2019-2020

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

PRIVACY AMENDMENT (PUBLIC HEALTH CONTACT INFORMATION) BILL
2020

EXPLANATORY MEMORANDUM

(Circulated by authority of the
Attorney-General, the Honourable Christian Porter MP)
GENERAL OUTLINE

1. This Bill elevates the provisions of the *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020* (the Determination) into primary legislation and introduces additional measures to strengthen privacy protections. The purpose of the Bill 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 amending the *Privacy Act 1988* (Privacy Act) to provide stronger privacy protections for users of the Commonwealth’s COVIDSafe app and data collected through the app (COVID app data) than the protections that would otherwise apply under Australian law.

2. As with the Determination, the Bill imposes strict requirements on the collection, use and disclosure of COVID app data. The Bill ensures data collected by COVIDSafe will only be used to facilitate contact tracing activities by State and Territory health officials or those in the service of State and Territory health authorities, and for the proper functioning, integrity and security of COVIDSafe and the National COVIDSafe Data Store.

3. Misuse of COVID app data will constitute a criminal offence. If the responsible person is subject to the Privacy Act because of the Bill or under the ordinary operation of the Privacy Act, individuals will also be able to make a complaint to the Information Commissioner under the Privacy Act. COVID app data will remain continually protected through encryption and the Bill makes it an offence to decrypt COVID app data stored on a communication device.

4. The Bill allows the reporting of de-identified statistics about the total number of registrations through COVIDSafe. This has been included to allow for evaluation and to ensure an appropriate degree of transparency and accountability about the collection, use and disclosure of COVID app data, without infringing on the privacy of the individual. De-identified data is information that is no longer about an identifiable individual or an individual who is reasonably identifiable.

5. The Bill is consistent with the approach that the use of the COVIDSafe app is strictly voluntary and that a COVIDSafe user’s informed consent is required to allow the app to collect data about the user and upload that data to the National COVIDSafe Data Store. The Bill specifically prohibits imposing a requirement on a person to download the COVIDSafe app, have the app in operation, or give consent for encrypted contact information to be uploaded to the National COVIDSafe Data Store at the point of a positive COVID-19 diagnosis.

6. The Bill requires the Commonwealth to store COVID app data uploaded through the COVIDSafe app in the Commonwealth’s National COVIDSafe Data Store, for the principal purpose of facilitating COVID-19 contact tracing activities by State and Territory health authorities. The Bill provides that the data held in the National COVIDSafe Data Store must be retained in Australia, and COVID app data that is or has been stored in the National COVIDSafe Data Store must not be disclosed to a person outside of Australia (except for the purposes of contact tracing by a State or Territory Government health official).
7. The Bill also provides a mechanism for COVIDSafe app users (and former users) to request the deletion of registration data uploaded from the user’s device. When the data store administrator receives such a request, they must take all reasonable steps to delete the data. The Bill also includes a requirement to delete COVID app data received in error and imposes an obligation to delete COVID app data from the National COVIDSafe Data Store at the end of the COVIDSafe data period (which will be determined by the Health Minister, with consideration of any advice from the Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee).

8. The Bill provides that any COVID app data relating to an individual is taken to be ‘personal information’ under the Privacy Act, and enables the Office of the Australian Information Commissioner (OAIC) to investigate complaints about breaches of the legislation and undertake assessments of compliance with privacy obligations under the legislation. Importantly, these powers allow the OAIC to investigate and assess State and Territory health authorities in relation to their handling of COVID app data.

9. Under the Bill, the OAIC has the ability to require State and Territory authorities’ cooperation with assessments and investigations and the power to refer matters as appropriate to the Commissioner of Police or the Director of Public Prosecutions to investigate criminal offences. The OAIC also has the power to refer matters to, and share information with State and Territory privacy regulators as appropriate. The scope of the OAIC’s powers in relation to State and Territory authorities is strictly limited to COVID app data.

10. The Bill also extends the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act to breaches involving COVID app data, including breaches of COVID app data held by the administrator of the National COVIDSafe Data Store and State and Territory health authorities. The data store administrator and State and Territory health authorities will be required to notify the Commissioner of any breach of a requirement contained in the Bill. The Commissioner can then respond to that notification by requiring the entity to prepare a statement about the breach in consultation with the Commissioner, and take reasonable steps to provide that statement to individuals to whom the COVID app data relates.

11. The Commissioner will have a discretion to grant an exemption, or a time-limited exemption, from the notification requirement on public interest grounds, and with regard to advice from a law enforcement body or the Australian Signals Directorate and any other matters the Commissioner considers relevant. This matches the Commissioner’s pre-existing discretion under the Privacy Act, and is intended to ensure that data breach notification is not required in cases where it may interfere with a police investigation into an offence committed under one of the provisions of the Bill.

12. The Bill’s requirements operate in place of any inconsistent requirements that would otherwise apply under Australian law. This includes any more stringent requirements about retaining Commonwealth records under the *Archives Act 1983* or less stringent requirements about handling personal information under the Privacy Act. However, the remainder of the Privacy Act, to the extent it is not inconsistent with the Bill, continues to apply to COVID app data that is personal information about an individual.

**FINANCIAL IMPACT**

13. This Bill has no significant impact on Commonwealth expenditure or revenue.
STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Privacy Amendment (Public Health Contact Information) Bill 2020

1. This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the Human Rights (Parliamentary Scrutiny) Act 2011.

Overview of the Bill

2. The Bill introduces strong privacy protections that apply to data collected through the COVIDSafe app to facilitate COVID-19 contact tracing efforts by State and Territory health authorities. These protections will be subject to criminal offences and oversight by the Australian Information Commissioner under the Privacy Act 1988 (Privacy Act), including the ability for individuals to make complaints to the Commissioner. The protections ensure that individuals must not be required to download, use or upload data through COVIDSafe by any person, and that informed consent is required before the Commonwealth collects data relating to a person through the COVIDSafe app. The protections also limit the ability to disclose COVID app data that is or has been stored in the Commonwealth’s National COVIDSafe Data Store outside of Australia. The Commonwealth will also be required to delete the National COVIDSafe Data Store when COVIDSafe is no longer required or is no longer likely to be effective as part of Australia’s response to COVID-19 (which must be determined based on expert medical advice).

Human rights implications

Right to health

3. Article 12 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) promotes the right of all individuals to enjoy the highest attainable standards of physical and mental health. This includes the application of measures for the prevention, treatment and control of epidemic, endemic, occupational and other diseases (Article 12(2)).

4. The United Nations Committee on Economic, Social and Cultural Rights (UNCECSR) states in General Comment No 14 (2000) that health is a ‘fundamental human right indispensable for the exercise of other human rights’, and that the right to health is not to be understood as the right to be healthy, but rather entails a right to ‘a system of health protection which provides equality of opportunity for people to enjoy the highest attainable level of health’.

5. The UNCECSR also states in General Comment No 14 that the ‘highest attainable standard of health’ takes into account the country’s available resources, and that this right may be understood as a right of access to a variety of public health and health care facilities, goods, services, programs, and conditions necessary for the realisation of the highest attainable standard of health.

6. The purpose of COVIDSafe is to assist relevant State and Territory health authorities with contact tracing. Contact tracing is critical to containing the spread of COVID-19 by
identifying individuals who may have been exposed to the virus, assisting them to take appropriate steps to avoid further transmission and providing advice about medical services available to them. Understanding the nature and extent of community transmission of COVID-19 is fundamental to the public health response to the pandemic.

7. The Bill promotes the right to health by assisting health authorities:
   a. facilitate efficient and accurate contact tracing via COVIDSafe to control the spread of COVID-19 in Australia and render appropriate health services as necessary
   b. provide access to critical health information about COVID-19 to individuals and families, and
   c. provide access to health services for groups that are more severely impacted by COVID-19, including older people, people with disability, Indigenous people and pregnant women.

Right to protection against arbitrary or unlawful interference with privacy

8. The protection against arbitrary or unlawful interference with privacy is contained in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Article 17 provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation, and that everyone has the right to the protection of the law against such interference or attacks.

9. Although the United Nations Human Rights Committee has not defined ‘privacy’, it should be understood to comprise freedom from unwarranted and unreasonable intrusions into activities that society recognises as falling within the sphere of individual autonomy.

10. The right to privacy under Article 17 can be permissibly limited in order to achieve a legitimate objective and where the limitations are lawful and not arbitrary. The term ‘unlawful’ in Article 17 of the ICCPR means that no interference can take place except as authorised under domestic law. Additionally, the term ‘arbitrary’ in Article 17(1) of the ICCPR means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances. The Committee has interpreted ‘reasonableness’ to mean that any limitation must be proportionate and necessary in the circumstances.

11. The measures in the Bill will promote the right to privacy by establishing a temporary standalone framework for the collection, use, disclosure and dealing of personal information, which introduces stronger provisions where appropriate than existing protections for this information handling under the Privacy Act. In this way, the Bill promotes the right to privacy by creating a stronger information privacy framework for COVID app data than would otherwise exist under prevailing law. The penalties introduced under this temporary standalone framework — including criminal penalties of up to five years imprisonment or 300 penalty units, or both — are considered to be reasonable, necessary and proportionate in light of the Bill’s objective to provide genuine privacy safeguards that build confidence in the COVIDSafe app. This in turn is intended to bolster the uptake and effectiveness of COVIDSafe as a new tool to help Australia respond to the serious health risks posed by COVID-19, until the point where COVIDSafe is no longer required or would no longer be effective.
12. To the extent that measures in the Bill that authorise the collection, use, disclosure or dealing of personal information may interfere with the right to privacy, they are lawful and non-arbitrary. The Bill aims to achieve the legitimate objective of combatting the community spread of COVID-19. COVIDSafe achieves this by collecting personal information about users who come into contact with each other, but limiting this collection to the minimum amount of information reasonable and necessary in order to facilitate effective contact tracing. COVIDSafe does not collect geolocation data. Should a user be diagnosed with COVID-19, State or Territory health authorities will use the information collected by COVIDSafe to contact other users whom the diagnosed person came into a contact with and inform them of the necessary next steps to contain the spread of the virus.

13. The Bill contains multiple protections to ensure that personal information is being collected in an appropriate and non-invasive manner in order to achieve the legitimate aims and objectives of contact tracing. Further, if a person is diagnosed with COVID-19 they will still have a choice as to whether to upload close contact data. The consent-based model ensures that this collection of personal information is reasonable, necessary and proportionate to achieving the legitimate aim of combatting COVID-19 through contact tracing.

14. The measures in this Bill reduce privacy risks, and safeguard the individual’s right to privacy through the further measures described below.

Choice whether to install the app

15. COVIDSafe is completely voluntary to download and use. The Bill ensures that individuals are given a free and informed choice regarding whether to download and use COVIDSafe by creating safeguards to protect individuals from disadvantage or other adverse consequences should an individual decide not to download or use COVIDSafe.

