Factsheet: COVIDSafe app and human rights

This factsheet is about Australia's COVIDSafe app and its consistency with international human rights law.

What is the COVIDSafe app and how does it work?

The COVIDSafe app is a tool that the Australian Government introduced to identify and contain COVID-19 outbreaks by making contact tracing faster and more effective.

Once downloaded onto a compatible device, users are provided with an explanation of how the app works, and are asked to consent to the Australian Department of Health collecting:

- their registration information to allow contact tracing by State or Territory health authorities; and
- their contact information (i.e. information on who they have been in contact with) from other COVIDSafe users who test positive for COVID-19.
-

If consent is provided, users are prompted to register their full name (or a pseudonym), their age range, their postcode and their mobile number. A unique encrypted reference code is then generated for the user.

Using Bluetooth, the COVIDSafe app recognises nearby devices that have the app installed and Bluetooth enabled.

When contact with another device is recognised, the COVIDSafe app exchanges an encrypted package of information between the devices. That package contains:

- the user's unique encrypted reference code;
- the Bluetooth signal strength of the contact to allow approximation of the users' distance from each other; and
- the date and time of the contact between the devices.

The package of information remains encrypted and stored on both users' devices for 21 days.

If a user tests positive to COVID-19, they are asked to consent to uploading their encrypted contact data from the COVIDSafe app to a secure information storage system called the National COVIDSafe Data Store. If consent is granted, then State and Territory health officials can use the uploaded contact data captured by the COVIDSafe app to support their usual contact tracing and to notify other users that they may have been exposed.

What is the domestic legal framework for the COVIDSafe app?

Initially, the COVIDSafe app and its data were regulated by a determination of the Health Minister under the Biosecurity Act 2015 (Cth). That determination was repealed by the Privacy Amendment (Public Health Contact Information) Act 2020 (Cth) (Amending Act), which inserts new provisions into the Privacy Act 1988 (Cth) (Privacy Act). Those new provisions set out the legislative framework for the COVIDSafe app and its data.

The new provisions include a range of protections for users of the COVIDSafe app. For example, under the new provisions, it is a criminal offence to:

The new provisions include a range of protections for users of the COVIDSafe app. For example, under the new provisions, it is a criminal offence to:

- collect, use or disclose COVIDSafe app data except in prescribed circumstances (section 94D);
- upload, or cause to be uploaded, COVIDSafe app data from a device to the National COVIDSafe Data Store without the user's consent (section 94E);
- retain COVIDSafe app data from the National COVIDSafe Data Store on a database outside of Australia (section 94F(1));
- disclose COVIDSafe app data from the National COVIDSafe Data Store to a person outside Australia, except State and Territory health authorities for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing (section 94F(2));
- decrypt COVIDSafe app data that is stored on a device (section 94G); and
- require, coerce or otherwise oblige (whether directly or indirectly) another person to install or use the COVIDSafe app, or to upload their contact data to the National COVIDSafe Data Store (section 94H).

The new provisions are also subject to oversight by the Australian Information Commissioner, and impose reporting requirements. In particular, periodic reports must be prepared by:

- the Health Minister about the operation and effectiveness of the COVIDSafe app and the National COVIDSafe Data Store (section 94ZA); and
- the Australian Information Commissioner about the performance of its functions and exercise of its powers under the new provisions (section 94ZB).

The human right to privacy under international law: sources, obligations and limitations

A central feature of the COVIDSafe app is the collection, use, disclosure and storage of users' data. Consequently, the human right that has received the greatest attention following the introduction of the app is the right to not be subjected to arbitrary or unlawful interference with one's privacy.

Sources

The principal source of that right under international law is Article 17 of the International Covenant on Civil and Political Rights (ICCPR), a treaty to which Australia is bound.

Although this factsheet will focus on the right to privacy under the ICCPR, it should be noted that similar rights are recognised by other international human rights treaties, including the Convention on the Rights of the Child (Article 16) and the Convention on the Rights of Persons with Disabilities (Article 22).

Additionally, it is arguable that the right to privacy has crystallised into international customary law, or at least constitutes an emerging custom.

Obligations

Like all rights that are recognised by international human rights law, the right to privacy under Article 17 of the ICCPR imposes correlative obligations on States, including Australia. In practice, these obligations are described as States' duties to respect, protect and fulfil human rights.

The Human Rights Committee (HRC) has provided further detail on the content of States' obligations in relation to the right to privacy under the ICCPR. For example, the HRC commented in the first paragraph of General Comment No. 16 that:

Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy … In the view of the Committee this right is required to be guaranteed against all such interferences … whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.

Many of the obligations imposed on Australia by Article 17 of the ICCPR are relevant to the COVIDSafe app. For example, in General Comment No. 16 at [10], the HRC commented that:

The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the [ICCPR]. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files…

Australia's domestic laws must be consistent with its obligations under international human rights law.

Limitations

Like most human rights, the right to privacy under the ICCPR can sometimes be limited.

Article 17 only prohibits 'unlawful' and 'arbitrary' interferences with privacy. Therefore, an interference with privacy that is neither unlawful nor arbitrary is permitted under the ICCPR.

