



The Hon. Greg Hunt MP
Minister for Health
Commonwealth of Australia

The Hon. Brad Hazzard MP
Minister for Health and Medical Research
New South Wales

The Hon. Martin Foley MP
Minister for Health
Victoria

The Hon Stephen Wade MLC
Minister for Health and Wellbeing
South Australia

The Hon. Jeremy Rockliff MP
Minister for Health
Tasmania

The Hon Yvette D'Ath MP
Minister for Health and Ambulance Services
Queensland

The Hon. Roger Cook MLA
Minister for Health
Western Australia

The Hon. Natasha Fyles
Minister for Health
Northern Territory

The Hon Rachel Stephen-Smith MLA
Minister for Health
Australian Capital Territory

6 October 2021

Human rights safeguards in home quarantine technology

Dear Honourable Ministers,

Digital Rights Watch and the Human Rights Law Centre are Australian organisations advocating for the protection of human rights.

We write to urge you to adopt strong safeguards around the use and management of the personal information being collected and used by your governments in home quarantine arrangements.

We do so in the spirit of constructive support for your governments' efforts to minimise the impact of COVID-19 on Australians. We strongly support moving away from mandatory hotel quarantine detention as the primary quarantine response and allowing home quarantine in appropriate circumstances. Technology can support this transition. However, it is essential that there are robust safeguards in place to prevent the misuse of people's personal information. Unprecedented steps to gather and temporarily store personal information may be necessary to respond to the pandemic, however, such exceptional measures must come with robust safeguards.

In particular, we are concerned that while much effort was made to ensure the legislation governing the COVIDSafe app had appropriate privacy protections, the same efforts have not been put in place for other technological approaches to managing COVID-19. This includes the collection of personal information to ‘check in’ to venues across Australia, and now, the apps reportedly being used in home quarantine trials in South Australia, New South Wales and Victoria. The information being collected is just as sensitive as that which was to be collected by the COVIDSafe app, and therefore deserves at least the same protections.

Failure to implement proper privacy safeguards creates a significant risk that the social licence for such policies will be undermined. Trust in government and digital tools used by government in the context of the pandemic is paramount to the success of these policy approaches.

Human Rights Risks

Our particular concerns include:

1. The use of facial recognition technology to confirm an individual’s location is an extreme measure. Privacy and security experts, as well as civil society and human rights organisations around the world (including the Australian Human Rights Commission and the United Nations High Commissioner for Human Rights) have called for a moratorium on government use of facial recognition technology until there are appropriate regulatory frameworks in place. In Australia, there is no such regulation to ensure that the use of facial recognition technology is necessary, proportionate, and protects human rights in its application.

Current facial recognition technology has also been shown to exhibit gender and racial biases. In particular, it often fails to recognise the faces of those with darker skin tones. We are concerned that a significant proportion of users of such home quarantine apps may face unreasonable technical barriers to effectively use the tool through no fault of their own. It is unacceptable to subject individuals to the consequences of not meeting requirements to ‘check in’ if they are unable to do so as a result of the technology exhibiting racial bias.

2. The South Australian Home Quarantine App Privacy Statement currently provides that the information collected by the app is “encrypted immediately upon submission then transferred and stored on a secure server within Australia under the control of the Government of South Australia.” It then goes on to say that “the information will be destroyed at the conclusion of COVID-19 pandemic unless required for enforcement purposes for any alleged breach of a direction by you under the *Emergency Management Act 2004*.”

We are not satisfied that this is adequate protection for the kind of information that this app will collect, particularly with regard to the biometric information collected in order to verify a person’s identity. Once the home quarantine period is over, it unclear what legitimate purpose would be served by the retention of the biometric information. It is also unknown when and whether there will be a conclusion to the Covid-19 pandemic. Additionally, there have been several well-documented cases of law

enforcement authorities seeking to access QR ‘check-in data’, which undermines community trust and thereby erodes the efficacy of contact tracing efforts. Without robust and specific protections in place, the information collected by home quarantine apps may later be used for secondary purposes unrelated to public health. This risks undermining support and compliance, and ultimately compromising the public health response.

3. The South Australian home quarantine app currently takes a centralised approach, in which personal information is collected and transmitted to a central storage hub. This presents significant privacy and security risks. On-device authentication is one alternative approach that would significantly reduce the access risks posed by a central repository.
4. Generally speaking, extensive work was done to ensure that the COVIDSafe app met privacy and security requirements so that the personal information of Australians was adequately protected. We have not seen this level of work put into the state-based home quarantine solutions. Any further use of this app (or similar apps) must be met with the same level of privacy and security considerations as the COVIDSafe app. The risks remain unchanged.
5. Finally, legislative privacy protection for people varies across states and territories. Only Victoria, Queensland and the ACT have a Charter of Human Rights or Human Rights Act that protects the right to privacy. Western Australia and South Australia do not have any specific privacy legislation at all. People who are required to use a home quarantine app should have the assurance of robust privacy protections, regardless of where they are in Australia.

Recommendations

We call on your governments to implement the following safeguards in the ultimate home quarantine app or apps rolled out across Australia:

1. The COVIDSafe app legislation should serve as the guiding document in setting up all COVID-19 public health solutions and regimes which require handling of individuals' personal information. In particular, protections should be introduced to:
 - i. ensure all personal information is only collected, used and disclosed for the purpose of supporting state and territory efforts to manage home quarantine, and only to the extent required to do so;
 - ii. limit the retention period of personal information to the minimum time necessary in order to meet specific public health requirements. Any biometric data obtained for home quarantine purposes should be deleted following the conclusion of the quarantine period, given the purpose of the collection will have been served; and
 - iii. prohibit individuals' biometric data from being linked, aggregated or otherwise combined with any other existing datasets.

2. The apps should perform on-device identity and location-checking, rather than such verification taking place remotely. This would be a more secure and privacy-enhancing approach. It would mean that facial recognition technology could still be used to meet the need for identity verification, but the data would remain on an individual's device, rather than their biometric data being transferred and stored in a centralised database.
3. Governments should commit to regulating the use of facial recognition and other biometric technology with robust human rights safeguards, as was recently recommended by the Australian Human Rights Commission.

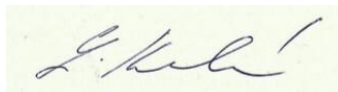
Australians will not have the power to make meaningful choices about providing personal information for home quarantine efforts. It is therefore essential that robust privacy and security protections are in place to ensure that this data is not retained longer than that which is necessary, and is protected from being misused or disclosed for purposes other than those supporting the COVID-19 public health response.

We would welcome the opportunity to discuss this matter with you.

Sincerely,



Hugh de Kretser
Executive Director
Human Rights Law Centre
hugh.dekretser@hrlc.org.au



Lucie Kraulcova
Executive Director
Digital Rights Watch
lucie@digitalrightswatch.org.au