Privacy Amendment (Public Health Contact Information) Act 2020

No. 44, 2020

An Act to amend the *Privacy Act 1988*, and for related purposes

Note: An electronic version of this Act is available on the Federal Register of Legislation (https://www.legislation.gov.au/)

Contents

1 Short title 1
2 Commencement 2
3 Schedules 2

Schedule 1—Amendments 3

Privacy Act 1988 3

Schedule 2—Repeals 24

Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020 24

Privacy Act 1988 24

Privacy Amendment (Public Health Contact Information) Act 2020

No. 44, 2020

An Act to amend the *Privacy Act 1988*, and for related purposes

[*Assented to 15 May 2020*]

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

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	15 May 2020
2. Schedule 1	The day after this Act receives the Royal Assent.	16 May 2020
3. Schedule 2, item 1	The day after this Act receives the Royal Assent.	16 May 2020
4. Schedule 2, items 2 to 4	At the end of 90 days after the day determined under subsection 94Y(1) of the *Privacy Act 1988* as amended by this Act.	

Note: This table relates only to the provisions of this Act as originally enacted.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. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.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

communication device means an item of customer equipment (within the meaning of the *Telecommunications Act 1997*).

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 communication 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 means the Department administered by the Health Minister.

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.

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 communication 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 VIIIA—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 COVID app data without consent; and
- retaining or disclosing uploaded data outside Australia; and
- decrypting encrypted COVID app data; and
- requiring participation in relation to COVIDSafe.

Other specific obligations relate to deletion of data and what is to happen after the COVIDSafe data period has ended (as determined by the Health Minister).

The general privacy law provided by this Act is applied to the requirements of this Part, in particular by:

- ensuring that COVID app data is taken to be personal information and breaches of this Part are interferences with privacy; and
- enhancing the Commissioner's role in dealing with eligible data breaches, making assessments and conducting investigations in relation to this Part; and
- enabling the Commissioner to refer matters to, and share information or documents with, State or Territory privacy authorities; and
- providing for this Act to apply to State or Territory health authorities in relation to COVID app data.

This Part imposes on State or Territory health authorities the Act's rules and privacy protections, and Commonwealth oversight, in relation to COVID app data, as Commonwealth property that those authorities receive.

This Part also cancels the effect of Australian laws that are inconsistent with the prohibitions in this Part.

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 Constitutional basis of this Part

Principal constitutional basis

(1) This Part relies on the Commonwealth's legislative powers with respect to matters that are peculiarly adapted to the government of a nation and cannot otherwise be carried on for the benefit of the nation.

Additional operation of this Part

(2) In addition to subsection (1), this Part also has effect as provided by subsections (3) to (5).

(3) This Part also has effect as if a reference in this Part to COVID app data were expressly confined to a reference to COVID app data that was collected or generated for the purposes of quarantine (within the meaning of paragraph 51(ix) of the Constitution).

(4) This Part also has effect as if a reference in this Part to COVID app data were expressly confined to a reference to COVID app data that was collected or generated using a service of a kind to which paragraph 51(v) of the Constitution applies (postal, telegraphic, telephonic and other like services).

(5) This Part also has effect as if it were expressly confined to giving effect to Australia's obligations under the International Covenant on Civil and Political Rights done at New York on 16 December 1966 ([1980] ATS 23), and in particular Article 17 of the Covenant, in relation to COVID app data.

Note: The Covenant is set out in Australian Treaty Series 1980 No. 23 ([1980] ATS 23) and could in 2020 be viewed in the Australian Treaties Library on the AustLII website (www.austlii.edu.au).

Division 2—Offences relating to COVID app data and COVIDSafe

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:

(i) an officer or employee of the data store administrator; or

(ii) a contracted service provider for a government contract with 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:

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

(iv) 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 communication devices through COVIDSafe; or

(ii) transferring encrypted data, through COVIDSafe, from a communication 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; or

(g) in the case of a use of COVID app data that the data store administrator is required by section 94L to delete—the use consists of access by the data store administrator for the purpose of, and only to the extent required for the purpose of, confirming that the correct data is being deleted.

(3) 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 this subsection: 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 of the COVID app data, or by the 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) either:

(i) is registration data; or

(ii) is stored, or has been stored (including before the commencement of this Part), on a communication 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) de-identified statistical information about the total number of registrations through COVIDSafe that is produced by:

(i) an officer or employee of the data store administrator; or

(ii) a contracted service provider for a government contract with the data store administrator.

(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 communication devices

A person commits an offence if:

(a) the person uploads, or causes to be uploaded, data from a communication 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 communication 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 who is outside Australia; and

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

(c) the person is not a person who:

(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 communication 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 communication device; or

(b) have COVIDSafe in operation on a communication device; or

(c) consent to uploading COVID app data from a communication 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 insists on providing less monetary consideration for the goods or services; or

(f) refuses to provide goods or services to another person, or insists on receiving more monetary consideration for the goods or services;

on the ground that, or on grounds that include the ground that, the other person:

(g) has not downloaded COVIDSafe to a communication device; or

(h) does not have COVIDSafe in operation on a communication device; or

(i) has not consented to uploading COVID app data from a communication device to the National COVIDSafe Data Store.

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

(3) To avoid doubt:

(a) subsection (2) is a workplace law for the purposes of the *Fair Work Act 2009*; and

(b) the benefit that the other person derives because of an obligation of the person under subsection (2) is a workplace right within the meaning of Part 3-1 of that Act.

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 communication 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 or former COVIDSafe user in relation to a communication device, or a parent, guardian or carer of that person, requests the data store administrator to delete any registration data of the person 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 communication 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 communication device

(1) The data store administrator must not collect from a person, through a particular communication 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 communication 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 delete all COVID app data from the National COVIDSafe Data Store.

