Privacy Amendment (Public Health Contact Information) Bill 2020

No. , 2020

(Attorney-General)

A Bill for an Act to amend the Privacy Act 1988, and for related purposes
## Contents

1. Short title .......................................................... 1  
2. Commencement ...................................................... 1  
3. Schedules ............................................................ 2  

### Schedule 1—Amendments  
*Privacy Act 1988*  
3  

### Schedule 2—Repeals  
*Privacy Act 1988*  
20
A Bill for an Act to amend the Privacy Act 1988, and for related purposes

The Parliament of Australia enacts:

1 Short title

This Act is the Privacy Amendment (Public Health Contact Information) Act 2020.

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.
### Commencement information

<table>
<thead>
<tr>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisions</td>
<td>Commencement</td>
<td>Date/Details</td>
</tr>
<tr>
<td>1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table</td>
<td>The day this Act receives the Royal Assent.</td>
<td></td>
</tr>
<tr>
<td>2. Schedule 1</td>
<td>The day after this Act receives the Royal Assent.</td>
<td></td>
</tr>
<tr>
<td>3. Schedule 2</td>
<td>At the end of 90 days after the day determined under subsection 94Y(1) of the Privacy Act 1988 as amended by this Act.</td>
<td></td>
</tr>
</tbody>
</table>

1. Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

2. Any information in column 3 of the table is not part of this Act.

3. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

### Schedules

4. Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.
Schedule 1—Amendments

Privacy Act 1988

1 Subsection 6(1)

Insert:

contact tracing has the meaning given by subsection 94D(6).

COVID app data has the meaning given by subsection 94D(5).

COVIDSafe means an app that is made available or has been made available (including before the commencement of this Part), by or on behalf of the Commonwealth, for the purpose of facilitating contact tracing.

COVIDSafe user, in relation to a mobile telecommunications device, means the person whose registration data was uploaded from the device when the user was registered through COVIDSafe.

data store administrator means:

(a) for the purposes of a provision of Part VIIIA specified in a determination under section 94Z—the agency specified in that determination (but not to the extent of any limitation in that determination); or

(b) otherwise—the Health Department.

former COVIDSafe user has the meaning given by subsection 94N(2).

Health Department has the same meaning as in the Biosecurity Act 2015.

Health Minister means the Minister administering the National Health Act 1953.

in contact: a person has been in contact with another person if the operation of COVIDSafe in relation to the person indicates that the person may have been in the proximity of the other person.
Schedule 1  Amendments

*mobile telecommunications device* means an item of customer equipment (within the meaning of the *Telecommunications Act 1997*) that is used, or is capable of being used, in connection with a public mobile telecommunications service (within the meaning of that Act).

*National COVIDSafe Data Store* means the database administered by or on behalf of the Commonwealth for the purpose of contact tracing.

*registration data*, of a person, means the information about the person that was uploaded from a mobile telecommunications device when the person was registered through COVIDSafe.

*State or Territory health authority* means the State or Territory authority responsible for the administration of health services in a State or Territory.

*State or Territory privacy authority* means a State or Territory authority that has functions to protect the privacy of individuals (whether or not the authority has other functions).

2  After Part VIII

Insert:

Part VIII A—Public health contact information

Division 1—Preliminary

94A  Simplified outline of this Part

There are several serious offences relating to COVID app data and COVIDSafe. They deal with:

• non-permitted collection, use or disclosure relating to COVID app data; and

• uploading relating to COVID app data without consent; and

• retaining or disclosing uploaded data outside Australia; and
94B Object of this Part

The object of this Part is to assist in preventing and controlling the entry, emergence, establishment or spread of the coronavirus known as COVID-19 into Australia or any part of Australia by providing stronger privacy protections for COVID app data and COVIDSafe users in order to:

(a) encourage public acceptance and uptake of COVIDSafe; and

(b) enable faster and more effective contact tracing.

94C Additional constitutional bases of this Part

Without limiting section 12B, this Part also relies on:
Schedule 1
Amendments

(a) the Commonwealth’s legislative powers under paragraph 51(xi) (quarantine) of the Constitution; and

(b) the Commonwealth’s legislative powers with respect to matters that are peculiarly adapted to the government of a nation and cannot otherwise be carried out for the benefit of the nation; and

(c) the Commonwealth’s legislative powers under paragraph 51(xxxix) (matters incidental) of the Constitution.