16. For example, an employer cannot make downloading or using COVIDSafe a condition of employment. A retailer cannot refuse a person entry to their premises, refuse to provide goods or services or insist on providing goods or services on different monetary terms, on the ground that a person has not installed or is not using COVIDSafe. At the same time, the Bill includes appropriate safeguards to ensure persons at private properties or residences remain able to control who enters that premises on any basis (excluding landlord/tenant or similar relationships, or employment/commercial relationships).

17. Requiring a person to download, use, or consent to upload COVID app data is an offence under this Bill and carries a maximum penalty of five years imprisonment or 300 penalty units, or both. This measure provides strong incentives against imposing requirements relating to the download and use of COVIDSafe.

Stringent limitations on the collection, use, disclosure and dealing of personal information

18. The Bill limits when personal information is shared to ensure that an individual’s personal information is only accessed when it is critical to do so to protect the health and wellbeing of the community and those with whom the individual has come into close contact. This will be achieved through providing that the personal information collected may only be used for particular specified purposes by relevant bodies, with broad prohibitions on the use
of that information for other purposes. These protections will apply to information collected through the COVIDSafe app at any time, including before commencement of the Bill.

19. When personal information is uploaded to the National COVIDSafe Data Store following a positive COVID-19 diagnosis, only State and Territory health authorities may access relevant data for the purpose of contact tracing. Officials, employees or contractors of the data store administrator may also access data but only for the purpose of enabling contact tracing by a State or Territory health authority, ensuring the proper functioning of the Data Store and ensuring that the Data Store is accurate and secure from unauthorised access. Access for law enforcement purposes or by the Information Commissioner will only be permitted to the extent necessary to enforce the privacy protections contained in the Bill.

20. State and Territory health authorities will put in place additional controls and procedures to ensure that only approved employees or personnel may access data in the National COVIDSafe Data Store for the purpose of contact tracing. Similarly, the data store administrator will put in place additional controls and procedures to ensure that only approved officials, employees or contractors may access data in the National COVIDSafe Data Store for the purposes permitted in the Bill.

21. The Bill also makes it unlawful for a person to decrypt COVID app data that is stored on a communication device. Breach of this provision is subject to a maximum penalty of five years imprisonment or 300 penalty units, or both. This measure provides strong incentives against attempting to decrypt COVID app data, protecting the integrity and security of users’ personal information.

22. By strictly limiting the collection, use, disclosure and dealing of an individual’s personal information, the Bill promotes the right to privacy.

Reporting requirements

23. The Bill also includes regular reporting obligations for the Health Minister to report on the operation and effectiveness of the COVIDSafe app and the National COVIDSafe Data Store, and for the Information Commissioner to report on the Commissioner’s performance of functions and exercise of powers under the Bill. This is designed to ensure an appropriate degree of transparency and to build public confidence in the strong privacy protections that will apply under the Bill.

Conclusion

24. The Privacy Amendment (Public Health Contact Information) Bill 2020 is compatible with human rights because it promotes the rights to health and privacy, and to the extent that it may limit those rights, those limitations are reasonable, necessary and proportionate.
NOTES ON CLAUSES

Preliminary

Clause 1 – Short title

1. This clause provides for the short title of the Bill to be the *Privacy Amendment (Public Health Contact Information) Act 2020*. 

Clause 2 – Commencement

2. This clause provides for the commencement of each provision in the Bill, as set out in the table. Item 1 in the table provides that sections 1 to 3 which concern the formal aspects of the Bill, as well as anything in the Bill not elsewhere covered by the table, will commence on the day on which the Bill receives Royal Assent.

3. The items in Schedule 1 come into effect on the day after this Bill receives Royal Assent. These provisions include all substantive requirements, protections and obligations in this legislation.

4. Item 1 in Schedule 2 comes into effect on the day after this Bill receives Royal Assent (see description of the item below for additional detail).

5. Items 2 to 4 in Schedule 2 come into effect at the end of 90 days after the day determined by the Minister for Health under subsection 94Y(1) of the *Privacy Act 1988* (Privacy Act), as amended by Part VIIIA. The date in the determination made by the Minister for Health determines that the COVIDSafe app is no longer required, which in turn triggers the COVIDSafe app being withdrawn from download and the National COVIDSafe Data Store being deleted (for further details, see the description of section 94Y below).

6. The purpose of items 2 to 4 of Schedule 2, and the delayed commencement, is contingent on the determination made under subsection 94Y(1) and has the effect of repealing the provisions provided for in this Bill (including the definitions that are included in subsection 6(1), and all provisions in Part VIIIA).

Clause 3 – Schedules

7. Legislation specified in a Schedule to this Bill is amended or repealed as set out by the items in the corresponding Schedule. In relation to this Bill:

   a. Schedule 1 sets out the legislation to be enacted on the day after Royal Assent;

   b. Schedule 2, item 1 provides for the repeal of the *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020* (the Determination) on the day after Royal Assent; and

   c. Schedule 2, items 2 to 4 set out the legislation to be repealed 90 days after the date in the direction made under subsection 94Y(1).
Schedule 1 - Amendments

Clause 1 – Subsection 6(1)

8. The provisions in this clause set out new definitions that are relevant to the operation of Part VIIIA (in addition to the existing definitions already included in subsection 6(1)). The new definitions that are set out in this Bill are described as follows:

a. *communication device* means an item of customer equipment (as defined in section 21 of the *Telecommunications Act 1997*). This definition is intended to cover consumer mobile phones, tablets, and other devices that are able to connect to a mobile network or Wi-Fi network. The purpose is to provide broad coverage of protections to ensure that they extend to all devices where a person may have installed COVIDSafe and may upload data through COVIDSafe to the National COVIDSafe Data Store. The term ‘communication device’ is intended to be descriptive only and is not intended to limit the kind of devices that may be caught by the operative element of the definition.

b. *contact tracing* is described in subsection 94D(6). Information about this definition is included in the description of subsection 94D(6) later in this memorandum.

c. *COVID app data* is described in subsection 94D(5). Information about this definition is included in the description of subsection 94D(5) later in this memorandum.

d. *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. This definition refers to the app known as ‘COVIDSafe’ that is available for free download through the Apple and Google app stores (for iOS and Android devices respectively). The definition ensures that any changes to the app (for example, new versions with technical updates) would still be captured where the app continued to be for the purpose of facilitating contact tracing, and was still made available on, or on behalf of, the Commonwealth.

e. *COVIDSafe user* means the person whose registration data (meaning that the registration data relates to that person) was uploaded from a communication device when that person registered through COVIDSafe. A COVIDSafe user refers to a person in relation to a particular communication device. A person may be multiple COVIDSafe users if the person has registered their details through multiple devices, even if the person has registered using identical details. This occurs as each device will separately collect data about others that the person has come into contact with, and the National COVIDSafe Data Store will treat this information (if uploaded), as coming from separate accounts.

f. *data store administrator* means the Commonwealth Government agency, or agencies responsible for administering the National COVIDSafe Data Store.
This is, by default, the Commonwealth Department of Health, however may also (for the purposes of Part VIIIA) be another agency as specified by the Department of Health in a determination made under section 94Z of this Bill. Details about how the Department of Health may determine another agency to be the data store administrator, and the limitations on the Department of Health’s ability to do so, are discussed in the description of section 94Z later in this memorandum.

g. **Former COVIDSafe user** is described in subsection 94N(2). Information about this definition is included in the description of subsection 94N(2) later in this memorandum.

h. **Health Department** means the Department administered by the Health Minister.

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

j. **in contact** means 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 proximity of the other person. For the purposes of Part VIIIA, a person will only have been considered to be ‘in contact’ with another person where both individuals are COVIDSafe users and have COVIDSafe operating and COVIDSafe subsequently detects the presence of the other person within the detectible proximity of COVIDSafe.

k. **National COVIDSafe Data Store** means the database administered by, or on behalf of the Commonwealth for the purpose of contact tracing. This definition refers to the database into which COVID app data will be uploaded and stored. There are specific requirements that relate to the National COVIDSafe Data Store which are outlined in Part VIIIA of this Bill.

l. **registration data**, of a person, means that information of a person that was uploaded from a communication device when the person was registered through COVIDSafe (name, or pseudonym, phone number, age range and postcode). Registration data comprises a component of COVID app data within the meaning of that term in subsection 94D(5). There are also separate rights and obligations that apply specifically to registration data under Part VIIIA of this Bill.

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

n. **State or Territory privacy authority** means a State or Territory authority that has functions to protect the privacy of individuals. Such an authority may also have other functions or may only have a particular kind of privacy protection function, reflecting that States and Territories have different regulatory arrangements in place to protect the privacy of individuals. However, such an authority would be included within the scope of this definition as that authority has a function to protect individual privacy.
Clause 2 – After Part VIII

Part VIII A

9. Part VIII A sets out the protections, rights and obligations relating to the COVIDSafe app, and any subsequent COVID app data collected through COVIDSafe together with offences and penalties for failure to comply with requirements and obligations. The part is divided into four divisions:

a. Division 1 – Preliminary matters, which sets out the outline, purpose and constitutional bases for Part VIII A.

b. Division 2 – Offences relating to COVID app data and COVIDSafe; which sets out offences for the unlawful collection, use, disclosure or decryption of COVID app data, permissible handling of COVID app data, and protections against requiring individuals to use COVIDSafe; breaches of sections in this division constitute criminal offences and may also be enforceable by the Information Commissioner as interferences with privacy under the Privacy Act due to the operation of Division 4.

c. Division 3 – Other obligations relating to COVID app data and COVIDSafe; which sets out obligations for the data store administrator and National COVIDSafe Data Store around retention and deletion of COVID app data. This Division also sets out the obligations where a person receives COVID app data in error. Breaches of sections in this division constitute interferences with privacy under the Privacy Act.

d. Division 4 – Application of general privacy measures; which sets out how the existing Privacy Act mechanisms, such as interferences with privacy, the Notifiable Data Breach scheme in Part III C, and Commissioner oversight of privacy matters, interact with Part VIII A.

e. Division 5 – Miscellaneous; which sets out when COVID app data must be deleted from the National COVIDSafe Data Store, how to determine the agency designated as the data store administrator, reporting obligations of the Health Minister and the Information Commissioner in relation to Part VIII A, ownership of COVID app data and the interaction of Part VIII A with other laws.

Part VIII A – Division 1 – Preliminary

Section 94 A – Simplified outline of this Part

10. Section 94 A provides a simple outline of matters that are dealt with in this Part. The outline briefly addresses offences, specific obligations relating to the deletion of data and the end of the COVIDSafe data period, general privacy law interactions, and the override provision in Division 5.

Section 94 B – Object of this Part
11. Section 94B sets out the object of this Part. The object is to assist in preventing and controlling the emergence, establishment or spread of the coronavirus known as COVID-19 in Australia or any part of Australia by providing stronger privacy protections for COVID app data and COVIDSafe users to encourage public acceptance and uptake of COVIDSafe; and enable faster and more effective contact tracing.

