Australian Privacy Foundation

https://www.privacy.org.au

Secretary@privacy.org.au

https://privacy.org.au/about/contacts/

The Hon Scott Morrison MP
Prime Minister
Parliament House
Canberra ACT 2600

Dear Prime Minister,

**Re: A national legislative commitment to control secondary use of COVID-19 check in data**

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A copy of our COVID-19 Surveillance Policy and COVID-19 Immunisation Passport Position Statement are attached as background to this request for legislative support.

**Summary**

The APF request that:

1. You commit our government to applying the same laws protecting the national COVIDSafe app to all State and Territorial COVID-19 check in data, including Quick Response (QR) code apps and

2. Individuals have the right to litigate in the courts for compensation regarding privacy breaches outside the law.[1]

**Rationale**

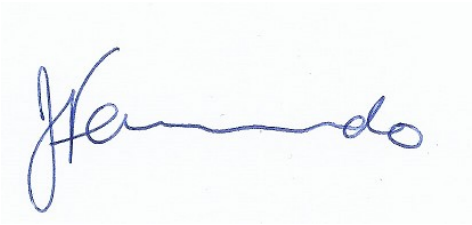
The COVID-19 pandemic has proved challenging for governments to manage over recent times, especially the Delta variant. The APF feel increasingly confused and alarmed by the plethora of State, and Territorial digital tools, founded on a complex mix of jurisdictional laws, regulating COVID-19 public health challenges.

The gap in Australia-wide government policy decisions about the proportionality justification for prohibiting or permitting routine police use of QR app data for purposes or uses other than informing app-users that a venue has become a close or casual contact site is cascading into a wicked problem that citizens manage every day.[1] Yet we are all required to comply with the complex mix of local State

and Territorial public health rules about the use of QR code data. The need for unified QR code data laws is growing increasingly crucial if the benefit of using QR technology will outweigh potential risk.

No access to QR code data beyond intended use is acceptable. This result is the key foundation of the community trust needed to advance public management of the COVID-19 pandemic. So, as an urgent priority, we ask for your commitment to achieving a federally unified, privacy enhancing, jurisdictional foundation for the use of QR data aimed at primary use outcomes only.

Yours sincerely



Dr. Juanita Fernando
Chair, Health Committee
Australian Privacy Foundation

Juanita.Fernando@privacy.org.au
Mob. 0408131535

ACKNOWLEDGEMENTS

I acknowledge and thank the members of the APF Health Committee and Board for their guidance herein.

REFERENCE

1. Greenleaf, G. & Kemp, K. Police access to COVID check-in data is an affront to our privacy. We need stronger and more consistent rules in place. The Conversation; 7 Sept. 2021. https://theconversation.com/police-access-to-covid-check-in-data-is-an-affront-to-our-privacy-we-need-stronger-and-more-consistent-rules-in-place-167360

**Australian Privacy Foundation Policy Statement on COVID-19 Surveillance**
**Version of 12 May 2021**

## General Context

Technological means for assisting with contact tracing and the containment of COVID19 have been heavily promoted and mandated throughout Australia. Many of these measures utilise the data collection and analysis potential of mobile phones, and represent forms of surveillance that would be unacceptable under other circumstances.

Given the protracted nature of the COVID19 pandemic and the plausibility of further pandemics occurring in the future, we assert the need for a concrete framework for assessing and regulating government policy in this area, with the overarching goal of upholding privacy and civil rights.

One of the core concerns with the implementation of novel surveillance regimes in times of exception is that, in many cases, governments are reluctant to dismantle systems of surveillance enacted during the crisis, seeking to justify their continued access to surveillance data after the immediate public health threats have subsided.

Acknowledging the substantial risk for data breaches, third party abuse and second party purpose creep (for example, where personal data is used for purposes unrelated to the public health response), any surveillance programmes enacted as part of the pandemic response must be independently justifiable, and subject to rigorous standards of transparency and accountability.