Division 2—Offences relating to COVID app data and COVID safe

94D Collection, use or disclosure of COVID app data

(1) A person commits an offence if:

(a) the person collects, uses or discloses data; and

(b) the data is COVID app data; and

(c) the collection, use or disclosure is not permitted under this section.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

(2) The collection, use or disclosure is permitted if:

(a) the person is employed by, or in the service of, a State or Territory health authority, and the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing; or

(b) the person is an officer, employee or contractor of the data store administrator, and the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of:

(i) enabling contact tracing by persons employed by, or in the service of, State or Territory health authorities; or

(ii) ensuring the proper functioning, integrity or security of COVIDSafe or of the National COVIDSafe Data Store; or

(c) in the case of a collection or disclosure of COVID app data—

the collection or disclosure is for the purpose of, and only to the extent required for the purpose of:
(i) transferring encrypted data between mobile telecommunications devices through COVIDSafe; or

(ii) transferring encrypted data, through COVIDSafe, from a mobile telecommunications device to the National COVIDSafe Data Store; or

(d) the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of, the Commissioner performing the functions or exercising the powers of the Commissioner under or in relation to this Part; or

(e) the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of:

(i) investigating whether this Part has been contravened; or

(ii) prosecuting a person for an offence against this Part; or

(f) in the case of a use of COVID app data by the data store administrator—the use is for the purpose of, and only to the extent required for the purpose of, producing de-identified statistical information about the total number of registrations through COVIDSafe.

Subsection (1) does not apply to the collection of COVID app data if:

(a) the collection of the COVID app data;

(i) occurs as part of the collection, at the same time, of data that is not COVID app data (non-COVID app data); and

(ii) is incidental to the collection of the non-COVID app data; and

(b) the collection of the non-COVID app data is permitted under an Australian law; and

(c) the COVID app data:

(i) is deleted as soon as practicable after the person becomes aware that it had been collected; and

(ii) is not otherwise accessed, used or disclosed by the person after it was collected.

Note: A defendant bears an evidential burden in relation to the matters in subsection (3); see subsection 13.3(3) of the Criminal Code.
(4) The admissibility of the non-COVID app data as evidence in any proceedings is not affected by the incidental collection or subsequent deletion of the COVID app data as required by subparagraph (3)(c)(i).

(5) **COVID app data** is data relating to a person that:

(a) has been collected or generated (including before the commencement of this Part) through the operation of COVIDSafe; and

(b) is stored, or has been stored (including before the commencement of this Part), on a mobile telecommunications device.

However, it does not include:

(c) information obtained, from a source other than directly from the National COVIDSafe Data Store, in the course of undertaking contact tracing by a person employed by, or in the service of, a State or Territory health authority; or

(d) information that is de-identified.

(6) **Contact tracing** is the process of identifying persons who have been in contact with a person who has tested positive for the coronavirus known as COVID-19, and includes:

(a) notifying a person that the person has been in contact with a person who has tested positive for the coronavirus known as COVID-19; and

(b) notifying a person who is a parent, guardian or carer of another person that the other person has been in contact with a person who has tested positive for the coronavirus known as COVID-19; and

(c) providing information and advice to a person who:

(i) has tested positive for the coronavirus known as COVID-19; or

(ii) is a parent, guardian or carer of another person who has tested positive for the coronavirus known as COVID-19; or

(iii) has been in contact with a person who has tested positive for the coronavirus known as COVID-19; or
(iv) is a parent, guardian or carer of another person who has been in contact with a person who has tested positive for the coronavirus known as COVID-19.

94E COVID app data on mobile telecommunications devices

A person commits an offence if:

(a) the person uploads, or causes to be uploaded, data from a mobile telecommunications device to the National COVIDSafe Data Store; and

(b) the data is COVID app data; and

(c) consent to the upload has not been given by:

(i) the COVIDSafe user in relation to that device; or

(ii) if the COVIDSafe user is unable to give consent—a parent, guardian or carer of the COVIDSafe user; or

(iii) if the COVIDSafe user has requested a parent, guardian or carer of the COVIDSafe user to act on the COVIDSafe user’s behalf—that parent, guardian or carer.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

94F COVID app data in the National COVIDSafe Data Store

(1) A person commits an offence if:

(a) the person retains data on a database outside Australia; and

(b) the data is COVID app data that has been uploaded from a mobile telecommunications device to the National COVIDSafe Data Store.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

(2) A person commits an offence if:

(a) the person discloses data to another person outside Australia; and

(b) the data is COVID app data that has been uploaded from a mobile telecommunications device to the National COVIDSafe Data Store; and

(c) the person is not a person who:
Schedule 1  Amendments

(i) is employed by, or in the service of, a State or Territory health authority; and
(ii) discloses the data for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