(3) As soon as reasonably practicable after the deletion, the data store administrator must:
(a) inform the Health Minister and the Commissioner that all COVID app data has been deleted from the National COVIDSafe Data Store; and
(b) take all reasonable steps to inform all COVIDSafe users (other than former COVIDSafe users) in relation to communication 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 communication devices.

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) Subsections 7(1A) and (1B) do not limit what is taken to be an act or practice for the purposes of subsection (1) of this section, or for the purposes of the application of this Act in relation to an interference with the privacy of an individual involving a breach of a requirement of this Part.

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

(1) For the purposes of this Act, if:
(a) the data store administrator; or
(b) an officer or employee of the data store administrator; or
(c) a contracted service provider for a government contract with the data store administrator;

breaches a requirement of this Part in relation to COVID app data:
(d) the breach is taken to be an eligible data breach by the data store administrator; and
(e) an individual to whom the data relates is taken to be at risk from the eligible data breach.

(2) For the purposes of this Act, if:
(a) a State or Territory health authority; or

(b) person employed by, or in the service of, the State or Territory health authority;

breaches a requirement of this Part in relation to COVID app data:

(c) the breach is taken to be an eligible data breach by the State or Territory health authority; and

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

(3) 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.

(4) Without limiting the circumstances in which the Commissioner may, under subparagraph (3)(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 (5) does not apply.

(5) 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.

(6) Paragraph (5)(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 (5) 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) 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) is satisfied that an investigation relating to the matter, or proceedings for an offence relating to the matter, will not be jeopardised, or otherwise affected, by continuation of the Commissioner's investigation;

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

(5) Upon receiving notice under subsection (3) or (4) 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 State or Territory privacy authority 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 State or Territory privacy authority 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 authority.

94X Application to State or Territory health authorities

(1) 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.

(2) However, subsection (1) does not, in relation to a State or Territory health authority:

(a) have the effect of applying Australian Privacy Principle 9 in relation to a government related identifier that has been assigned by that State or Territory or by a State or Territory authority of that State or Territory; or

(b) have the effect of applying this Act in relation to data or information that is not 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.

(3) The Secretary of the Health Department must not determine under subsection (1) that any of the following is the data store administrator:

(a) an enforcement body mentioned in paragraph (a) to (ea) of the definition of ***enforcement body*** in subsection 6(1);

(b) an intelligence agency;

(c) the Australian Geospatial-Intelligence Organisation;

(d) the Defence Intelligence Organisation.

94ZA Reports on operation and effectiveness of COVIDSafe and the National COVIDSafe Data Store

(1) The Health Minister must, as soon as practicable after:

(a) the end of the 6 month period starting on the commencement of this Part; and

(b) the end of each subsequent 6 month period (if any) starting on or before the day determined under subsection 94Y(1);

cause a report to be prepared on the operation and effectiveness of COVIDSafe and the National COVIDSafe Data Store during that 6 month period.

Note: Section 94D prevents the inclusion of COVID app data in the report. It would not be a permitted collection, use or disclosure under subsection 94D(2).

(2) If the day determined under subsection 94Y(1) occurs during the 6 month period starting on the commencement of this Part, the report under subsection (1) of this section relating to that period must be prepared within 3 months after that day.

(3) The Health Minister must cause copies of a report prepared under subsection (1) to be laid before each House of the Parliament within 15 sitting days of that House after the completion of the preparation of the report.

94ZB Reports by the Commissioner

(1) The Commissioner must, as soon as practicable after:

(a) the end of the 6 month period starting on the commencement of this Part; and

(b) the end of each subsequent 6 month period (if any) starting on or before the day determined under subsection 94Y(1);

cause a report to be prepared on the performance of the Commissioner's functions, and the exercise of the Commissioner's powers, under or in relation to this Part during the period.

Note: Section 94D prevents the inclusion of COVID app data in the report. It would not be a permitted collection, use or disclosure under subsection 94D(2).

(2) If the day determined under subsection 94Y(1) occurs during the 6 month period starting on the commencement of this Part, the report under subsection (1) of this section relating to that period must be prepared within 3 months after that day.

(3) The Commissioner must publish a report prepared under subsection (1) on the Commissioner's website.

(4) This section does not affect the matters that section 30 of the *Australian Information Commissioner Act 2010* requires the Commissioner to include in an annual report.

94ZC 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 or an authority of the Commonwealth).

94ZD 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

Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020

1 The whole of the instrument

Repeal the instrument.

Privacy Act 1988

Note: The repeals made by items 2 and 3 of 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.

2 Subsection 6(1)

Repeal the following definitions:

(a) definition of ***communication device***;
(b) definition of ***contact tracing***;
(c) definition of ***COVID app data***;
(d) definition of ***COVIDSafe***;
(e) definition of ***COVIDSafe user***;
(f) definition of ***data store administrator***;
(g) definition of ***former COVIDSafe user***;
(h) definition of ***Health Department***;
(i) definition of ***Health Minister***;
(j) definition of ***in contact***;
(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***.

3 Part VIIIA

Repeal the Part.

4 Transitional

After the commencement of this item:

(a) the powers of the Commissioner under or in relation to Part VIIIA of the *Privacy Act 1988* as amended by this Act continue to apply in relation to matters that arose under or in relation to that Part before that commencement; and

(b) any obligations of the Health Minister or the Commissioner under that Part relating to a report continue to apply;

as if the repeals made by items 2 and 3 of this Schedule had not been made.

[*Minister's second reading speech made in—*
House of Representatives on 12 May 2020
Senate on 13 May 2020]

(75/20)