As to the meaning of 'unlawful' and 'arbitrary', the HRC has commented in General Comment No. 16 that:

3. The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the [ICCPR].

4. The expression "arbitrary interference" is also relevant to the protection of the right provided for in article 17. In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the [ICCPR] and should be, in any event, reasonable in the particular circumstances.

The HRC has interpreted the requirement of reasonableness to imply that any interference with privacy must be proportional to the end sought and must be necessary in the circumstances.

Accordingly, the right to privacy under the ICCPR can be limited in circumstances where the interference with privacy is lawful, reasonable, necessary and proportionate to a legitimate end that is being sought. Although Article 17 does not explicitly specify which ends are to be considered legitimate, it is likely that an interference with privacy that aims to protect public health and the rights of others would satisfy this requirement.

Does the COVIDSafe app raise any privacy issues under international human rights law?

The COVIDSafe app, and the collection, use, disclosure and storage of its data, will be inconsistent with Australia's obligations under international human rights law to the extent that any interference with privacy is 'unlawful' or 'arbitrary'.

Unlawfulness (in the sense contemplated by the ICCPR) is unlikely to be an issue in the current circumstances as the legislative framework regulating the COVIDSafe app and its data appears to be sufficiently accessible and precise.

Nevertheless, a lawful interference with privacy may still be inconsistent with the ICCPR if the interference is 'arbitrary'.

The following three considerations will be of ongoing relevance in assessing whether any interference with privacy associated with the COVIDSafe app is 'arbitrary'.

Effectiveness

An intrusion into privacy that is ineffective in achieving its goals is likely to constitute an arbitrary interference.

Accordingly, if evidence were to emerge that the COVIDSafe app is unable to achieve its aims, then that would indicate an arbitrary interference with privacy.

Criticisms regarding the functionality of the app on iPhones have already been reported.

However, even if those issues were to be resolved, the efficacy of the COVIDSafe app, and the collection, use, disclosure and storage of its data, should be regularly and independently measured and monitored. That is especially important because ineffectiveness is one of the legislative triggers for ending the use of the COVIDSafe app and its data under the newly inserted sections 94P and 94Y of the Privacy Act. Indeed, the explanatory memorandum to the Amending Act at [156] confirms that section 94Y 'is intended to ensure that the COVIDSafe app is only used for so long as it is a proportionate response to prevent or control COVID-19'.

The reporting requirements of the Health Minister and Information Commissioner will be important in this regard.

Consent

The provision of consent reduces the interference with privacy.

The practical operation of the COVIDSafe app, and its legislative framework, depend heavily on the consent of users. For example, users must choose to download the app in the first instance, they must choose to register, they must consent to the collection of their data, they must turn their device on for the app to operate, they must consent to uploading their data to the National COVIDSafe Data Store in the event that they test positive for COVID-19, and the app can be deleted at any time. The legislation also heavily penalises conduct that would undermine the quality of a user's consent.

As a result, it is unlikely that any current interference with privacy will be arbitrary.

However, if the existing safeguards were to be diluted or removed, then the risk of arbitrariness would increase.

Use for ulterior purposes

The Australian government has gone to great lengths to reassure the public that the COVIDSafe app and its data will only be used for the purpose of combatting COVID-19.

Those sentiments are reflected in the legislative framework. For example, the newly inserted section 94D(2) of the Privacy Act permits the collection, use or disclosure of COVIDSafe app data only for prescribed purposes, and only to the extent required for those purposes. Additionally, the explanatory memorandum to the Amending Act suggests at [78] and [171] that the newly inserted section 94ZD is intended to ensure that powers in the enabling legislation of law enforcement, intelligence or other regulatory bodies cannot override the protections contained in the COVIDSafe app's own legislative framework.

It is essential that guarantees of this sort remain intact.

The intrusion into privacy would be significantly greater, and the likelihood of arbitrariness would substantially increase, in the event that the COVIDSafe app and its data were to become useable for ulterior purposes.

Other potential human rights issues

The COVIDSafe app may also give rise to human rights issues beyond those relating to privacy.

For example:

- Should the identity of a COVIDSafe user become ascertainable, there arises a risk of discrimination contrary to international human rights law.
- In the event that a human right (e.g. the right to privacy under the ICCPR) is violated, individuals must have access to an effective remedy. A State's failure to ensure such access is itself inconsistent with international human rights law.
- The COVIDSafe app is fundamentally a response to a public health crisis. Therefore, any problem with the app or its data may agitate the human right to the enjoyment of the highest attainable standard of health.

Currently, the use of the COVIDSafe app is voluntary. If that feature were to be undermined and, for example, landlords, employers, schools or social security providers could lawfully mandate use of the COVIDSafe app, then many related human rights issues would potentially arise.

This factsheet was prepared by Hall & Wilcox.

For queries, contact Anthony Hallal at Anthony.Hallal@hallandwilcox.com.au or Tamara Charlwood at Tamara.Charlwood@hallandwilcox.com.au