Police Access to COVID Check-In Data Is An Affront to Our Privacy. We Need Stronger and More Consistent Rules in Place

Graham Greenleaf and Katharine Kemp

[2021] *UNSWLRS* 92
The Conversation (Online, 7 September 2021)

UNSW Law
UNSW Sydney NSW 2052 Australia

Police access to COVID check-in data is an affront to our privacy. We need stronger and more consistent rules in place

Graham Greenleaf Professor of Law and Information Systems, UNSW
Katharine Kemp Senior Lecturer, Faculty of Law & Justice, UNSW

This article was originally published in *The Conversation* on 7 September 2021

The Australian Information Commissioner this week called for a ban on police accessing QR code check-in data, unless for COVID-19 contact tracing purposes.

State police have already accessed this data on at least six occasions for unrelated criminal investigations, including in Queensland and Western Australia — the latter of which has now banned this. Victorian police also attempted access at least three times, according to reports, but were unsuccessful.

The ACT is considering a law preventing police from engaging in such activity, but the position is different in every state and territory.

We need cooperation and clarity regarding how COVID surveillance data is handled, to protect people's privacy and maintain public trust in surveillance measures. There is currently no consistent, overarching law that governs these various measures — which range from QR code check-ins to vaccine certificates.

Last week the Office of the Australian Information Commissioner released a set of five national COVID-19 privacy principles as a guide to "best practice" for governments and businesses handling personal COVID surveillance data.

But we believe these principles are vague and fail to address a range of issues, including whether or not police can access our data. We propose more detailed and consistent laws to be enacted throughout Australia, covering all COVID surveillance.

Multiple surveillance tools are being used

There are multiple COVID surveillance tools currently in use in Australia.

Proximity tracking through the COVIDSafe app has been available since last year, aiming to identify individuals who have come into contact with an infected person. But despite costing millions to develop, the app has reportedly disclosed only 17 unique unknown cases.

Over the past year we've also seen widespread attendance tracking via QR codes, now required by every state and territory government. This is probably the most extensive surveillance operation Australia has ever seen, with millions of check-ins each week. Fake apps have even emerged in an effort to bypass contact tracing.

In addition, COVID status certificates showing vaccination status are now available on MyGov (subject to problems of registration failure and forgery). They don't yet display COVID test results or COVID recovery status (as they do in countries in the European Union).

It's unclear exactly where Australian residents will need to show COVID status certificates, but this will likely include for travel between states or local government areas, attendance at events (such as sport events and funerals) and hospitality venues, and in some "no jab no job" workplaces.

As a possible substitute for hotel quarantine, South Australia is currently testing precise location tracking to enable home quarantine. This combines geolocation tracking of phones with facial recognition of the person answering the phone.

The proposed principles don't go far enough

The vague privacy principles proposed by Australia's privacy watchdogs are completely inadequate in the face of this complexity. They are mostly "privacy 101" requirements of existing privacy laws.

Here they are summarised, with some weaknesses noted.

1. **Data minimisation.** The personal information collected should be limited to the minimum necessary to achieve a legitimate purpose.
2. **Purpose limitation.** Information collected to mitigate COVID-19 risks "should generally not be used for other purposes". The term "generally" is undefined, and police are not specifically excluded.
3. **Security**. "Reasonable steps" should be taken to protect this data. Data localisation (storing it in Australia) is mentioned in the principles, but data encryption is not.
4. **Data retention/deletion**. The data should be deleted once no longer needed for the purpose for which it was collected. But there is no mention of a "sunset clause" requiring whole surveillance systems to also be dismantled when no longer needed.
5. **Regulation under privacy law**. The data should be protected by "an enforceable privacy law to ensure individuals have redress if their information is mishandled". The implied call for South Australia and Western Australia to enact privacy laws is welcome.

A proposal for detailed and consistent laws

Since COVID-19 surveillance requirements are justified as "emergency measures", they also require emergency quality protections.

Last year, the federal COVIDSafe Act provided the strongest privacy protections for any category of personal information collected in Australia. Although the app was a dud, the Act was not.

The EU has enacted thorough legislation for EU COVID digital certificates, which are being used across EU country borders. We can learn from this and establish principles that apply to all types of COVID surveillance in Australia. Here's what we recommend:

1. **Legislation, not regulations, of "emergency quality".** Regulations can be changed at will by the responsible minister, whereas changes in legislation require parliamentary approval. Regarding COVID surveillance data, a separate act in each jurisdiction should state the main rules and there should be no exceptions to these — not even for police or ASIO.

2. **Prevent unjustifiable discrimination.** This would include preventing discrimination against those who are unable to get vaccinated such as for health reasons, or those without access to digital technology such as mobile phones. In the EU, it's free to obtain a paper certificate and these must be accepted.
3. **Prohibit and penalise unauthorised use of data.** Permitted uses of surveillance data should be limited, with no exceptions for police or intelligence. COVID status certificates may be abused by employers or venues that decide to grant certain rights privileges based on them, without authorisation by law.
4. **Give individuals the right to sue.** If anyone breaches the acts we propose above for each state, individuals concerned should be able to sue in the courts for compensation for an interference with privacy.
5. **Prevent surveillance creep**. The law should make it as difficult as possible for any extra uses of the data to be authorised, say for marketing or town planning.
6. **Minimise data collection.** The minimum data necessary should be collected, and not collected with other data. If data is only needed for inspection, it should not be retained.
7. **Ongoing data deletion.** Data must be deleted periodically once it is no longer needed for pandemic purposes. In the EU, COVID certificate data inspected for border crossings is not recorded or retained.
8. **A "sunset clause" for the whole system**. Emergency measures should provide for their own termination. The law requires the COVIDSafe app to be terminated when it's no longer required or effective, along with its data. A similar plan should be in place for QR-code data and COVID status certificates.
9. **Active supervision and reports**. Privacy authorities should have clear obligations to report on COVID surveillance operations, and express views on termination of the system.
10. **Transparency.** Overarching all of these principles should be requirements for transparency. This should include publicly releasing medical/epidemiological advice on necessary measures, open-source software in all cases of digital COVID surveillance, initial privacy impact assessments and sunset clause recommendations.

COVID-19 has necessitated the most pervasive surveillance most of us have ever experienced. But such surveillance is really only justifiable as an emergency measure. It must not become a permanent part of state surveillance.