## Three Categories of COVID19 Surveillance

In Australia, we identity three principal categories of relevance with respect to COVID19 surveillance policies: 'Proximity Tracking', 'Attendance Tracking' and 'Entitlements'.

## 'Proximity Tracking'

The **COVIDSafe app** was proposed in 2020 as an aid to contact tracing. The app draws on Bluetooth signals to create records of 'contact events' between devices which *a)* have the app downloaded, *b)* have Bluetooth activated, and *c)* are within Bluetooth range.

There was a brief but robust public debate around the app's implications for privacy during the couple of weeks from its release until legislation was enacted. Given that use of the app has been entirely voluntary, significant but deficient efforts were made by the government

to assuage privacy concerns and promote the kind of trust required for a significant participation rate.

Despite continuing problems with transparency, accountability and data security, the COVIDSafe experiment was extraordinary in stimulating a broad public discussion around data privacy and bringing about an addition to Australia's 1988 Privacy Act: the COVIDSafe Act (Part VIII *Privacy Act 1088*).

**'Attendance Tracking'**

Unlike the COVIDSafe app, **QR 'check-in' codes** have effectively become mandatory for Australians, owing to their enforcement in most venues and indoor spaces. Despite carrying greater potential risks of privacy violations from both state and non-state actors, QR systems been introduced with far fewer protections and assurances than those that accompanied the COVIDSafe app.

**'Entitlements'**

Recent changes made to the Australian Immunisation Register Act, along with the expected rollout of an app-based 'vaccine passport' raise important ethical concerns around the privacy of personal health information, the rights of individuals in the face of discrimination on the basis of health information, and the potential for digital identification systems to become a perennial means of controlling and managing individuals within and across borders – with some similarities to China's 'social credit' system.[1]

**General Principles**

To protect against the various threats to privacy and civil liberties that these policies and programs might entail, we propose a set of general principles to guide policy and decision-making in this area.

1. **The use of surveillance technologies to manage the COVID19 pandemic often runs contrary to the protection of privacy and civil liberties.**
2. **Health, location and behavioural data are inherently sensitive**
3. **The need for digital surveillance tools to manage COVID19 cannot be assumed.**
4. **IT surveillance policies must be problem-oriented rather than tool-oriented.**

5. **Pandemic management policies should aim for privacy by design.**

6. **COVID19 surveillance regimes must be subject to regular, independent evaluation.**
7. **The scope of the COVIDsafe act should be expanded to cover all current and future pandemic surveillance policies.**

8. **The benefit of surveillance programmes must outweigh individual privacy and security threats.**

**General Principles (Extended)**

1. **The use of surveillance technologies to manage the COVID19 pandemic often runs contrary to the protection of privacy and civil liberties.**
    a. A ratcheting-up of government-on-population surveillance should not be taken lightly. While governments may be tempted to 'throw the kitchen sink' at a problem in the midst of an acute crisis, this approach is not defensible in Australia.
2. **Health, location and behavioural data are inherently sensitive**
    a. The categories of data targeted by COVID19 surveillance programmes carry specific and serious risks for various vulnerable groups, with harms associated with potential data breaches, discrimination, and access by government and law enforcement for purposes unrelated to public health.
    b. Likewise, the collection and use of these data classes impacts on everyone's privacy by restricting our ability to control the information that circulates about ourselves.
3. **The need for digital surveillance tools to manage COVID19 cannot be assumed.**

    a. Some investments in IT surveillance solutions have not only presented limitations and risks for privacy and civil rights, but have delivered minimal returns relative to resources expended.

    b. In the case of contact tracing, for example, manual methods have proven far more effective than the much-hyped digital solution of 'proximity tracking' through the COVIDSafe app.
    c. Likewise, it is uncertain how useful vaccination passports will be in facilitating travel and other activities. Emerging evidence has shown that while vaccines are effective in lowering the risk of severe illness, they may not reliably stop

[1] Bill Birtles, 'China Uses Social Credit Surveillance System to Ban Millions from Buying Plane and Train Tickets', *ABC News*, 23 February 2019 <https://www.abc.net.au/news/2019-02-23/china-bars-millions-from-travel-for-social-credit-offences/10843156>.

individuals from spreading the virus itself. This concern is particularly relevant in the context of new and emerging variants of the virus.

