Law Council
OF AUSTRALIA

Law Council of Australia
Principles for the design of a COVID-19 contact tracing app
April 2020

1. Clear governing legal and administrative frameworks

Principles:

- The applicable laws governing the operation of the app must be identified and communicated clearly, as must the individual entities responsible for its administration. The applicable administrative policies should be made available to the public.
- If the app is to be implemented by suspending any general requirements of applicable privacy laws, this approach must be acknowledged and justified rigorously. Eg, if there is an intention to declare a state of emergency under the *Privacy Act 1988* (Cth).
- The regime should be established legislatively, to set clear, certain and stable legal parameters that cannot be removed or amended by unilateral executive action. Those parameters should provide for all of the following matters:
    - the matters set out under principles (2)-(9) below; and
    - the maximum period in which the app will operate; and
    - principles of non discrimination, and in particular, a guarantee that the laws governing the use of the app are not intended to override the operation of any Commonwealth, State or Territory anti-discrimination laws (which prohibit discrimination on the grounds of age, race, ethic origin, nationality, gender, sexual orientation and disability); and
    - specific provision for the obligations of third party contracted service providers who may be engaged to support the delivery of the app, and who may have access to personal information collected by the app. This should include specific obligations with respect to the notification of data breaches.
- The implementation of the framework should also be subject to adequate safeguards and independent oversight to ensure that the app is not used in a way which discriminates against any person on the basis of the matters prohibited by anti-discrimination laws, as well as on the basis of poverty or homelessness.
- An exposure draft Bill should be released as soon as practicable, to provide the public and civil society groups with an opportunity to comment before a Bill is introduced to and passed by the Australian Parliament. The extrinsic materials to an exposure draft Bill should include a Privacy Impact Analysis and the source code for the app.

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639 • *Email* mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601 • DX 5719 Canberra • 19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Law Council
OF AUSTRALIA

2. A voluntary, 'opt-in' model, which obtains users' informed consent to the collection of their personal information, and enables users to 'opt out' at any time

Principles:

- Use of the app must be voluntary throughout its period of use. In particular:
    - the app should apply an 'opt in' model whereby individual users must specifically download the app and expressly consent to its use, including any continuous background operation on a device; and
    - there must be readily accessible means for users to 'opt out' at any time (eg, a functionality for user 'de-registration') and a clear explanation of what will happen to any data collected by the app before the person 'opted out'; and
    - use of the app must not be prescribed as a condition to the availability of exceptions to 'stay-at-home' directions under health or emergency legislation, or as a condition to a person's attendance at their workplace or educational institution or public places.
- The app must seek, and obtain, the informed consent of users to the collection, use, handling and dissemination of their personal information, prior to its installation and operation on a device.
- The app must include adequate arrangements for obtaining the informed consent of persons who lack legal capacity to give personal consent, including minors.
- The source code for the app should be released publicly, to give all prospective users an opportunity to examine it as part of their decision-making about whether to consent.
- The app must include adequate arrangements to notify and seek further consent from users for any updates that change the parameters for the collection, use, handling and dissemination of their personal information. This includes changes to the parameters for the identification and recording of close contacts, and changes to the data security standards for data held on a user's device or on Australian Government servers.
- The app must include clear and accessible arrangements for any users to 'opt out' of the app if they do not wish to consent to any changes, before they are installed.

3. Limitations on the collection of users' personal information to what is strictly necessary for the purpose of contract tracing

Principles:

- The app must only collect the minimum amount of data that is necessary to perform contact tracing of persons who test positive for COVID-19. There should be a public justification of why it is necessary to collect each piece of personal information.
- The information to be collected, the purpose of its collection and how it will be used must be identified clearly and precisely to users before their consent is obtained to the use of the app.
- Data on contacts between individual persons must be stored in accordance with relevant encryption standards locally on a user's device. It must not be transmitted to Commonwealth data servers unless and until a person tests positive for COVID-19.

Law Council
OF AUSTRALIA

4. Security of information held on Australian Government data servers

Principles:

- Information must only be transmitted, in encrypted form, to Australian Government data servers if a person tests positive to COVID19, for the sole purpose of the Australian Government transmitting it to the relevant State or Territory health agency.
- The Australian Government must not decrypt the data held on its servers.
- The Australian Government must ensure that the storage of the data on its servers complies with the information security requirements of the Commonwealth Protective Security Policy Framework, including the requirement to safeguard information from cyber threats. This should be publicly certified by a competent entity such as the Australian Signals Directorate.
- There should be a public explanation of why a centralised data storage model has been adopted. This explanation should address the perceived costs and benefits of centralised data storage, relative to a decentralised data storage model.

See further, key areas (6) and (8) below in relation to secondary use and deletion

5. Limitations on access to personal information by States and Territories to what is strictly necessary for the sole purpose of contact tracing

Principles:

- Personal information should only be transmitted to States and Territories if a user of the app has tested positive to COVID19, and specifically authorises the disclosure of data collected by the app and stored on their device.
- State and Territory health agencies should not be permitted to undertake data matching from information held on Australian Government data servers.