12. The chapeau of section 94B refers to assisting in preventing and controlling the emergence, establishment or spread of COVID-19 in Australia or any part of Australia by providing stronger privacy protections for COVID app data.

13. The purpose of COVIDSafe is provided at paragraph 94B(b); that purpose is to enable faster and more effective contact tracing. The content of paragraph 94B(a), to encourage public acceptance and uptake of the app, is the central feature of the protections of this Part by ensuring that COVID app data is not mishandled or used in a manner inconsistent with achieving the stated purpose of COVIDSafe, and subsequent community expectations.

Section 94C – Constitutional basis of this Part

14. Section 94C sets out the constitutional basis of this Part. Subsection 94C(1) makes clear that the Part’s principal constitutional basis is 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 (sometimes referred to as the nationhood power).

15. The effect of subsections 94C(2)-(5) is that the Part also relies on the following provisions of the Constitution:

   a. the Commonwealth’s legislative powers under paragraph 51(ix) with regard to quarantine;

   b. the Commonwealth’s legislative powers under paragraph 51(v) with regard to postal, telegraphic, telephonic, and other like services; and

   c. the Commonwealth’s legislative powers under paragraph 51(xxix) with regard to external affairs, in the sense of giving effect to Australia’s obligations under Article 17 of the ICCPR (which refers to measures to protect from arbitrary or unlawful interferences with privacy).

Part VIII A – Division 2 – Offences relating to COVID app data and COVIDSafe

16. This Division sets out offences for prohibited actions in relation to COVID app data. These offences relate to non-permitted collection, use or disclosure of COVID app data, decryption of COVID app data, and placing requirements on another person to install or use COVIDSafe.

Section 94D – Collection, use or disclosure of COVID app data

17. Section 94D sets out a general prohibition on collecting, using or disclosing COVID app data unless that collection, use or disclosure falls within the permitted purposes outlined in the section.
Subsection 94D(1) – Offence of collecting, using or disclosing COVID app data

18. Subsection 94D(1) sets out the elements of the offence for collecting, using or disclosing COVID app data. For a person to have committed an offence under this section, a person must have collected, used or disclosed data that is COVID app data, and where that collection, use or disclosure is not permitted under any provision in section 94D.

19. The maximum penalty for contravening subsection 94D(1) is five years imprisonment or 300 penalty units, or both. All penalties for offences under this Part are equal to the penalty for failing to comply with the Determination (made on 25 April 2020, and which would be repealed by item 1 of Schedule 2 as described later in this memorandum). Equivalent penalties represent the continued need for heightened protections for COVID app data.

20. This offence is needed to provide a strong protection against misuse of COVID app data and to assure the community of the seriousness with which misuse of COVID app data is taken.

21. The terms ‘collects’, ‘uses’ and ‘discloses’ are used consistently with how they are understood in the context of the Privacy Act.

22. To make out an offence, the prosecution is required to demonstrate that the collection, use or disclosure was not permitted under section 94D. The permitted purposes in relation to paragraph 94D(1)(c) are set out in subsection 94D(2).

Subsection 94D(2) – Permitted uses of COVID app data

23. Subsection 94D(2) sets out permissible collections, uses and disclosures of COVID app data. The offence in subsection 94D(1) would not apply to a person using COVID app data in a manner consistent with this subsection. Each permissible action is detailed below, however can be summarised as:

a. Paragraph 94D(2)(a) sets out how COVID app data may be used by State or Territory health authorities;

b. Paragraphs 94D(2)(b), 94D(2)(f) and 94D(2)(g) set out how COVID app data may be used by the data store administrator or a contracted service provider for a government contract with the data store administrator;

c. Paragraph 94D(2)(c) sets out how COVID app data may be collected or disclosed in the course of the normal operation of the COVIDSafe app and the National COVIDSafe Data Store; and

d. Paragraphs 94D(2)(d) and 94D(2)(e) set out when law enforcement and regulatory bodies with responsibilities for enforcing obligations or prosecuting penalties arising under this Part can collect, use or disclose COVID app data for those functions.

24. The permissions in each of these paragraphs is detailed further below. Each permissible action requires that the extent of that action is ‘for the purpose, and only to the extent required for the purpose of’ achieving the relevant purpose. This adds an additional
obligation on any person handling COVID app data and ensures that each person using COVID app data for a permitted purpose considers whether their collection, use or disclosure is the minimum necessary in order to achieve that purpose.

25. Paragraph 94D(2)(a) permits a person employed by, or in the service of, a State or Territory health authority to collect, use or disclose COVID app data if it is for the purpose, and only to the extent required for that purpose, of undertaking contact tracing.

26. As the States and Territories are responsible for contact tracing initiatives, paragraph 94D(2)(a) allows relevant persons employed by, or in the service of, a State or Territory health authority to access COVID app data to allow them to contact COVIDSafe app users who have been identified as being in contact with a user who has been diagnosed with COVID-19 and subsequently uploaded their information to the National COVIDSafe Data Store.

27. Paragraph 94D(2)(a) refers to persons employed by, or in the service of, a State or Territory health authority. The term ‘in the service of’ a State or Territory health authority allows those authorities to rely on the resources available to them to facilitate contact tracing, while retaining a requirement that there be adequate proximity and oversight by the State or Territory health authority. This may include contracted service providers, or other contractors, but anticipates that, due to the extraordinary conditions imposed by COVID-19, there may be persons involved in the contact tracing process who are not technically employees or officers of a State or Territory health authority.

28. Paragraph 94D(2)(b) provides that a person who is an officer or employee of the data store administrator, or a contracted service provider for a government contract with the data store administrator, is permitted to collect, use or disclose COVID app data for the purpose of, and only to the extent required for the purpose of:

   a. enabling contact tracing by persons employed by, or in the service of, State or Territory health authorities; or
   
   b. ensuring the proper functioning, integrity or security of COVIDSafe or the National COVIDSafe Data Store.

29. The terms ‘contracted service provider’ and ‘government contract’ are defined in existing subsection 6(1) of the Privacy Act. The use of these terms is intended to cover any contractor engaged by the data store administrator, as well as any sub-contractors for the same contract.

30. The term ‘enabling contact tracing’ in subparagraph 94D(2)(b)(iii) does not allow the data store administrator to undertake contact tracing activities using COVID app data; it only allows the data store administrator to take any steps necessary (and permitted) to ensure that State and Territory health authorities can collect the relevant COVID app data to be able to undertake their contact tracing activities as provided for in paragraph 94D(2)(a).

31. The term ‘ensuring the proper functioning, integrity or security’ of COVIDSafe or the National COVIDSafe Data Store in subparagraph 94D(2)(b)(iv) allows the data store administrator to undertake such actions as are required to ensure the ongoing operability of both COVIDSafe and the National COVIDSafe Data Store to ensure that the requirements,
both under this Part and any other obligations in the Privacy Act or other Australian laws are adhered to.

32. This paragraph is intended to be read broadly, in light of the objects of the Part and the COVIDSafe app. It is intended in part to capture actions that are technical in nature – meaning that they are required to support the purpose of COVIDSafe and the National COVIDSafe Data Store in ensuring secure collection, storage and disclosure of COVID app data as required to allow States and Territory health authorities to undertake contact tracing while ensuring that the COVID app data is safe from interference, misuse or unauthorised access. It is also intended to capture more general measures to ensure the proper functioning of the COVIDSafe app, such as sending notifications through the app to COVIDSafe users where this is desirable or required. The interaction with COVID app data should be limited to the smallest extent possible while allowing for the continued and proper administration of COVIDSafe and the National COVIDSafe Data Store.

33. Paragraph 94D(2)(c) provides that in the case of collection or disclosure of COVID app data, that collection or disclosure is for the purpose of, and only to the extent required for the purpose of:

   a. Transferring encrypted data between communication devices through COVIDSafe; or

   b. Transferring encrypted data through COVIDSafe from a communication device to the National COVIDSafe Data Store.

34. Subparagraph 94D(2)(c)(i) facilitates encrypted COVID app data moving between communication devices where users who both have COVIDSafe installed interact in such a way that the interaction is recorded through what is known as a Bluetooth handshake to between the two communication devices.

35. Subparagraph 94D(2)(c)(ii) facilitates the transfer of COVID app data moving from a COVIDSafe user’s communication device to the National COVIDSafe Data Store. It is anticipated that this would happen in two circumstances:

   a. Where a COVIDSafe user initially registers their details in COVIDSafe, that data is uploaded to the National COVIDSafe Data Store; and

   b. If a user is diagnosed with COVID-19 and consents to upload data relating to their interactions with other COVIDSafe users.

36. These subparagraphs are needed to alleviate any doubt as whether these actions, which occur during the usual and intended operation of COVIDSafe and the National COVIDSafe Data Store, might constitute an authorised collection or disclosure of COVID app data by any person or entity.

37. Paragraph 94D(2)(d) permits collection, use or disclosure for the purpose of, and only to the extent required for the purpose of, allowing the Commissioner to perform their functions or exercise the powers of the Commissioner under, or in relation to, this Part.

38. The Commissioner has relevant powers and functions relating to protecting the privacy of Australians. The Commissioner has the powers specified in Division 4 of this Part,
together with any powers and functions under the Privacy Act. As the Commissioner is the
key regulator with oversight of the handling of COVID app data, the Commissioner is
required to be able to collect, use or disclose COVID app data in connection with exercising
their powers.

39. The Commissioner’s exercise of powers may include, but is not limited to:
investigating a suspected interference with privacy, whether of their own initiative, or in
response to a complaint, or assessing whether an entity handling COVID app data is
complying with their obligations.

40. Paragraph 94D(2)(e) permits the collection, use or disclosure of COVID app data for
the purpose of, and only to the extent required for the purpose of:

a. Investigating whether this Part has been contravened; or

b. Prosecuting a person for an offence against this Part.

41. This Part provides strong penalties for contraventions of the Part. These penalties are
only effective if suspected contraventions can be investigated, and where appropriate,
subsequently prosecuted.

42. The strong override provisions in section 94ZD of this Part ensures that other
Australian laws do not override the protections in this Part.

43. Paragraph 94D(2)(f) permits the data store administrator to use COVID app data to
produce de-identified statistical information about the total number of registrations through
COVIDSafe.

44. As de-identification is a use of COVID app data, no other entity is permitted to
de-identify COVID app data in any way. This means that the only way that de-identified
information can be derived from COVID app data is by the data store administrator, and only
for the extremely limited purposes of producing de-identified statistical information about the
total number of registrations through COVIDSafe.

45. Once statistical information about the total number of registrations has been de-
identified in accordance with this paragraph, paragraph 94D(5)(d) states that the data is no
longer COVID app data and protections and requirements in this Part no longer apply. There
is a strong public interest, including for public health reasons, in being able to share
information publicly about how many total users have registered through COVIDSafe.
Ensuring that the scope of de-identified information is limited proactively addresses the
possibility of COVID app data not being properly de-identified or being released in a form
that could be readily re-identified.