4. **IT Surveillance policies must be problem-oriented rather than tool-oriented.**
    a. In their preoccupation with the functionality and promise of digital solutions, policymakers often neglect to analyse the context and specifics of the problem that is being targeted.
    b. To prove their worth, IT surveillance measures must not only boast impressive functionality, but be strategically targeted to a specific problem area in which less invasive means have, or are very likely to prove ineffective.
5. **Pandemic management policies should aim for privacy by design.**
    a. The QR code 'attendance tracking' systems implemented in the UK and New Zealand might provide best practice examples of how this might be achieved, if evidence is available that they are also effective in contact tracing. In both cases, governments opted for an entirely de-centralised system where data is stored only on individuals' communication devices, creating a 'digital diary' that contact tracers can access directly in the event of an infection.
    b. Without a centralised database, there is little to no temptation for governments to use data for unrelated purposes, and minimal risk of data breaches by private actors.
    c. Systems constructed with privacy in mind have the benefit of requiring far fewer protections, safeguards and risk management protocols.
    d. While it may be too late to adopt this approach for Australia's already implemented 'proximity tracking' and 'attendance tracking' programmes, this should be a core priority of future pandemic-management policy, if evidence becomes available that these approaches.
6. **COVID19 surveillance regimes must be subject to regular, independent evaluation.**
    a. Independent assessments should be legally mandated and carried out by scientific, privacy and health experts.
    b. Experts must be given sufficient access to information, and legislators legally required to disclose any findings or professional advice to the public.
    c. Preliminary assessments should be made public well before any new legislation is put to parliament, allowing for a timely debate and consideration from the public.
    d. If the benefit of a given measure is found to be minimal and does not clearly outweigh the impact on privacy and civil liberties, it should be discontinued.
    e. All ongoing policies that limit privacy or civil rights must be subject to regular independent assessments to determine both whether the measure has been

effective, and continues to satisfy the principles of necessity and proportionality considered against the risks to privacy and civil rights.

7. **The scope of the COVIDsafe act should be expanded to cover all current and future pandemic surveillance policies.**
    a. In the absence of constitutional privacy rights or a strict requirement to adhere to the international treaty obligations, Australian states and territories require a legal regime to ensure that all surveillance policies proposed to manage COVID19 are subject to a consistent set of conditions and parameters.
    b. With small amendments, the COVIDsafe act (or equivalent State or Territory acts) could be adapted to perform this function. The objective is to create a set of legal conditions, protections and safeguards to which all current and future surveillance programmes must accord.
8. **The benefit of surveillance programmes must outweigh individual privacy and security threats.**
    a. The potential benefits of any new or ongoing surveillance regime for pandemic management must be carefully considered and weighed against the risks and harms to privacy and civil rights.
    b. Evaluations of benefit should be made by independent scientific and health experts rather than government ministers.

Australian Privacy Foundation (APF)
Position Statement, August 11, 2021

# Digital COVID-19 Vaccine Passport

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. Our COVID-19 Surveillance Policy Statement is a foundation of this Digital COVID-19 Vaccine Passport Position Statement.[1]

## PART 1

### 1. APF STATEMENT

**DIGITAL COVID-19 VACCINE PASSPORT**

An Australian digital COVID-19 Vaccine Passport is not useful for the introduction of proof of domestic vaccination measures.[2] Emerging evidence has shown that while vaccines are effective in lowering the risk of severe illness, they do not prevent individuals from spreading the virus itself. This concern is particularly relevant in the context of new and emerging variants of the virus.[1]

Incorrect information stored on COVID digital certificates combine with function creep, growing fraud concerns, and the Australian digital divide to undermine APF trust in COVID-19 Vaccine Passports, as articulated in Part 2.

