COVID19 tracking app

21 April

AMNESTY Position

The extraordinary response by our society and Government to the COVID19 crisis shows initial signs of flattening the curve. While many of the steps taken by Australia's Governments have been welcome, the announcement of a specific app to trace contact between civilians raises several questions.

Protecting the privacy of all those in Australia is a fundamental right we all share. Measures that violate the right to privacy can degrade trust in public authorities – and in doing so undermine the effectiveness of any public health response. Amnesty International recommends several principles that need to be directly addressed to ensure our right to privacy is protected in any such endeavour:

1. **Consent:** Adoption or downloading of any app must be the free choice of any person in Australia, no third party should be able to mandate use of the application.

2. **De-identification:** Any and all data collected by the app must only be used to trace the spread of the disease and not be identifiable to a particular citizen. All data collected must be non-identifiable and not traceable to an individual.

3. **Data protection**: All data collected, retained or aggregated by the app must be uniquely held by the entity alone. Data must not be shared with any other application on a person's device without pre, prior and informed consent,. That data must also not be shared or attainable by any third entity, other than the relevant state or territory health department. Users who download the app should be encouraged to encrypt their back ups.

4. **Data Transmission:** Any data collected must be secure and transmitted to the relevant health department and stored safely and securely and must not be scraped or collected by any other parties.

5. **Safe and Secure**: Any tracking of data through the COVID-19 app must only be used for the intended purpose of improving traceability of the spread of the disease. The data must not be shared with any other department, including law enforcement and national security agencies, nor available to any other third party not part of the agreement, either through the data collection repository, nor through individual

engagement with a law enforcement official. Data must not be used for commercial purposes.

6. **Independent oversight:** The collection and use of data should be independently overseen and regulated. An independent oversight mechanism must be able to scrutinize the full range of human rights impacts, beyond data protection and privacy. The watchdog should be able to access data and algorithms, be empowered to issue binding rulings, and be funded in a manner commensurate to the task.

7. **Sunset Clause:** Any data collected must be destroyed at the conclusion of the current pandemic, as determined by the public health authorities, and not used for any other purpose.