46. Paragraph 94D(2)(g) permits the data store administrator to use COVID app data if it
consists of access for the purpose of, and only to the extent required for the purpose of,
confirming that the correct data is being deleted under section 94L. Section 94L allows a
COVIDSafe user or former COVIDSafe user to request the deletion of their registration data.
Paragraph 94D(2)(g) is included to ensure that, in the process of actioning such a request, the
data store administrator is not in breach of subsection 94D(1).
Subsection 94D(3) – Defence for inadvertent collection of COVID app data

47. Subsection 94D(3) provides a defence to the collection of COVID app data in very limited circumstances. The offence does not apply if the collection occurred as part of the collection, at the same time, of non-COVID app data, and that the collection of the COVID app data was incidental to the collection of the non-COVID app data. Additionally, the collection of the non-COVID app data must have been permitted under an Australian law.

48. To rely on the defence in subsection 94D(3), after the collection of the COVID app data in the circumstances described above and outlined in paragraphs 94D(3)(a) and 94D(3)(b), paragraph 94D(3)(c) requires that the collecting person take positive steps to ensure that the COVID app data be deleted as soon as practicable after the person becomes aware that the COVID app data has been collected, and that the COVID app data is not accessed, used, or disclosed by the person after it was collected. The ‘soon as practicable’ timeframe has been included to provide an appropriate degree of flexibility in cases where there may be compelling reasons not to delete the COVID app data straight away, while still reflecting the expectation that the COVID app data will be deleted.

49. A person wishing to rely on this defence bears an evidential burden of proof meaning that the person must show, on the balance of probabilities, that all matters in subsection 94D(3) were applicable. This is addressed in the note at the end of subsection 94D(3).

50. This defence recognises that there may be circumstances where COVID app data is inadvertently collected as part of a wider collection of information. Inserting the positive obligations of data deletion and no further interactions with the data ensures that the defence is limited to only incidental collection, and that in these circumstances, the collecting person can derive no benefit from that collection.

Subsection 94D(4) – Admissibility of non-COVID app data collected alongside COVID app data

51. Subsection 94D(4) provides that where COVID app data and non-COVID app data have been collected together in the circumstances specified in subsection 94D(3), the admissibility of the non-COVID app data is not affected by the incidental collection or subsequent deletion of the COVID app data as required by subparagraph 94D(3)(c)(i).

52. Where COVID app data is incidentally collected in the circumstance in subsection 94D(3), it cannot be used as evidence in any investigation or prosecution. If the investigation or prosecution pertains to a contravention of this Part, the collection, use or disclosure of COVID app data must be done in accordance with paragraph 94D(2)(e).

53. Subsection 94D(4) ensures that where COVID app data is incidentally collected, proactive steps must be taken to delete the COVID app data as soon as practicable. By ensuring that the non-COVID app data remains admissible, a balance is achieved between ensuring that COVID app data is not used or disclosed in any manner inconsistent with subsection 94D(2) while also ensuring that lawful actions unrelated to this Part are not materially affected through the inadvertent collection of COVID app data.
54. COVID app data is data relating to a person that has been collected or generated (including before the commencement of this Part) through the operation of COVIDSafe, where that data is either:

   a. registration data, which COVIDSafe is designed not to store on a communication device; or

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

55. COVID app data is not 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 de-identified statistical information about the total number of registrations through COVIDSafe which is produced under paragraph 94D(2)(f).

56. COVID app data is information that is both ‘collected’ and ‘generated’ to ensure that data that is calculated or otherwise derived from within the COVIDSafe app on a communication device is also caught within the definition. COVIDSafe does not collect geolocation data.

57. Data falls within the definition of COVID app data both when it is held on a user’s communication device (in the case of data other than registration data), and after that data is uploaded to the National COVIDSafe Data Store. Additionally, the process of encrypting or decrypting COVID app data at any point through the normal operation and administration of COVIDSafe or the National COVIDSafe Data Store (as permitted under subsection 94(2)) is not intended to be material when considering whether data is COVID app data.

58. COVID app data captures data that was collected or generated prior to the commencement of this Bill. This is to capture any data that was collected or generated since COVIDSafe was released for public download on 26 April 2020. While protections against misuse, mishandling, or any sort of unauthorised collection or disclosure of COVID app data have been protected through the Determination, providing that data collected prior to commencement of this Bill allows the protections in this Part, and all relevant oversight by the Commissioner, to apply to that data once the Part commences.

59. Paragraph 94D(5)(c) clarifies that where States and Territories collect information through contact tracing, even where that contact tracing was facilitated by COVID app data, the information subsequently collected is not COVID app data. The overall purpose of COVIDSafe is to assist in the contact tracing process, and once a contact tracer makes contact with a person, any information subsequently collected is not subject to the protections in this Part. This is necessary as otherwise this Part risks hindering the effectiveness of contact tracing by limiting how States and Territories use any information gathered through the contact tracing process in formulating and deploying their public health response. Paragraph 94D(5)(c) is also intended to apply in cases where the information a State or Territory health authority collects during the contact tracing process is the same as the COVID app data: for example, if the authority verifies over the phone that a person’s preferred name and contact phone number are the same name and number they used when registering for COVIDSafe, and makes a new record of information containing that name and number.
60. Paragraph 94D(5)(d) provides that COVID app data does not include de-identified statistical information about the total number of registrations through COVIDSafe produced by an officer or employee of or a contracted service provider to the data store administrator. Paragraph 94D(5)(d) is referring to the de-identified statistical information that the data store administrator is permitted to produce under paragraph 94D(2)(f). As discussed above, paragraph 94D(2)(f) has been included due to the strong public interest reasons for allowing the wider disclosure of de-identified statistical information about the overall number of registered COVIDSafe users, and has been tailored to address the risk of releasing de-identified COVID app data that could later be re-identified. Paragraph 94D(5)(d) ensures this limited amount of information can be publicly released, including through a report by the Health Minister under section 94ZA (discussed below), without contravening subsection 94D(2).

Subsection 94D(6) – Definition of ‘contact tracing’

61. Contact tracing is the process of identifying persons who have been in contact with a person who has tested positive for COVID-19. Subsection 94D(6) specifies that this process may include:

   a. Notifying a person that the person has been in contact with a person who has tested positive for COVID-19;
   
   b. Notifying a parent, guardian or carer of another person that the other person has been in contact with a person who has tested positive for COVID 19;
   
   c. Providing information and advice to a person who has tested positive, or has been in contact with a person who has tested positive, or is the parent, guardian or carer of a person who falls into either of the prior categories.

62. The definition of contact tracing is consistent with the clinical view of what is required, including not only notification, but advice and information as required.

63. The definition of ‘contact tracing’ incorporates parents, guardians and carers to recognise that there are vulnerable people, including persons with disability, the elderly, and children, where it may be appropriate for the contact tracer to talk to a person responsible for that person.

Section 94E – COVID app data on communication devices

64. Section 94E provides an offence for uploading COVID app data from a COVID app user’s communication device to the National COVIDSafe Data Store without the consent of the COVIDSafe user.

65. Specifically, section 94E sets out three elements that must be satisfied for a person to commit an offence. First, a person must intentionally upload, or cause to upload, data from a communication device. Second, the person must be reckless that the data is COVID app data. Third, the person must be reckless to the fact that the COVID app user did not give consent (or their parent, guardian or carer must not have consented, in cases where the person is unable to consent or has requested their parent, guardian or carer to act on their behalf).
66. The purpose of this section is to establish that COVID app data – incorporating both initial registration data, and, where applicable, further data about the COVIDSafe user’s interactions with other COVIDSafe users, must not be uploaded to the National COVIDSafe Data Store without the consent of the COVIDSafe user or (where applicable) their parent, guardian or carer. In effect, section 94E prevents any person from compelling another person to upload their data to the Data Store under any circumstance, and embeds the two-stage consent process of the COVIDSafe app by ensuring that the consent of COVIDSafe users must be sought prior to uploading any further data (after initial registration) through COVIDSafe to the National COVIDSafe Data Store.

67. The provision for parents, guardians or carers acting on behalf of another person in this section recognises that there are vulnerable people who are utilising COVIDSafe who may either rely on a responsible person to assist with decision making, or have a preference for another person to make representations on their behalf. The categories of person who can consent on the behalf of a person are limited to reduce the risk of consent being given on behalf of another person against their wishes and to cover categories where a person is most likely to be assisting a person who either cannot consent, or may request another person consent on their behalf. This may include, but is not limited to, children, persons with disability, and the elderly.

68. The maximum penalty for contravening section 94E is five years imprisonment or 300 penalty units, or both.

Section 94F – COVID app data in the National COVIDSafe Data Store

69. Section 94F contains two offences which restrict COVID app data held in the National COVIDSafe Data Store from being transmitted overseas. Subsection 94F(1) prohibits the retention of COVID app data on a database outside Australia; and subsection 94F(2) prohibits the disclosure of COVID app data to any person outside Australia.

70. Each of the offences under section 94F attract a maximum penalty of five years imprisonment or 300 penalty points, or both.

71. Both offences relate to the retention or disclosure of ‘COVID app data that has been uploaded from a communication device to the National COVIDSafe Data Store’. This phrase refers to the information that is held in the National COVIDSafe Data Store after upload. The phrase does not refer to COVID app data stored on a communication device during the ordinary operation of COVIDSafe where the data has not been uploaded to the National COVIDSafe Data Store.

72. Subsection 94F(1) sets out two elements which, if satisfied, constitutes an offence. Firstly, a person must intentionally retain data on a database outside Australia, and secondly, the person must be reckless to the fact that the data on the database is COVID app data that has been uploaded from a communication device to the National COVIDSafe Data Store.

73. The purpose of the offence in subsection 94F(1) is to ensure that all COVID app data stored on the National COVIDSafe Data Store is held in Australia, and that overseas servers are not utilised for this purpose.

74. Under subsection 94F(2) a person commits the offence if they intentionally disclose data to another person outside Australia, and the person is reckless to the fact that the data is
COVID app data that has been uploaded from a communication device to the National COVIDSafe Data Store. However, the offence does not apply if the person is a person employed by, or in the service of, a State or Territory health authority who discloses the data in the process of undertaking contact tracing.

75. This offence ensures that COVID app data is not disclosed to any person outside Australia, even where such a disclosure would otherwise be consistent with a permitted disclosure under subsection 94D(2) of this Part. This offence acts to prevent any extraterritorial disclosure and provides that all collections, uses and disclosures of COVID app data is appropriately regulated by Australian law.

Section 94G – Decrypting COVID app data

76. Section 94G provides that a person commits an offence if the person decrypts COVID app data. A person commits an offence if they meet the two elements of the offence, being that a person intentionally decrypts encrypted data; and the person is reckless to the fact that the data is COVID app data that is being stored on a communication device.

77. The maximum penalty for decrypting COVID app data is five years imprisonment, or 300 penalty units, or both.

78. The purpose of this offence is to prevent any person from decrypting COVID app data while it is stored on a communication device. This offence does not contain any exceptions and applies to all persons and entities. The effect of subsection 94ZD ensures that no powers in law enforcement or intelligence related legislation may override the protections in this Part, including this offence.