Mask-wearing, good hygiene practices and social distancing measures, in addition to vaccination itself, are essential if Australians are to work our way out of the COVID-19 pandemic.

## PART 2

### 2.1 CONTEXT

Ongoing quarantine controls, known as 'lockdowns', have been mandated by Australian States and Territories as a response to the growing threat of the COVID-19 pandemic. The current variant, Delta, is more infectious and resistant to vaccines than earlier variants. The plausibility of exponential COVID variants emerging over time indicates these will be characterised by a higher reproduction ratio, proving more dangerous to peoples' health and wellbeing than Delta.

The Australian Immunisation Register (AIR), which records an individual's COVID vaccine status, is available online through a myGov account and the Express Medicare app; the digital records can be stored on a third party application installed on person's smart phone, but no rights to cross state and territorial borders or avoid lockdowns are linked to these records at present.[3-4] Current community, parliamentary and health authority debate over formal rights linked to a government-issued Digital COVID-19 Vaccine Passport (the Passport) for application for everyday life during lockdown, and as a condition of employment for people in some businesses and industry sectors, has prompted this statement.[3-4]

### 2.2 DIRECT BENEFIT OF VACCINATION

The direct benefit of COVID-19 vaccines in preventing infection generally ranges from higher than 80% to more than 90%. People who are fully vaccinated against COVID-19 can still acquire the virus and spread it to others despite the substantial control of this risk. Immunisation does not completely control the spread of COVID19.[1-2] Also, emerging evidence indicates that full immunisation against the virus may last around 8 months, so information stored in the Passport might prove useless after that time unless an individual has received regular booster vaccinations and these are recorded on AIR.[1] Reliance on the Passport to provide information about the spread of COVID-19 is therefore quite troubling.

### 2.3 UNEQUAL ACCESS TO VACCINE

Australians do not have equal access to COVID-19 vaccines. For example, many shift-workers, casual and contract workers do not benefit from terms and conditions of employment that facilitate time taken off for acquiring a vaccine. Should Australia depend on a digital passport system for avoiding lockdown, these people will be inherently disadvantaged and their participation in community life may be constrained.

### 2.4 THE DIGITAL DIVIDE

Australia's digital divide is substantial and growing over time.[8] More than 2.5 million Australians have no access to the Internet and so are excluded from all digital tools, while many mobile phone end-users do not own devices capable of functions other than telephony and basic text message services. These Australians will be unable to access digital COVID vaccination certificates or the Passport at all.

## 3. SPECIFIC APF CONCERNS

### 3.1 FAKE PASSPORTS

The market for fake COVID-19 vaccine passports is booming.[6] In recognition of this fact, a QR code will need to be added to the federal government's COVID Digital Certificate for validation as a Passport.[3] Function creep is already emerging in discussions of the Passport. The evidence shows that time and again, governments have used national digital systems "that have suffered from scope and function creep and have used data retrospectively in ways that were never intended".[9] Evidence suggests additional linkages will be added to the Digital Certificate Passport, adding to the behemoth of information currently held by the federal government about Australian citizens. Australians have no legally enforceable right to privacy. We therefore question the capacity of the Passport to maintain our civil liberties.

### 3.2 FLAWED AIR DATABASE

The AIR database, which records peoples' vaccine status, informs an individual's COVID Digital Certificate. But AIR records are not reliable. Some errors in the records mean that people cannot

receive a COVID vaccination because the AIR show this has already happened, while other errors mean vaccinations are not recorded at all.[7] This puts all AIR data in doubt. The poor quality of information stored in the government database means that records stored on the Passport are incorrect, forgeries notwithstanding.

Logically, these mistakes erode any confidence people or businesses may have in Passport accuracy.