94G Decrypting COVID app data

A person commits an offence if:
(a) the person decrypts encrypted data; and
(b) the data is COVID app data that is stored on a mobile telecommunications device.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

94H Requiring the use of COVIDSafe

(1) A person commits an offence if the person requires another person to:
(a) download COVIDSafe to a mobile telecommunications device; or
(b) have COVIDSafe in operation on a mobile telecommunications device; or
(c) consent to uploading COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

(2) A person commits an offence if the person:
(a) refuses to enter into, or continue, a contract or arrangement with another person (including a contract of employment); or
(b) takes adverse action (within the meaning of the Fair Work Act 2009) against another person; or
(c) refuses to allow another person to enter:
   (i) premises that are otherwise accessible to the public; or
   (ii) premises that the other person has a right to enter; or
(d) refuses to allow another person to participate in an activity;  
or  
(e) refuses to receive goods or services from another person; or  
(f) refuses to provide goods or services to another person;  
on the ground that, or on grounds that include the ground that, the  
other person:  
(g) has not downloaded COVIDSafe to a mobile  
telecommunications device; or  
(h) does not have COVIDSafe in operation on a mobile  
telecommunications device; or  
(i) has not consented to uploading COVID app data from a  
mobile telecommunications device to the National  
COVIDSafe Data Store.

Penalty:  Imprisonment for 5 years or 300 penalty units, or both.

**94J  Extended geographical jurisdiction for offences**

Section 15.1 (extended geographical jurisdiction—category A) of the *Criminal Code* applies to all offences against this Division.

**Division 3—Other obligations relating to COVID app data and COVIDSafe**

**94K  COVID app data not to be retained**

The data store administrator must take all reasonable steps to ensure that COVID app data is not retained on a mobile telecommunications device:

(a) for more than 21 days; or  
(b) in any case in which it is not possible to comply with  
paragraph (a) within 21 days—for longer than the shortest  
practicable period.

**94L  Deletion of registration data on request**

(1) If the COVIDSafe user in relation to a mobile telecommunications device, or a parent, guardian or carer of that person, requests the data store administrator to delete any registration data of the person
Schedule 1  Amendments

that has been uploaded from the device to the National COVIDSafe Data Store, the data store administrator:

(a) must take all reasonable steps to delete the data from the National COVIDSafe Data Store as soon as practicable; and

(b) if it is not practicable to delete the data immediately—must not use or disclose the data for any purpose.

(2) A request under subsection (1) may only be made by a parent, guardian or carer of the COVIDSafe user if:

(a) the COVIDSafe user is unable to make a request under subsection (1); or

(b) the COVIDSafe user has requested that parent, guardian or carer to act on the COVIDSafe user’s behalf.

(3) Subsection (1) does not:

(a) prevent the data store administrator from accessing data for the purpose of, and only to the extent required for the purpose of, confirming that the correct data is being deleted; or

(b) require the data store administrator to delete from the National COVIDSafe Data Store data relating to the person that:

(i) was uploaded from another mobile telecommunications device in relation to which another person is a COVIDSafe user; and

(ii) was collected through the other device interacting with the device mentioned in subsection (1).

(4) This section does not apply to data that is de-identified.

94M Deletion of data received in error

A person who receives COVID app data in error must, as soon as practicable:

(a) delete the data; and

(b) notify the data store administrator that the person received the data.
94N Effect of deletion of COVIDSafe from a mobile telecommunications device

(1) The data store administrator must not collect from a person, through a particular mobile telecommunications device, COVID app data relating to the person if the person is a former COVIDSafe user in relation to that device.

(2) A person is a former COVIDSafe user, in relation to a mobile telecommunications device, at a particular time if:
   (a) COVIDSafe has been deleted from the device in relation to which the person was the COVIDSafe user; and
   (b) after COVIDSafe was last deleted from that device—COVIDSafe has not been downloaded to that device.

94P Obligations after the end of the COVIDSafe data period

(1) After the end of the day determined under subsection 94Y(1), the data store administrator must not:
   (a) collect any COVID app data; or
   (b) make COVIDSafe available to be downloaded.

(2) As soon as reasonably practicable after the end of the day determined under subsection 94Y(1), the data store administrator must:
   (a) delete all COVID app data from the National COVIDSafe Data Store; and
   (b) after the deletion, take all reasonable steps to inform all COVIDSafe users (other than former COVIDSafe users) in relation to mobile telecommunications devices that:
      (i) all COVID app data has been deleted from the National COVIDSafe Data Store; and
      (ii) COVID app data can no longer be collected; and
      (iii) they should delete COVIDSafe from their mobile telecommunications devices.
Schedule 1  Amendments

Division 4—Application of general privacy measures

94Q COVID app data is taken to be personal information

COVID app data relating to an individual is taken, for the purposes of this Act, to be personal information about the individual.