79. This offence only relates to COVID app data on communication devices as communication devices cannot be afforded the same protections as COVID app data that has been uploaded to the National COVIDSafe Data Store. Should any person attempt to collect data from the National COVIDSafe Data Store, unless it was through a permitted purpose provided in subsection 94D(2)(b), that person would be in breach of subsection 94D(1).

80. There is no exception provided for COVIDSafe users to decrypt their own COVID app data as that data also relates to other COVIDSafe users, and decrypting that information may infringe upon their privacy.

81. Cyber-security researchers may examine whether there are any security issues relating to the standard of encryption that has been used to protect COVID app data on communication devices, however the act of decrypting, or attempting to decrypt (see section 11.1 of the Criminal Code Act 1995) COVID app data would constitute an offence.

Section 94H – Requiring the use of COVIDSafe

82. Section 94H provides for two offences. The purpose of these offences taken together is to ensure that no person can require, coerce, or otherwise oblige (whether directly or indirectly) any other person to install or have COVIDSafe operating on their communication device, or to upload COVIDSafe data from a communication device to the National COVIDSafe Data Store.
83. Each of the offences under section 94H attracts a maximum penalty of five years imprisonment or 300 penalty units, or both.

84. Subsection 94H(1) provides that a person commits an offence if that person requires another person to do any of the following:
   
   a. Download COVIDSafe to a communication device;
   
   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.

85. Subsection 94H(2) requires that a person cannot cause another person disadvantage by virtue of that person not having COVIDSafe installed, not having COVIDSafe operating on the person’s communication device; or not consenting to uploading COVID app data from a communication device to the National COVIDSafe Data Store. A person cannot take any of the following actions against another person on the basis that the second person had not taken any of the aforementioned actions:
   
   a. Refusing to enter into, or continue, a contract or arrangement with another person (paragraph 94H(2)(a))
   
   b. Taking adverse action (within the meaning of the Fair Work Act 2009) against another person (paragraph 94H(2)(b))
   
   c. Refusing to allow another person to enter either premises that are otherwise accessible to the public, or premises that the other person has a right to enter (subparagraphs 94H(2)(c)(i) and 94H(2)(c)(ii))
   
   d. Refusing to allow another person to participate in an activity (paragraph 94H(2)(d))
   
   e. Refusing to receive goods or services from another person or insisting on providing less monetary consideration for the goods or services (paragraph 94H(2)(e))
   
   f. Refusing to provide goods or services to another person or insisting on receiving more monetary consideration for the goods or services (paragraph 94H(2)(f)).

86. Paragraphs 94H(2)(a) and 94H(2)(b) are intended to protect employees from disadvantageous action being taken against them by their employer on the basis that the employee refuses to take specific actions in regard to COVIDSafe. It is intended that refusing to allow an employee to enter their normal workplace, even if the workplace does not fall within the premises listed in paragraph 94H(2)(c), would constitute a contravention of paragraphs 94H(2)(a), 94H(2)(b), 94H(2)(d) or 94H(2)(e) in that an employer is disadvantaging an employee, either through failure to allow an employee to continue their work contract, constituting adverse action, refusing to receive services from a person, or refusing to allow a person to participate in an activity.
87. Paragraph 94H(2)(c) is intended to limit the application of this offence to ensure that persons at private properties or residences are able to control who enters that premises on any basis. Though the effect of subparagraph 94H(2)(c)(i) is clear in its reference to otherwise publicly accessible locales, subparagraph 94H(2)(c)(ii) is equally required to protect against unlawful disadvantage. Subparagraph 94H(2)(c)(ii) is required to ensure that persons such as landlords or co-tenants do not place requirements on other tenants, subletters or similar. A person still commits an offence if their exclusion of a person from a premises does not fall within the scope of paragraph 94H(2)(c) if the conduct of the person also falls into another category under subsection 94H(2).

88. Paragraph 94H(2)(d) refers to prohibiting a person participating in an ‘activity’. It is intended that ‘activity’ be interpreted broadly to ensure that people are not excluded from events, working, sports, religious services, or another act that may be described as an activity.

89. Paragraphs 94H(2)(e) and 94H(2)(f) prohibit refusing to provide or receive goods or services, or to provide or receive goods and services on the same terms, on the basis of failure to take actions relating to COVIDSafe. It is intended that ‘goods or services’ be interpreted broadly, noting that the term attracts a degree of commerciality, and is not expected to extend to ‘gifting’ or other social interactions. The references to insisting on providing less monetary consideration for goods and services, or receiving more monetary consideration for goods and services, is intended to deal with cases where, for example, a person insists on offering a better or worse price for a person depending on whether they are using COVIDSafe.

90. Where a person’s conduct falls within two overlapping paragraphs in subsection 94H(2), the person can only be convicted of a single offence under subsection 94H(2) in relation to that conduct.

91. Subsection 94H(3) includes an avoidance of doubt provision that subsection (2) is workplace law and the benefits derived by a person under that subsection are a workplace right for the purposes of the Fair Work Act 2009. The intent of subsection 94H(3) is to clarify the interaction between subsection 94H and the treatment of workplace laws and workplace rights under the Fair Work Act 2009.

Section 94J – Extended geographical jurisdiction for offences

92. Section 94J provides that section 15.1 of the Criminal Code 1995, being Category A in regard to extended geographical jurisdiction, applies to all offences in Division 2 of this Part.

93. Category A, in regard to extended geographical jurisdiction, means that offences in this Division constitute an offence irrespective of the geographical location of where that offence occurred (for example, an act done wholly outside Australia which meets the requirements of an offence under this Division would constitute an offence).
Part VIIIA – Division 3 – Other obligations relating to COVID app data and COVIDSafe

94. This Division sets out requirements in relation to the deletion of data, both from a COVIDSafe user’s communication device, and from the National COVIDSafe Data Store after COVIDSafe is no longer required; retention of COVID app data on a COVIDSafe user’s communication device; and obligations on any person who received COVID app data in error.

95. For a person whose acts and practices are subject to the Privacy Act (including due to the operation of sections 94R and 94X, as discussed below), a failure to comply with a section in this Division constitutes an interference with privacy under the Privacy Act and enlivens the enforcement powers of the Commissioner.

Section 94K – Retention of COVID app data

96. Section 94K places an obligation on the data store administrator to take all reasonable steps to ensure that COVID app data is not retained on a COVIDSafe user’s communication device for a period longer than 21 days. In circumstances where it is not possible to ensure that data is not retained for longer than 21 days, the data store administrator must ensure that the data is not retained for a period longer than the shortest practicable period.

97. This obligation ensures that the data store administrator administers COVIDSafe in a manner that ensures that COVID app data collected on COVIDSafe users’ communication devices is deleted on a rolling 21 day basis. The purpose of this requirement is to recognise that data about a COVIDSafe user’s interaction with other users across the previous 21 day period is the extent of COVIDSafe data that is needed to perform effective contact tracing. The approach in section 94K, by limiting the duration of COVID app data that is retained on a communication device to 21 days, provides the scope of COVID app data that can be uploaded to the National COVIDSafe Data Store is only the minimum COVID app data needed the enable contact tracing.

98. Paragraph 94K(b) states that where it is not possible to ensure that data is retained for a period not longer than 21 days, the data store administrator must ensure that the extended period is the shortest practicable period. The subsection recognises that there may be circumstances where a communication device retains COVID app data for longer than 21 days, for example, where the device has been turned off at the end of the 21-day period. Where a situation of this kind occurs, the data store administrator must ensure that COVIDSafe is administered in a manner that ensures that COVID app data which has been retained for longer than 21 days is not retained for a period longer than the shortest practicable period necessary for that data to be deleted from the communication device.

Section 94L – Deletion of registration data on request

99. Subsection 94L(1) provides that a COVIDSafe user or former COVIDSafe user may request that the data store administrator delete any registration data of the user that has been uploaded from the user’s communication device to the National COVIDSafe Data Store. Where a COVIDSafe user makes this request, the data store administrator must take all reasonable steps to delete that data, and if it is not practicable to delete that data immediately, the data store administrator must not use or disclose that data for any purpose.
100. The purpose of this section is to ensure that COVIDSafe users who no longer wish for the National COVIDSafe Data Store to hold their registration data can request that the data store administrator delete the data. The effect of deleting registration data is that interactions with the user by other users cannot be linked back to the person whose registration data has been removed from the National COVIDSafe Data Store. It is however, not practicable for the data store administrator to delete all interactions that the requesting COVIDSafe user has had with other users. The fact that this information is not effective without a user’s registration data is the reason a deletion request under section 94L may not extend to all COVID app data relating to the user.

101. Paragraph 94L(1)(b) specifies that where it is not practicable to immediately delete the relevant registration data, the data store administrator must not use or disclose that data for any purpose. This subsection recognises the technical practicalities that data cannot be completely deleted immediately after a request is made. Paragraph 94L(1)(a) would place an ongoing obligation on the data store administrator to ensure that the data is deleted, however paragraph 94L(1)(b) provides an additional safeguard where that data cannot be used or disclosed should there be any delay in deletion due to the impact of practical limitations.

102. Subsection 94L(2) allows a request for deletion of registration data relating to a COVIDSafe user to be made by that user’s parent, guardian or carer in circumstances where the COVIDSafe user is either unable to make the request, or where that user has requested that their parent, guardian or carer make the request on their behalf. The purpose of subsection 94L(2) is to ensure that vulnerable persons such as persons with disability, children or the elderly, who use COVIDSafe and wish for their registration data to be deleted, are not disadvantaged on the basis of being unable to make a request themselves.

103. Paragraph 94L(3)(a) provides that the data store administrator is not prevented from accessing data for the purpose of, and only to the extent required for the purpose of, confirming the correct data has been deleted. The purpose of this paragraph is to clarify that the actions of the data store administrator in confirming that the relevant and correct data has been deleted is specifically permitted in the course of responding to a request for deletion of initial registration data. A similar provision has also been included in paragraph 94D(2)(g) to ensure that the data store administrator does not commit an offence under section 94D when accessing COVID app data for this purpose. (Noting it is not necessary to include a similar provision in section 94D applying to the actual deletion of registration data under section 94L, given this would not be a ‘use’ of COVID app data and would not attract any penalty under subsection 94D(1)).

104. Paragraph 94L(3)(b) has the effect of limiting the scope of the COVID app data that the data store administrator is required to delete. The data store administrator is not required to delete data that was uploaded from another COVIDSafe user’s device in relation to the other user’s interactions with the requesting user, or any data that has been uploaded from the requesting user’s device in relation to their interaction with other users. The purpose of this limitation is discussed above in relation to this section.

