The Senate

Standing Committee for the Scrutiny of Bills

Scrutiny Digest 8 of 2020

17 June 2020

ISSN 2207-2004 (print)
ISSN 2207-2012 (online)

This document was prepared by the Senate Standing Committee for the Scrutiny of Bills and printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

Membership of the committee

Current members

Senator Helen Polley (Chair)	ALP, Tasmania
Senator Dean Smith (Deputy Chair)	LP, Western Australia
Senator the Hon Kim Carr	ALP, Victoria
Senator Perin Davey	NATS, New South Wales
Senator Janet Rice	AG, Victoria
Senator Paul Scarr	LP, Queensland

Secretariat

Mr Glenn Ryall, Secretary

Ms Alexandra Logan, Principal Research Officer

Ms Katie Helme, Senior Research Officer

Ms Sarah Batts, Senior Research Officer

Mr Andrew McIntyre, Senior Research Officer

Ms Georgia Fletcher, Legislative Research Officer

Committee legal adviser

Professor Leighton McDonald

Committee contacts

PO Box 6100
Parliament House
Canberra ACT 2600

Phone: 02 6277 3050

Email: scrutiny.sen@aph.gov.au

Website: http://www.aph.gov.au/senate_scrutiny

Contents

Introduction

Terms of reference

Since 1981 the Senate Standing Committee for the Scrutiny of Bills has scrutinised all bills against certain accountability standards to assist the Parliament in undertaking its legislative function. These standards focus on the effect of proposed legislation on individual rights, liberties and obligations, and on parliamentary scrutiny. The scope of the committee's scrutiny function is formally defined by Senate standing order 24, which requires the committee to scrutinise each bill introduced into the Parliament as to whether the bills, by express words or otherwise:

(i) trespass unduly on personal rights and liberties;

(ii) make rights, liberties or obligations unduly dependent upon insufficiently defined administrative powers;

(iii) make rights, liberties or obligations unduly dependent upon non-reviewable decisions;

(iv) inappropriately delegate legislative powers; or

(v) insufficiently subject the exercise of legislative power to parliamentary scrutiny.

Nature of the committee's scrutiny

The committee's long-standing approach is that it operates on a non-partisan and consensual basis to consider whether a bill complies with the five scrutiny principles. In cases where the committee has scrutiny concerns in relation to a bill the committee will correspond with the responsible minister or sponsor seeking further explanation or clarification of the matter. If the committee has not completed its inquiry due to the failure of a minister to respond to the committee's concerns, Senate standing order 24 enables Senators to ask the responsible minister why the committee has not received a response.

While the committee provides its views on a bill's level of compliance with the principles outlined in standing order 24 it is, of course, ultimately a matter for the Senate itself to decide whether a bill should be passed or amended.

Publications

It is the committee's usual practice to table a *Scrutiny Digest* each sitting week of the Senate. The Digest contains the committee's scrutiny comments in relation to bills introduced in the previous sitting week as well as commentary on amendments to bills and certain explanatory material. The Digest also contains responses received in relation to matters that the committee has previously considered, as well as the committee's comments on these responses. The Digest is generally tabled in the Senate on the Wednesday afternoon of each sitting week and is available online after tabling.

General information

Any Senator who wishes to draw matters to the attention of the committee under its terms of reference is invited to do so. The committee also forwards any comments it has made on a bill to any relevant Senate legislation committee for information.

Chapter 1

Comment bills

1.1 The committee comments on the following bills and, in some instances, seeks a response or further information from the relevant minister.

Coronavirus Economic Support and Recovery (No-one Left Behind) Bill 2020

Purpose	This bill seeks to create the *Coronavirus Economic Support and Recovery (No-One Left Behind) Act* 2020, which will provide for a coronavirus economic support and recovery fund, amend the law relating to social security and expand eligibility for the JobKeeper scheme
Sponsor	Senator Larissa Waters
Introduced	Senate on 11 June 2020

Parliamentary scrutiny

Significant matters in delegated legislation[1]

1.2 Schedule 1 to the bill seeks to establish a $22.3 billion Coronavirus Economic Support and Recovery Fund. Subitem 1(3) provides that, in 2020-21, the Fund must provide for a $2.3 billion recovery package for the arts and entertainment sector, a $12 billion manufacturing investment fund, a $6 billion electricity transmission fund, and additional funding of $2 billion for the Australian Renewable Energy Agency. Subitem 1(4) provides for certain limitations on both the manufacturing and electricity transmission investments of the Fund.