### 3.3 SECURE PERSONAL DEVICES & THE DIGITAL INDEX

Recent research findings measuring Australia's digital inclusion index highlight significant barriers to digital ability, especially in technological skills domains, across the population. Mobile phone and tablet only end-users on the Internet, more than 19% of people, score well below the national average in digital ability regardless of their level of engagement with services and applications.[8] Working with Internet privacy and security tools on personal devices is a major technical challenge for many of these individuals. When these figures are added to the approximately 10% of people with no access to the Internet at all found in the inclusion study, almost a third of Australians, many of whom are already considered members of vulnerable groups in society, will find a digital Passport (and their inability to use one) to be a direct impediment to their daily lives.[8]

## 4. CONCLUSION

This position statement is not intended to discourage Australians from COVID-19 vaccination. Combined with mask-wearing, good hygiene practices and social distancing measures, vaccination is a core means of working our way out of lockdown, containing, and finally eliminating the health and wellbeing costs currently linked to the COVID-19 pandemic. Rather, we feel federal government health authorities can do better than apply a poor-quality digital Passport Band-Aid to the novel pandemic as Australia steers its way out of this crisis.

The APF would be glad to help authorities develop appropriate responses to the issues discussed in this statement.

## 5. NOTES

1. Conflict of Interest- None. The author is fully vaccinated against COVID-19.
2. Acknowledgement: I acknowledge and thank the members of the APF Health Committee and Board for their guidance herein.

## 6. REFERENCES

1. Australian Privacy Foundation (APF) COVID-19 Surveillance; Policy Statement, 12 May 2021. https://privacy.org.au/policies/covid-19-surveillance/
2. Koer, N. & Baylis, F. Nope. A Covid-19 Travel Pass isn't just like the Yellow Card, the Hastings Centre. 13 May 2021. https://www.thehastingscenter.org/nope-a-covid-19-travel-pass-isnt-just-like-theyellow-card/

3. McDonald, K. COVID-19 Digital Certificate can be added to Apple Wallet and Google Pay, Pulse IT. August 3, 2021. https://www.pulseitmagazine.com.au/australian-ehealth/6183-covid-19-digitalcertificate-can-be-added-to-apple-wallet-and-google-pay?utm_source=Pulse%2BIT++eNewsletters&utm_campaign=b8c2445f41-PulseIT_eNews_05_08_2021&utm_medium=email&utm_term=0_b39f06f53f-b8c2445f41-413218536&goal=0_b39f06f53f-b8c2445f41-413218536&mc_cid=b8c2445f41&mc_eid=8fccaf7520
4. Ziffer, D. Australians have a 'vaccine passport' to avoid border closures. We're not using it. Yet, ABC News, 28 June 2021. https://www.abc.net.au/news/2021-06-28/vaccine-passports-could-endlockdowns-for-some/100242506
5. Hon. Craig Lundy MP. No Domestic COVID Vaccine Passports Bill 202: A Bill for an Act to protect the right of Australians to make their own health decisions in relation to COVID vaccination, and for related purposes. Presented and read a first time 21 June 2021, second reading moved 21 June 2021.
The Parliament of the Commonwealth of Australia, HOUSE OF REPRESENTATIVES. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r 6724
6. Bacchi, U. Booming market for fake COVID-19 vaccine passports sparks alarm, Rueters. 9 April 2021. https://www.reuters.com/article/health-coronavirus-vaccine-passports-idUSL8N2M05AB
7. Knaus, C. "I am still waiting": some Australians turned away from getting Covid vaccine because of register errors, The Guardian. 3 August 2021. https://www.theguardian.com/society/2021/aug/03/iam-still-waiting-some-australians-turned-away-from-getting-covid-vaccine-because-of-register-errors
8. Thomas, J. & Barraket, J. et *al.* Measuring Australia's digital divide. The Australian Digital Inclusion Index 2020.Telstra. https://digitalinclusionindex.org.au/wpcontent/uploads/2020/10/TLS_ADII_Report-2020_WebU.pdf
9. Michael, K. & Abbas, R. The coronavirus contact tracing app won't log your location, but it will reveal who you hang out with, The Conversation. April 16 2020. https://theconversation.com/thecoronavirus-contact-tracing-app-wont-log-your-location-but-it-will-reveal-who-you-hang-out-with136387