105. Failure to comply with this provision constitutes an interference with privacy under section 13 of the Privacy Act.

Section 94M – Deletion of data received in error
Section 94M creates an obligation on a person who receives COVID app data in error. This obligation requires that, where a person receives COVID app data in error, that person must as soon as practicable delete the data and notify the data store administrator that the data had been received in error. The section will not apply during the course of the ordinary operation and administration of the COVIDSafe app and the National COVIDSafe Data Store, or where COVID app data is subsequently used or disclosed for one of the limited purposes permitted under Part VIIIA.

The purpose of this section is to ensure that, where COVID app data has been mistakenly provided to a person whose acts and practices are subject to the Privacy Act (including due to the operation of Part VIIIA), that person must take practical steps to delete the data. The chapeau of section 94M refers to these practicable steps as a person may not be aware that they have received COVID app data, or may not know that the data is COVID app data. Therefore, as soon as practicable after the person realises that they received COVID app data, the deletion and notification obligations take effect.

The notification requirement in subsection 94M(b) ensures that the data store administrator is aware and can take appropriate steps to rectify any unintended provision of COVID app data to any person. The provision of data to a person in error may constitute an eligible data breach for the purpose of section 94S of this Part.

Failure to comply with section 94M is an interference with privacy under section 13 of the Privacy Act. However, while a person who receives data in error does not necessarily collect the information, any further use or disclosure of that data would fall within the offence in subsection 94D(1). Deleting COVID app data in accordance with paragraph 94M(a) would not be a use of COVID app data and would not attract any penalty under subsection 94D(1).

Section 94N – Effect of deletion of COVIDSafe from a communication device

Subsection 94N states the effect of deletion of COVIDSafe from a communication device.

Subsection 94N(1) prevents the data store administrator from collecting COVIDSafe information from a person through a device from which that person has uninstalled COVIDSafe.

A contravention of subsection 94N(1) by the data store administrator is an interference with privacy under section 13 of the Privacy Act.

Subsection 94N(2) defines a ‘former COVIDSafe user’ to be a person, in relation to a communication device, that has deleted COVIDSafe from a device in relation to which the person was a COVIDSafe user, if the person has not reinstalled COVIDSafe on that device since that time.

Following the reasoning in the description of the definition of ‘COVIDSafe user’, the definition of ‘former COVIDSafe user’ relates to a person’s interaction with a particular device, rather than an overall account. This has been included as a person may have multiple devices with COVIDSafe installed, and a person who has registered separately on each of those devices would be a COVIDSafe user in relation to each of those devices. The effect of deleting COVIDSafe from a single device creates the effect that a person may be a COVIDSafe user in regards to one device, but a former COVIDSafe user in regards to
another device. For a person to require that the data store administrator is prevented under section 94N from collecting any further information about them, they would need to be a former COVIDSafe user in relation to all devices for which they were a COVIDSafe user.

Section 94P – Obligations after the end of the COVIDSafe data period

115. Section 94P contains the obligations on the data store administrator once the Health Minister has issued a determination under section 94Y of this Part which determines the end date of the COVIDSafe data period.

116. Subsection 94P(1) relates to the ceasing of acts and practices by the data store administrator that facilitate the collection of COVID app data. This subsection requires that after the date determined by the Minister for Health under subsection 94Y(1), the data store administrator must not collect any COVID app data or make COVIDSafe available to download.

117. Paragraph 94P(1)(a) requires that the data store administrator not collect any COVID app data, meaning that the data store administrator must not allow further registrations to be uploaded, or allow any further information about users’ interactions to be uploaded to the National COVIDSafe Data Store. This paragraph sets out the first stage in the overall deletion of centrally-held COVID app data by ensuring that no further COVID app data is collected once the date determined is reached.

118. Paragraph 94P(1)(b) requires that the data store administrator must not make COVIDSafe available to be downloaded once it is no longer required for contact tracing. This is intended to ensure COVIDSafe will no longer be accessible to new COVIDSafe users.

119. Subsections 94P(2) and (3) place requirements on the data store administrator in relation to deleting COVID app data in the National COVIDSafe Data Store.

120. The data store administrator must, as soon as reasonably practicable, ensure that all COVIDSafe data is deleted after the day determined. Subsection 94P(2) is an unambiguous and absolute requirement that all COVID app data must be deleted from the National COVIDSafe Data Store at the end of the COVIDSafe data period.

121. Subsection 94P(3) contains requirements for the data store administrator to make various notifications after all COVID app data has been deleted from the National COVIDSafe Data Store under subsection 94P(2). Under paragraph 94P(3)(a), the data store administrator must notify the Health Minister and the Commissioner of the deletion. Under paragraph 94P(3)(b), the data store administrator must take all reasonable steps to inform current COVIDSafe users that the deletion has occurred, that COVID app data can no longer be collected, and that they should delete COVIDSafe from their communication devices. Paragraph 94P(3)(b) is intended to work in such a way that the notification requirement can be met through a broad range of communication activities, such as public announcements and related communications activities.

Part VIII A – Division 4 – Application of general privacy measures

Section 94Q – COVID app data is taken to be personal information
122. Section 94Q provides that COVID app data relating to an individual is taken, for the purposes of the Privacy Act, to be personal information about the individual. This has been included to ensure that COVID app data is considered to be ‘personal information’ under the Privacy Act, given that existing definition of that term in subsection 6(1) of the Privacy Act refers (in summary) to information or opinion ‘about’ an identified or reasonably identifiable individual.

Section 94R – Breach of requirement is an interference with privacy

123. Section 94R provides that an act or practice in breach of a requirement of Part VIIIA in relation to an individual constitutes an act or practice involving an interference with the privacy of that individual for the purposes of section 13. The note in this section clarifies that because a breach of a requirement in Part VIIIA will also constitute an interference with privacy, individuals will be able to make complaints to the Commissioner about potential breaches of Part VIIIA in accordance with the complaint procedure detailed in section 36. Subsection 94R(1) is not, however, intended to have the effect that an act or practice that would be exempt under the ordinary operation of the Privacy Act (that is, other than because of the operation of Part VIIIA) would be an ‘interference with the privacy of an individual’.

124. Subsections 7(1A) and (1B) would normally operate to provide exemptions for the disclosure of personal information to the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Australian Signals Directorate and the Office of National Intelligence. This Clause provides that these exemptions do not apply. A disclosure in breach of a requirement of Part VIIIA in relation to an individual to one of the agencies listed in subsection 7(1A) or (1B) will still constitute an interference with the privacy of that individual. The reference to subsection 7(1B) is not intended to extend the coverage of Part VIIIA to a disclosure by an agency with an intelligence role or function where the disclosure would otherwise be exempt under section 7. The scope of the Commissioner’s jurisdiction in relation to an ‘act or practice’ under the Privacy Act would remain the same under this Part, but for subsections 7(1A) and (1B) being expressly disapplied.

125. It is not necessary for section 94R to include an equivalent to section 94J in Division 2, which deals with the extended geographical jurisdiction for offences in that Division. For an interference with privacy under section 94R, it is intended that the Privacy Act’s existing extraterritorial operation under section 5B of the Act would automatically apply.

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

126. This section imposes data breach notification requirements on the data store administrator (including in relation to a data breach of a contracted service provider of the data store administrator) and a State or Territory health authority handling COVID app data (including in relation to a data breach of a person in the service of the State or Territory health authority). These data breach notification requirements are intended to maintain consistency with the Notifiable Data Breaches scheme in existing Part IIIC of the Privacy Act.

127. Subsections 94S(1) and (2) have the effect that any breach of the Part by the data store administrator (or a contracted service provider to the data store administrator), or a State or Territory health authority (or a person in the service of the State or Territory health authority), is taken to be an ‘eligible data breach’ of the data store administrator or of the State or Territory health authority, as the case may be. ‘Eligible data breach’ is defined in
existing subsection 26WE(2) of the Privacy Act, and under that provision determining whether unauthorised access, unauthorised disclosure or loss of personal information is an ‘eligible data breach’ requires an assessment of the harm that would or may result to an individual. That kind of harm assessment will not be required in relation to any breach of this Part, as the breach will automatically be considered an ‘eligible data breach’ for the purposes of section 26WE(2).

128. Paragraphs 94S(1)(e) and (2)(d) have the effect that, for an eligible data breach of that kind, any individual to whom the COVID app data in question relates is taken to be ‘at risk’ from the eligible data breach. The term ‘at risk’ is part of the definition of an ‘eligible data breach’ in existing Privacy Act paragraph 26WE(2)(d). Paragraphs 94S(1)(e) and (2)(d) have been included for technical reasons, given the ordinary operation of existing Privacy Act Part IIIC requires (in summary) assessing whether an individual is ‘at risk’ from an eligible data breach. Where Part IIIC requires an entity to (in summary) provide a notice to the Commissioner under section 26WK about such an eligible data breach, the entity will also always need to either take reasonable steps under section 26WL to notify the contents of the notice to individuals ‘at risk’ from the eligible data breach, where it is practicable to do so.

129. Once the data store administrator or a State or Territory health authority has reasonable grounds to believe that an eligible data breach is taken to have occurred for the purposes of subsection 94S(1) or (2), subsection 94S(3) will require the data store administrator or the State and Territory health authority (as the case may be) to notify the Commissioner of the breach.

130. The effect of paragraph 94S(3)(a) is to make clear that existing provisions of Part IIIC relating to assessing harm and undertaking an assessment of a potential data breach do not apply to a potential data breach of this kind. This is because they will have no role to play where an eligible data breach is taken to have occurred under subsection 94S(1) or (2), because notification to the Commissioner will be required regardless of the risk of harm to individuals.

131. Subparagraph 94S(3)(b)(i) contains the specific obligation for the data store administrator or a State and Territory health authority to notify the Commissioner. The effect of subparagraph 94S(3)(b)(ii) is that the Commissioner may then require the data store administrator or the State and Territory health authority to comply with the obligations in existing sections 26WK and 26WL to prepare a notice containing specific information about the eligible data breach, provide that notice to the Commissioner, and take reasonable steps to convey the contents of the notice to individuals at risk of harm (which in this case will cover all individuals to whom the COVID app data in question relates, because of paragraphs 94S(1)(e) and (2)(d)).

132. Paragraph 94S(3)(c) has been included to ensure that, where the Commissioner requires the data store administrator or State and Territory health authority to notify the eligible data breach under subparagraph 94S(3)(b)(ii), various exemptions that would apply under the ordinary operation of existing Part IIIC will not be available. Before outlining those exemptions, it is useful to note that neither subsection 94S(3) nor any other part of section 94S is intended to exclude the operation of:

   a. Existing Privacy Act section 26WM, which might have some operation in relation to an eligible data breach notified under new section 94S where, for example, the Commissioner requires notification in cases where the same
eligible data breach is simultaneously a data breach of two entities exercising different functions as the data store administrator. If this occurs, the effect of section 26WM is that once either entity has notified the eligible data breach, both entities will be taken to have met their data breach notification obligations under the Privacy Act.

b. Existing Privacy Act section 26WR, which (in summary) allows the Commissioner to issue a direction requiring an entity to notify an eligible data breach, where the Commissioner has reasonable grounds to believe that an eligible data breach of the entity has occurred.