1.3 Beyond these provisions, little detail about how the Fund will operate is provided on the face of the bill, with the establishment, governance and operation of the Fund to be set out in delegated legislation.

1.4 The committee's view is that significant matters, such as how a fund to which the Commonwealth will invest a significant amount of public money is to operate, should be included on the face of primary legislation unless a sound justification provided. In this instance, the explanatory memorandum contains no explanation as to why further details as to how the Fund is to operate was not included in the bill or

1 Schedule 1. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(iv) and (v).

any indication of what specific matters are likely to be included in the delegated legislation made under the bill.

1.5 The committee draws this matter to the attention of senators and leaves to the Senate as a whole the appropriateness of allowing the establishment, governance and operation of the proposed Coronavirus Economic Support and Recovery Fund to be set out in delegated legislation.

Delegation of legislative power

Broad discretionary powers[2]

1.6 Part 1 of Schedule 2 to the bill seeks to provide that if a person is receiving a disability support pension or carer payment, the rate of the pension or payment is increased by the amount of the COVID-19 supplement. Proposed subsections 121(3) and 211(3) provide that the minister may, by legislative instrument, extend the initial period of the supplement by a period of up to 3 months. Proposed subsections 121(5) and 211(5) provide that the minister may, by legislative instrument, determine the amount of the supplement. Proposed subsections 121(7) and 211(7) provide that the minister may, by legislative instrument, determine the amount of the supplement for any extension period.

1.7 The committee commented on similar provisions in the Coronavirus Economic Response Package Omnibus Bill 2020.[3] The committee considers that these provisions provide the minister with a broad discretionary power to alter or extend the operation of supplement payments by legislative instrument in circumstances where there is limited guidance on the face of the primary legislation as to when these powers should be exercised.

1.8 Noting the above, the committee considers that if the Parliament is sitting changes to the COVID-19 supplement scheme should be made by introducing a bill for consideration by the Parliament, rather than relying on the use of the broad discretionary power to modify the scheme by delegated legislation.

2 Schedule 2, Part 1. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(ii) and (iv).

3 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5 of 2020*, pp. 14–15; Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 6 of 2020*, pp. 24–25.

Green New Deal (Quit Coal and Renew Australia) Bill 2020

Purpose	This bill seeks to amend establish Renew Australia, a public authority to lead the national transition to new clean energy systems. It also seeks to prohibit the mining, burning, export and importation of thermal coal in Australia
Sponsor	Mr Adam Bandt MP
Introduced	House of Representatives on 10 June 2020

Strict liability[4]

1.9 Subclause 64(10) provides that it will be an offence, subject to a penalty of 100 penalty units, for a person who has permission to export thermal coal to contravene the requirements or conditions of the permission. Proposed subclause 64(11) provides that the offence is one of strict liability.

1.10 Under general principles of the criminal law, fault is required to be proved before a person can be found guilty of a criminal offence (ensuring that criminal liability is imposed only on persons who are sufficiently aware of what they are doing and the consequences it may have). When a bill states that an offence is one of strict liability, this removes the requirement for the prosecution to prove the defendant's fault. In such cases, an offence will be made out if it can be proven that the defendant engaged in certain conduct, without the prosecution having to prove that the defendant intended this, or was reckless or negligent. As the imposition of strict liability undermines fundamental criminal law principles, the committee expects the explanatory memorandum to provide a clear justification for any imposition of strict liability, including outlining whether the approach is consistent with the *Guide to Framing Commonwealth Offences.*[5] No justification is provided in the explanatory memorandum.

1.11 The *Guide to Framing Commonwealth Offences* states that the application of strict liability is only considered appropriate where the offence is not punishable by imprisonment and only punishable by a fine of up to 60 penalty units for an

4 Clause 64. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(i).

5 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, pp 22–25.

individual.[6] In this instance, the bill proposes applying strict liability to an offence with a maximum penalty of 100 penalty units.

1.12 The committee draws this matter to the attention of senators and leaves to the Senate as a whole the appropriateness of including a strict liability offence with a penalty above what is recommended in the *Guide to Framing Commonwealth Offences.*

6 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, p. 23.

