broad power granted to multiple agencies to access the data for law enforcement.

One reason for the controversy was the relatively low threshold for use of these laws: authorities could access data relating to any suspected offence punishable by three years or more in prison.

Australia is now facing a crisis that is orders of magnitude more serious. Many Australians would be willing to see their information used in this way if it saves lives, limits the economic impact, and impedes the spread of COVID-19.

The Commonwealth has the legal power to do it, the security and privacy issues can be managed, and the benefits may be significant.

Patrick Fair is principal of Patrick Fair Associates, and Chairman of the Communications Security Reference Panel at the Communications Alliance.

Authors: Patrick Fair, Adjunct Professor, School of Information Technology, Deakin University

Read more https://theconversation.com/privacy-vs-pandemic-government-tracking-of-mobile-phones-could-be-a-potent-weapon-against-covid-19-134895