94R Breach of requirement is an interference with privacy

(1) An act or practice in breach of a requirement of this Part in relation to an individual constitutes an act or practice involving an interference with the privacy of the individual for the purposes of section 13.

Note: The act or practice may be the subject of a complaint under section 36.

(2) Subsection (1) applies despite subsections 7(1A) and (1B).

94S Breach of requirement may be treated as an eligible data breach

(1) For the purposes of this Act, if the data store administrator, or a State or Territory health authority, breaches a requirement of this Part in relation to COVID app data:

(a) the breach is taken to be an eligible data breach; and

(b) an individual to whom the data relates is taken to be at risk from the eligible data breach.

(2) Part IIIC applies in relation to such a breach as if:

(a) subsection 26WE(3) and sections 26WF, 26WH and 26WJ did not apply in relation to the breach; and

(b) Subdivision B of Division 3 of that Part:

(i) required the data store administrator, or State or Territory health authority, to notify the Commissioner that there were reasonable grounds to believe that there had been an eligible data breach; and

(ii) only required compliance with sections 26WK and 26WL in relation to the breach if the Commissioner required the administrator or authority so to comply; and

(c) sections 26WN, 26WP, 26WQ, 26WS and 26WT did not apply in relation to the breach.
(3) Without limiting the circumstances in which the Commissioner may, under subparagraph (2)(b)(ii), require the administrator or authority so to comply, the Commissioner must so require if:

(a) the Commissioner is satisfied that the breach may be likely to result in serious harm to any of the individuals to whom the information relates; and

(b) subsection (4) does not apply.

(4) The Commissioner may decide not to require compliance, or to allow an extended period for compliance, if the Commissioner is satisfied on reasonable grounds that requiring compliance, or requiring compliance within the ordinary period for compliance, would not be reasonable in the circumstances, having regard to the following:

(a) the public interest;

(b) any relevant advice given to the Commissioner by:

(i) an enforcement body; or

(ii) the Australian Signals Directorate;

(c) such other matters (if any) as the Commissioner considers relevant.

(5) Paragraph (4)(b) does not limit the advice to which the Commissioner may have regard.

94T Commissioner may conduct an assessment relating to COVID app data

(1) The Commissioner’s power under section 33C to conduct an assessment includes the power to conduct an assessment of whether the acts or practices of an entity or a State or Territory authority in relation to COVID app data comply with this Part.

(2) Without limiting subsection 33C(2), if:

(a) the Commissioner is conducting under that subsection an assessment of a matter of a kind mentioned in subsection (1) of this section; and

(b) the Commissioner has reason to believe that an entity or a State or Territory authority being assessed has information or a document relevant to the assessment;
the Commissioner may, by written notice, require the entity or
authority to give the information or produce the document within
the period specified in the notice, which must not be less than 14
days after the notice is given to the entity or authority.

Note: For a failure to give information etc., see section 66.

94U Investigation under section 40 to cease if COVID data offence
may have been committed

(1) This section applies if, in the course of an investigation under
section 40, the Commissioner forms the opinion that:

(a) an offence against Division 2 of this Part; or
(b) an offence against section 6 of the Crimes Act 1914, or
section 11.1, 11.2, 11.4 or 11.5 of the Criminal Code, being
an offence that relates to an offence against that Division;

may have been committed.

(2) The Commissioner must:

(a) inform the Commissioner of Police or the Director of Public
Prosecutions of that opinion; and

(b) in the case of an investigation under subsection 40(1), give a
copy of the complaint to the Commissioner of Police or the
Director of Public Prosecutions, as the case may be; and

(c) subject to subsection (3) of this section, discontinue the
investigation except to the extent that it concerns matters
unconnected with the offence that the Commissioner believes
may have been committed.

(3) If the Commissioner of Police or the Director of Public
Prosecutions:

(a) has been informed of the Commissioner’s opinion under
paragraph (2)(a); and

(b) decides that the matter will not be, or will no longer be, the
subject of proceedings for an offence;

the Commissioner of Police or the Director of Public Prosecutions,
as the case requires, must give a written notice to that effect to the
Commissioner.