See further, key areas (6) and (8) below in relation to secondary use and deletion

6. Prohibition on any secondary use and disclosure of personal information obtained from the app, for purposes other than contact tracing

Principles

- There should be a prohibition on **any** secondary use or disclosure of personal information collected by the app for purposes other than contact tracing.
- This prohibition should be implemented legislatively, to ensure that it is legally effective and is not vulnerable to repeal or amendment by unilateral executive action.
- The basis for this prohibition is the strong public interest in the uptake of the app for the purpose of responding to a public health emergency. This interest necessitates the removal of disincentives to individual participation that may arise from existing laws that would otherwise apply to authorise secondary use and disclosure for other purposes, such as law enforcement or intelligence collection.

Law Council
OF AUSTRALIA

Principle 6 (ctd) prohibition on any secondary use and disclosure

- The prohibition should apply to secondary use or disclosure by Commonwealth, State or Territory agencies who have lawful possession, custody or control of personal information collected by the app. It should also apply to any subsequent use or disclosure by third parties who have received information unlawfully or by mistake.
- The prohibition should override all existing laws that would otherwise apply to permit secondary use and disclosure of personal information collected by the app. It is particularly important that the prohibition overrides the following:
    - Australian Privacy Principle 6.2(e) which can permit disclosures to law enforcement agencies (and, for the avoidance of doubt, use and derivative use immunities in relation to information collected by the app); and
    - any voluntary disclosures to, and by, entities whose acts and practices are not regulated by the Commonwealth, State or Territory Privacy Acts, such as intelligence agencies (for example, ASIO); and
    - any laws under which a warrant or another form of specific authorisation could be issued to authorise an entity to gain access to the information. (For example, computer access warrants, search warrants, authorisations to access telecommunications data, and notice-based compulsory production and access powers available to law enforcement and intelligence agencies including Part 15 of the Telecommunications Act 1997.)

7. Robust and appropriately resourced independent oversight, including complaints resolution, breach enforcement and compensation rights

Principles:

- The use of the app should be subject to independent oversight by Commonwealth, State and Territory Privacy Commissioners, in accordance with the complaints, investigation and enforcement mechanisms under relevant privacy legislation.
- Governments of all levels should consult their respective Privacy Commissioners about the adequacy of their resources to perform oversight of the app, and should commit to ensuring that the Commissioners are adequately resourced for this task.
- Consideration should be given to the availability and adequacy of statutory compensation for persons whose personal information collected by the app is disclosed or used in breach of Commonwealth, State or Territory Privacy Acts and specific legislation governing the use of the app (as applicable).
- Governments of all levels should publicly commit to cooperating fully with inquiries of Parliamentary Committees and independent oversight agencies concerning their involvement in the development and operation of the app.

Law Council
OF AUSTRALIA

8. Requirements for the deletion of personal information and independent assurance

Principles:

- There must be requirements for the deletion of personal information in the following circumstances:
    - The app should delete contact data stored on a device after the expiry of a prescribed period (eg, 21 days). The period should be determined and publicly justified by reference to epidemiological standards, such as the length of time a person with COVID-19 is infectious. (This period should also apply if a person 'opts out' of the app, so that stored data can be retained for the prescribed period, should a person test positive at or around the time they 'opt out')
    - When contact tracing has been completed for a person who has tested positive to COVID-19, the data about their contacts should be deleted from Australian Government data servers and the records of State and Territory agencies. There should be a prescribed period within which data this must be deleted.
    - On the expiry of the prescribed period of operation for the app, the app should cease to collect data, and all data must be deleted from Australian Government data servers and State and Territory records. There should be a prescribed period within which this data must be deleted.
- The prescribed periods in which data must be deleted may include a reasonable period of time in which personal information may be used for the purpose of being de-identified (for example, anonymised or aggregated) so that the de-identified data can be used in accordance with principle 9 below. This period should be no longer than is necessary, and that period should be specifically identified and justified.
- Compliance with the deletion requirements must be subject to independent assurance, for example, by Commonwealth, State and Territory Privacy Commissioners. The public should be informed of the outcomes of these assurance checks.

9. De-identification of personal information

Principles:

- The de-identification of personal information obtained from the app should be permitted for designated purposes connected with the public health response to COVID-19, or public health responses to pandemics more generally. This should cover activities of the following kind:
    - collecting and analysing statistical or other aggregated information about the incidence and transmission of COVID-19;
    - identifying patterns or trends in community transmission (for example, potential 'hotspots' for infection and community transmission);
    - planning and delivering healthcare treatment or prevention activities, or other forms of support services for infected or at-risk persons;
    - monitoring and evaluating the effectiveness of contact tracing activities; and
    - research relating to COVID-19, contact tracing for communicable diseases, or other similar subjects.