133. Paragraph 94S(3)(c) does, however, have the effect of excluding the exemptions for law-enforcement related activities (sections 26WN and 26WS) and cases where an inconsistency with a secrecy provision arises (sections 26WP and 26WT) that would normally be available when an entity is complying with existing sections 26WK and 26WL, either on the entity’s own initiative or following a direction from the Commissioner under section 26WR. This means that these exemptions will not be available where the Commissioner requires the data store administrator or State or Territory health authority to notify an eligible data breach involving a breach of this Part under subparagraph 94S(3)(b)(ii) or section 26WR.

134. Paragraph 94S(3)(c) also has the effect of excluding the Commissioner’s discretion under section 26WQ in the ordinary operation of Part IIIC to grant an exemption or a time-limited exemption from the obligation to notify an eligible data breach. However, subsections 94S(4) and (5) have been included with similar effect to ensure that section 94S does not inadvertently undermine the policy intention of the existing Part IIIC data breach notification requirements. This policy intention (in summary) is to require notification of an eligible data breach that holds a likely risk of serious harm to individuals, unless the Commissioner considers it reasonable in the circumstances to grant an exemption.

135. The effect of subsection 94S(4)(a) is that the Commissioner must, under subparagraph 94S(3)(b)(ii), require notification of an eligible data breach involving a breach of the Part where the eligible data breach may give rise to a likely risk of serious harm to any individual to whom the COVID app data relates (paragraph 94S(4)(a)). This would not limit the Commissioner’s discretion to require an eligible data breach to be notified in cases where the harm to the individual or individuals in question may not rise to the level of a likely risk of serious harm.

136. However, the effect of paragraph 94S(4)(b) is that, in cases where the Commissioner considers that an eligible data breach involving a breach of the Part may hold a likely risk of serious harm, the Commissioner would retain a discretion to grant either an exemption or a time-limited exemption from complying with sections 26WK and 26WL. This discretion would be available where the Commissioner is satisfied on reasonable grounds that requiring compliance with sections 26WK and 26WL, or requiring compliance with sections 26WK and 26WL within the usual timeframes that apply under those sections, would not be reasonable in the circumstances. An example might be if the Commissioner considered on reasonable grounds that notifying a breach of the Part as an eligible data breach might compromise a police investigation into whether that breach constitutes a criminal offence. In that case, the Commissioner could, for example, decide to grant a time-limited exemption
from the notification requirement until the point where notification would no longer compromise the investigation.

137. In deciding whether to exercise the discretion in subsection 94S(5), the Commissioner would need to have regard to a list of matters that match the matters to which the Commissioner must have regard before granting an exemption under existing subsection 26WQ(3). These include:

   a. the public interest (paragraph 94S(5)(a));

   b. any relevant advice to the Commissioner from a law enforcement body or the Australian Signals Directorate (paragraph 94S(5)(b), noting the Commissioner is neither required to seek out nor follow such advice, and can also have regard to any other advice (subsection 94S(6)); and

   c. any other matters the Commissioner considers relevant (paragraph 94S(5)(c)).

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

138. Subsection 94T(1) extends the Commissioner’s assessment power under section 33C and allows the Commissioner to conduct assessments of whether the acts or practices of an entity (which includes the data store administrator) or a State or Territory health authority in relation to COVID app data comply with the requirements of Part VIII A.

139. Subsection 94T(2) allows the Commissioner to give a notice to the entity or State or Territory health authority being assessed under subsection 94T(1), requiring the entity or authority to give the Commissioner information or produce a document relevant to the assessment. The notice must specify a time period of not less than 14 days in which the information or the document must be produced to the Commissioner.

140. Subsection 94T(2) also makes clear that the subsection does not limit the Commissioner’s discretion under subsection 33C(2) to conduct an assessment in the manner the Commissioner sees fit.

141. The note at the end of section 94T refers to the criminal offence under existing Privacy Act section 66 for failure to give information or produce a document to the Commissioner when required to do so under the Privacy Act (unless an exemption applies). Failure of this kind carries a penalty of imprisonment for 12 months, a fine of 20 penalty units ($4,200 in current terms), or both for an individual, and a fine of 100 penalty units ($21,000 in current terms) for a body corporate.

Section 94U – Investigations under section 40 to cease if COVID app data offence may have been committed

142. Section 94U provides that, if in the course of an investigation under Privacy Act section 40, the Commissioner forms the opinion that a criminal offence or ancillary offence against Division 2 may have been committed, the Commissioner must inform the Commissioner of Police or the Director of Public Prosecutions that an offence may have been committed. This section is intended to ensure that responsibility for investigating a contravention of the offences under Part VIII A is clear.
Section 94U has largely been designed to match the processes that apply under existing sections 49 and 49A of the Privacy Act where the Commissioner forms the opinion that certain kinds of criminal offences may have been committed. The main difference is that, whereas sections 49 and 49A require the Commissioner to cease investigating after informing the Commissioner of Police or the Director of Public Prosecutions of the Commissioner’s opinion, section 94U allows the Commissioner to continue investigating in some circumstances.

In the case of an investigation under Privacy Act subsection 40(1), that is, an investigation following a complaint to the Commissioner, paragraph 94U(2)(b) would require the Commissioner to give a copy of the complaint to the Commissioner of Police or the Director of Public Prosecutions. More generally, however, in relation to any investigation under Privacy Act section 40, it is intended that the Commissioner would have discretion to provide information that was critical to the Commissioner forming the opinion that an offence or ancillary offence may have been committed to the Commissioner of Police or the Director of Public Prosecutions.

Subsection 94U(2)(c) provides that the Commissioner must then discontinue the investigation except to the extent that it concerns matters unconnected with the offence that may have been committed, unless subsection 94U(5) applies, which involves two possible scenarios:

a. Firstly, subsection 94U(3) provides that, if the Commissioner of Police or the Director of Public Prosecutions decides not to investigate or prosecute the offence, the Commissioner of Police or the Director of Public Prosecutions must give written notice to that effect to the Commissioner under subsection 94U(3).

b. Secondly, subsection 94U(4) provides that, if the Commissioner of Police or the Director of Public Prosecutions is satisfied that a police investigation or criminal proceedings will not be jeopardised or otherwise affected by the Commissioner continuing to investigate the matter under the Privacy Act, the Commissioner of Police or the Director of Public Prosecutions may give written notice to that effect to the Commissioner under subsection 94U(4).

Upon receiving a notice under subsection 94U(3) or 94U(4), subsection 94U(5) provides that the Commissioner may continue the investigation which was previously discontinued.

Section 94V – Referring COVID app data matters to State or Territory privacy authorities

Section 94V allows the Commissioner to transfer a complaint made under section 36 of the Privacy Act about a potential breach of a requirement in Part VIIIA to a State or Territory privacy authority. This complaint transfer mechanism is intended to reduce the administrative burden on the Commissioner to investigate complaints made about COVID app data. It also reflects the expectation that the Commissioner may receive privacy complaints about State or Territory health authorities that fall outside the scope of Part VIIIA but may involve a breach of applicable State or Territory privacy legislation.

This section also recognises that State and Territory privacy authorities may be best placed to investigate State and Territory health authorities in some circumstances. Complaints
will only be transferred if the complainant could have made the complaint to the relevant State or Territory privacy authority and the complaint could be more conveniently or effectively dealt with by that authority.

149. Subsection 94V(2) provides that if the Commissioner transfers a complaint, the complainant must be notified in writing and the Commissioner must give information or documents that relate to the complaint and are in the Commissioner’s possession or control.

150. Once a complaint has been transferred to a State or Territory privacy authority, subsection 94V(3) provides that the complaint is taken to have been made to that State or Territory privacy authority for the purposes of the Privacy Act. This means that the State or Territory privacy authority will be able to investigate the complaint in accordance with the authority’s standard procedures.

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

151. Subsection 94W(1) allows the Commissioner to share information or documents with a State or Territory privacy authority for the purpose of the Commissioner exercising powers, or performing functions or duties under the Privacy Act in relation to the requirements of Part VIIIA or to allow a State or Territory privacy authority to exercise its powers, or perform its functions or duties. This section reflects the expectation that the Commissioner may need to, and should be able to, work closely with the Commissioner’s counterparts in State or Territory privacy authorities (however such authorities are structured or described), given that Part VIIIA imposes obligations on State and Territory health authorities.

152. Subsections 94W(2) and (3) deal with how the Commissioner may share information or documents with State or Territory privacy authorities, which is expected to most commonly involve the Commissioner sharing information or documents about a State or Territory health authority. Subsection 94W(2) provides that the Commissioner may share information or documents with a State or Territory privacy authority if the information or documents were acquired by the Commissioner in the course of exercising powers, or performing functions or duties under the Privacy Act and 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. However, subsection 94W(3) makes clear that the Commissioner is not required to transfer a complaint or part of a complaint to a State or Territory privacy authority under section 94V in order to share information or documents with a State or Territory privacy authority under section 94W.

Section 94X – Application to State or Territory health authorities

153. Section 94X extends the operation of the Privacy Act to State and Territory health authorities. The Privacy Act will apply to a State or Territory health authority as if the authority were an organisation for the purposes of the Privacy Act, to the extent that the authority deals with COVID app data. This will require State and Territory health authorities to comply with the Privacy Act in their handing of COVID app data and allow individuals to make complaints to the Commissioner about State and Territory health authorities’ handling of COVID app data.

154. A consequence of extending the Privacy Act to cover State and Territory health authorities in this way is that, except where Part VIIIA imposes stricter requirements and
where paragraph 94X(2)(a) does not apply (as discussed below), the Australian Privacy Principles (APPs) will apply to COVID app data that a State or Territory health authority holds. In practice, the stricter requirements in Part VIIIA are expected to form the main obligations of State and Territory health authorities under the Privacy Act due to the operation of section 94X. However, some obligations under the APPs are expected to continue to apply, such as obligations to maintain a privacy policy in relation to COVID app data under APP 1, to take such steps (if any) as are reasonable to notify an individual of the collection of COVID app data relating to them under APP 5, and to take reasonable steps to ensure that COVID app data is held securely under APP 11. The Commissioner will also have the discretion to issue guidance material for State or Territory health authorities about their obligations under the Privacy Act when the new Part commences.