(4) Upon receiving such a notice the Commissioner may continue the
investigation discontinued under paragraph (2)(c).
94V Referring COVID data matters to State or Territory privacy authorities

(1) If:

(a) a complaint has been made under section 36 about an act or practice that may involve a breach of a requirement of this Part; and

(b) before the Commissioner commences, or after the Commissioner has commenced, to investigate the matter, the Commissioner forms the opinion that:

(i) the complainant has made, or could have made, a complaint relating to that matter to a State or Territory privacy authority; and

(ii) that matter could be more conveniently or effectively dealt with by that State or Territory authority;

the Commissioner may decide not to investigate the matter, or not to investigate the matter further.

(2) If the Commissioner so decides, the Commissioner must:

(a) transfer the complaint to that State or Territory authority; and

(b) give notice in writing to the complainant stating that the complaint has been so transferred; and

(c) give to that State or Territory authority any information or documents that relate to the complaint and are in the possession, or under the control, of the Commissioner.

(3) A complaint transferred under subsection (2) is taken, for the purposes of this Act, to have been made to that State or Territory authority.

94W Commissioner may share information with State or Territory privacy authorities

(1) Subject to subsection (2), the Commissioner may share information or documents with a State or Territory privacy authority:

(a) for the purpose of the Commissioner exercising powers, or performing functions or duties under this Act in relation to the requirements of this Part; or

(b) for the purpose of the State or Territory privacy authority exercising its powers, or performing its functions or duties.
(2) The Commissioner may only share information or documents with a receiving body under this section if:

(a) the information or documents were acquired by the Commissioner in the course of exercising powers, or performing functions or duties, under this Act; and

(b) the Commissioner is satisfied on reasonable grounds that the receiving body has satisfactory arrangements in place for protecting the information or documents.

(3) To avoid doubt, the Commissioner may share information or documents with a State or Territory privacy authority under this section whether or not the Commissioner is transferring a complaint or part of a complaint to the body.

94X Application to State or Territory health authorities

This Act applies in relation to a State or Territory health authority, as if the authority were an organisation, to the extent that the authority deals with, or the activities of the authority relate to, COVID app data.

Division 5—Miscellaneous

94Y Determining the end of the COVIDSafe data period

(1) Subject to subsection (2), the Health Minister must, by notifiable instrument, determine a day if the Health Minister is satisfied that, by that day, use of COVIDSafe:

(a) is no longer required to prevent or control; or

(b) is no longer likely to be effective in preventing or controlling;

the entry, emergence, establishment or spread of the coronavirus known as COVID-19 into Australia or any part of Australia.

(2) The Health Minister must not make a determination under subsection (1) unless the Health Minister has consulted, or considered recommendations from, the Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee.
(3) The Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee may recommend to the Health Minister that the Health Minister make a determination under subsection (1).

94Z Agencies may be determined to be data store administrator

(1) The Secretary of the Health Department may, by notifiable instrument, determine that a particular agency is the data store administrator for the purposes of one or more provisions of this Part specified in the determination.

(2) The determination may limit the extent to which the agency is the data store administrator for those purposes.

94ZA COVID App data remains property of the Commonwealth

COVID App data is the property of the Commonwealth, and remains the property of the Commonwealth even after it is disclosed to, or used by:

(a) a State or Territory health authority; or

(b) any other person or body (other than the Commonwealth an authority of the Commonwealth).

94ZB Operation of other laws

(1) This section cancels the effect of a provision of any Australian law (other than this Part) that, but for this section, would have the effect of permitting or requiring conduct, or an omission to act, that would otherwise be prohibited under this Part.

(2) However, the cancellation does not apply to a provision of an Act if the provision:

(a) commences after this Part commences; and

(b) expressly permits or requires the conduct or omission despite the provisions of this Part.
Schedule 2—Repeals

Note: The repeals made by this Schedule commence at the end of 90 days after the day determined under subsection 94Y(1) of the Privacy Act 1988 as amended by this Act.

Privacy Act 1988

1 Subsection 6(1)

Repeal the following definitions:

(a) definition of contact tracing;
(b) definition of COVID app data;
(c) definition of COVIDSafe;
(d) definition of COVIDSafe user;
(e) definition of data store administrator;
(f) definition of former COVIDSafe user;
(g) definition of Health Department;
(h) definition of Health Minister;
(i) definition of in contact;
(j) definition of mobile telecommunications device;
(k) definition of National COVIDSafe Data Store;
(l) definition of registration data;
(m) definition of State or Territory health authority;
(n) definition of State or Territory privacy authority.

2 Part VIII A

Repeal the Part.