155. Subsection 94X(2) qualifies the effect of section 94X:

a. Paragraph 94X(2)(a) provides that APP 9 of the Privacy Act will not apply to a State or Territory health authority in relation to a ‘government-related identifier’ (which is defined in existing Privacy Act subsection 6(1)) issued by that State or Territory, or a State or Territory authority in that jurisdiction. This is necessary because section 94X provides that State or Territory health authorities handling COVID app data are taken to be ‘organisations’ for the purposes of the Privacy Act (as defined in existing subsection 6(1)), and the ordinary operation of APP 9 restricts how an organisation can make use of government-related identifiers issued by the Commonwealth or a State or Territory authority. It would not be appropriate for APP 9 to restrict how a State or Territory health authority can handle a government-related identifier from the same jurisdiction when dealing with or undertaking activities related to COVID app data.

b. Paragraph 94X(2)(b) has been included to make clear that subsection 94X(1) does not extend the operation of the Privacy Act to cover how a State or Territory Government handles data or information other than COVID app data. This reflects the distinction in the definition of COVID app data in subsection 94D(5) between data that was collected or generated through the operation of COVIDSafe and stored on a communication device and information obtained from sources other than the National COVIDSafe Data Store. For the purposes of section 94X, this distinction is intended to operate so that, after obtaining COVID app data from the National COVIDSafe Data Store, any information a State or Territory health authority subsequently obtains during the contact tracing process would not be subject to the Privacy Act (though applicable State or Territory laws may protect such information).

Part VIIIA – Division 5 – Miscellaneous

Section 94Y – Determining the end of the COVIDSafe data period

156. Section 94Y sets out the process for determining the end of the COVIDSafe data period. The end of the COVIDSafe data period is the date by which the Health Minister is satisfied that the COVIDSafe app is no longer required, or 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. When the Health Minister is satisfied that this criteria is met, the Health Minister must, by notifiable instrument, determine
the end of the COVIDSafe data period. This provision 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.

157. The Health Minister must not determine the end of the COVIDSafe data period unless the Health Minister has consulted, or considered recommendations from, the Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee. The Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee may at their own initiative recommend that the Health Minister determine the end of the COVIDSafe data period: subsection 94Y(3).

Section 94Z – Agencies may be determined to be data store administrator

158. Section 94Z allows the Secretary of the Health Department to determine, by notifiable instrument, that another agency is the data store administrator for the purposes of one or more provisions of Part VIIIA. The Secretary’s determination may limit the extent to which the agency is the data store administrator for those purposes. The role of the data store administrator is required to ensure the proper functioning of the COVIDSafe app, for example to execute data deletion requests from COVIDSafe users and to administer State and Territory health authorities’ access to the National COVIDSafe Data Store. The data store administrator is also required to ensure the ongoing integrity and security of the COVIDSafe app, and can produce de-identified statistical information about the total number of registrations through COVIDSafe. This section anticipates that the Health Department may require the support of other agencies in the administration of the National COVIDSafe Data Store and will allow the Secretary of the Health Department (subject to some restrictions) to leverage relevant expertise from across the Commonwealth Government in the administration of the National COVIDSafe Data Store.

159. ‘Agency’ is a defined term in Privacy Act subsection 6(1) applying to Commonwealth Government entities. Subsection 94Z(3) has the effect of limiting the Secretary’s ability to determine that a particular agency is the data store administrator for the purposes of one or more provisions of Part VIIIA. Specifically, the Secretary must not make a determination in relation to any of the following agencies:

   a. Due to paragraph 94Z(3)(a): the Australian Federal Police, the Australian Commission for Law Enforcement Integrity, the Australian Criminal Intelligence Commission, the Department of Home Affairs, the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission or the Commonwealth Director of Public Prosecutions, as agencies named in paragraphs (a) to (ea) of the definition of ‘enforcement body’ in subsection 6(1) of the Privacy Act, which together comprise all named Commonwealth bodies that fall under that definition.

   b. Due to paragraph 94Z(3)(b): the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Australian Signals Directorate and the Office of National Intelligence, as agencies named in the definition of ‘intelligence agency’ in subsection 6(1) of the Privacy Act.

   c. Due to paragraphs 94Z(3)(c) and (d): the Australian Geospatial-Intelligence Organisation and the Defence Intelligence Organisation, which have been included in these paragraphs because they are not included in the definition of
‘intelligence agency’ in subsection 6(1) of the Privacy Act, given that
definition is not used in the Privacy Act to provide an exhaustive list of the
agencies in the Australian intelligence community.

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

160. Section 94ZA introduces a requirement for the Health Minister to prepare reports on
the operation and effectiveness of the COVIDSafe app and the National COVIDSafe Data
Store as soon as practicable after the end of each six month period beginning from the
commencement of Part VIIIA (paragraph 94ZA(1)(a)). The Health Minister would,
additionally, be required to produce a further report as soon as practicable following a six
month period after the Minister determines a day under subsection 94Y(1), which is intended
to ensure a final report is prepared once COVIDSafe and the National COVIDSafe Data Store
have ceased operation (paragraph 94ZA(1)(b)).

161. The note following subsection 94ZA(1) describes the effect of section 94D, which
would prohibit the Health Minister’s reports from containing COVID app data. As the
definition of COVID app data does not include de-identified statistical information produced
by the data store administrator about the total number of COVIDSafe registrations
(paragraph 94D(5)(d)), this information could be included in the Health Minister’s reports
under section 94ZA. However, it is not expected the reports could contain any information
that identifies or could be reasonably used to identify an individual. For an abundance of
clarity, the note states that section 94ZA is not intended to expand the list of permitted
collections, uses or disclosures in subsection 94D(2).

162. Subsection 94ZA(2) has been included to ensure that, if the Health Minister
determines a day under subsection 94Y(1) less than six months after the Part commences, the
Minister would still be required to produce a report under section 94ZA within 3 months after
the day determined under subsection 94Y(1).

163. Subsection 94ZA(3) requires the Health Minister to table the report prepared under
this section in Parliament within 15 sitting days after the report has been prepared.

Section 94ZB – Reports by the Commissioner

164. Section 94ZB complements the Health Minister’s reporting obligation under
section 94ZA by introducing a requirement for the Commissioner to publish regular reports
on the Commissioner’s website about the Commissioner’s performance of functions and
exercise of powers under the Part. This is expected to provide another source of public
information and assurance about the operation of Part VIIIA, in addition to any public
statements the Commissioner may choose to make from time to time about the
Commissioner’s performance of functions and exercise of powers under Part VIIIA.

165. As with the Health Minister under section 94ZA, the Commissioner would be
required to prepare reports as soon as practicable after the end of each six month period
beginning from the commencement of Part VIIIA (paragraph 94ZB(1)(a)), and would
additionally be required to produce a further report as soon as practicable following a six
month period after the Health Minister determines a day under subsection 94Y(1) (paragraph
94ZB(1)(b)). Subsection 94ZB(2) would ensure that, if the Health Minister determines a day
under subsection 94Y(1) less than six months after the Part commences, the Commissioner
would still be required to produce a report under section 94ZB within 3 months after the day determined under subsection 94Y(1).

166. The note following subsection 94ZB(1), which is expressed in the same terms as the equivalent note in section 94ZA, describes the effect of section 94D, which would prohibit the Commissioner’s reports from containing COVID app data. As the definition of COVID app data does not include de-identified statistical information produced by the data store administrator about the total number of COVIDSafe registrations (paragraph 94D(5)(d)), this information could be included in the Commissioner’s reports. However, it is not expected the reports could contain any information that identifies or could be reasonably used to identify an individual. For an abundance of clarity, the note states that section 94ZB is not intended to expand the list of permitted collections, uses or disclosures in subsection 94D(2).

167. It is expected that the Commissioner’s reports would be similar to the periodic reports the Commissioner voluntarily publishes on the Commissioner’s website about the operation of the Notifiable Data Breaches scheme in Part IIIIC of the Privacy Act. The section 94ZB report might include, for example, information such as the number of complaints and eligible data breach notifications received under Part VIIIA, and the number of assessments, investigations and any other regulatory action commenced and/or undertaken under the Part.

168. Subsection 94ZB(3) requires the Commissioner’s reports be published on the Commissioner’s website.

169. Subsection 94ZB(4) clarifies that this reporting obligation does not affect the matters that section 30 of the Australian Information Commissioner Act 2010 requires to be included in the Commissioner’s annual report. The Commissioner will retain discretion about how to otherwise make appropriate public statements about the Commissioner’s performance of functions and exercise of powers under the new Part, and about how to best include details about these matters in the Commissioner’s annual report.

Section 94ZC – COVID app data remains property of the Commonwealth

170. Section 94ZC provides that 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 State or Territory health authority or any other person or body (other than the Commonwealth or an authority of the Commonwealth). Prescribing COVID app data as Commonwealth property ensures the requirements detailed in Part VIIIA continue to apply to any collection, use or disclosure of COVID app data, including in circumstances where COVID app data has been used or disclosed by State or Territory health authorities.

Section 94ZD – Operation of other laws

171. Subsection 94ZD(1) provides that all other statutory provisions will be superseded by Part VIIIA of the Privacy Act to the extent that there are inconsistencies in the manner in which COVID app data may be handled. For example, powers in the enabling legislation of law enforcement or other regulatory bodies which would otherwise allow for the collection, use or disclosure of COVID app data prohibited by Part VIIIA will be overridden to the extent of the inconsistency. The requirements in Part VIIIA operate in place of any more stringent requirements about retaining Commonwealth records, for example, under the Archives Act 1983.
172. However, subsection 94ZD(2) provides that Part VIIIIA will be overridden by a
provision of an Act that commences after the commencement of Part VIIIIA and expressly
permits or requires the conduct or omission despite the provisions of Part VIIIIA. Such a
provision would require Parliamentary consideration.

Schedule 2 – Repeals

173. The repeal made by item 1 of this Schedule commences the day after this Bill receives
Royal Assent. The repeals made by items 2 to 4 of this Schedule commence at the end of 90
days after the day determined by the Health Minister under subsection 94Y(1) of the
Privacy Act, as amended by this Part (for further details, see the description of section 94Y
above).

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

Clause 1 – The whole instrument

174. This Clause provides that the whole of the Determination will be repealed on the day
this Bill receives Royal Assent.

Privacy Act 1988

Clause 2 – Subsection 6(1)

175. This Clause provides that all definitions inserted into the Privacy Act by Item 1 of
Schedule 1 will be repealed from the Privacy Act at the end of 90 days after the day the
Health Minister makes a determination in relation to the end of the COVIDSafe data period
under subsection 94Y(1). These definitions are the:

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;
1. definition of *registration data*;

m. definition of *State or Territory health authority*;

n. definition of *State or Territory privacy authority*.

**Clause 3 – Part VIIIA**

176. This Clause provides that Part VIIIA will be repealed from the Privacy Act at the end of 90 days after the day the Health Minister makes a determination in relation to the end of the COVIDSafe data period under subsection 94Y(1).

**Clause 4 – Transitional**

177. Paragraph (a) of this Clause operates to ensure that the Commissioner’s full suite of regulatory powers under the Privacy Act to respond to a contravention or possible contravention of Part VIIIA will continue to apply after the repeal of Part VIIIA in relation to matters before repeal.

178. Paragraph (b) of this Clause operates to preserve the respective reporting obligations of the Health Minister under section 94ZA and the Commissioner under section 94ZB following the repeal of Part VIIIA. This will ensure that, if the Health Minister or Commissioner has not yet prepared the final report as required under section 94ZA or 9ZB at the time of repeal, the Minister or Commissioner will still be required to prepare that final report.