Interactive Gambling Amendment (Banning Social Casinos and Other Measures) Bill 2020

Purpose	This bill seeks to create a criminal offence and civil liability for any person who provides social casino services to Australian customers
Sponsor	Mr Andrew Wilkie MP
Introduced	House of Representatives on 10 June 2020

Significant matters in delegated legislation[7]

1.13 The bill seeks to insert proposed section 64E into the *Interactive Gambling Act 2001*, which would allow the ACMA to seek an injunction from the Federal Court to require a carriage service provider to take steps to disable access to online locations that provide certain social casino services.

1.14 Proposed subsection 64E(11) provides that the minister may, by legislative instrument, exempt a particular online search engine provider or an online search engine provider that is in a particular class from applications for an injunction.

1.15 From a scrutiny perspective, the committee is concerned that proposed subsection 64E(11) appears to confer on the minister a broad power to exempt online search engine providers from the operation of the legislation in circumstances where there is no guidance on the face of the primary legislation regarding the conditions for the exercise of the power. Additionally, the committee's longstanding view is that significant matters should be included in the primary legislation unless a sound justification for the use of delegated legislation is provided. The explanatory memorandum does not include any information as to why it is necessary that certain online search engine providers be exempted or why this has been left to delegated legislation.

1.16 It is unclear to the committee why at least high-level guidance about when the power to exempt online search engine providers is to be used could not be included on the face of the primary legislation. In this regard, the committee notes that a legislative instrument, made by the executive, is not subject to the full range of parliamentary scrutiny inherent in bringing the proposed changes in the form of an amending bill.

1.17 The committee draws this matter to the attention of Senators and leaves to the Senate as a whole the appropriateness of providing the minister with a broad

7 Schedule 1, item 7. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(ii) and (iv).

power to declare, by delegated legislation, that online search engine providers must not be specified in applications for an injunction.

National Disability Insurance Scheme Amendment (Strengthening Banning Orders) Bill 2020

Purpose	This bill seeks to broaden the circumstances in which the NDIS Quality and Safeguards Commissioner may make a banning order against a provider or person, and clarifies the Commissioner's powers
Portfolio	National Disability Insurance Scheme
Introduced	House of Representatives on 12 June 2020

Broad discretionary powers[8]

1.18 Item 3 of Schedule 1 to the bill seeks to amend the *National Disability Insurance Scheme Act 2013* to insert proposed subsection 73ZN(2A) to provide that the NDIS Quality and Safety Commissioner (the Commissioner) may make an order prohibiting or restricting a person from being involved in the provision of specified supports or specified services to people with disability if the Commissioner reasonably believes that the person is not suitable to be so involved. The banning order applies to persons who have not previously been an NDIS provider or employed or otherwise engaged by an NDIS provider.

1.19 The committee notes that this provision provides the Commissioner with a broad discretionary power to ban persons from providing disability services in circumstances where there is limited guidance on the face of the bill as to how or when the power should be exercised. The committee notes that there is no definition of when a person will not be suitable nor are there any criteria regarding suitability on the face of the bill.

1.20 The committee expects that the inclusion of broad discretionary powers should be justified in the explanatory memorandum. In this instance, the explanatory memorandum contains no justification for the inclusion of this broad discretionary power.

1.21 The committee therefore requests the minister's advice as to:

- **why it is necessary and appropriate to provide the Commissioner with a broad power to ban persons from providing disability services; and**
- **whether the bill can be amended to include additional guidance on the exercise of the power on the face of the primary legislation.**

8 Schedule 1, item 3, proposed subsection 73ZN(2A). The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(ii).

Significant matters in delegated legislation

Privacy[9]

1.22 Proposed subsection 73ZS(5A) provides that the NDIS Provider Register (the Register) may include the name of a person, their ABN and any details of the banning order in relation to a person against whom a banning order is made under subsection 73ZN(2) or (2A). The rules (delegated legislation) may prescribe any other matter that may be included on the Register.

1.23 The committee's view is that significant matters, such as the matters that can be included on a public register, should be in the primary legislation unless a sound justification for the use of delegated legislation is provided. In this instance, the explanatory memorandum states:

> It is not anticipated at this stage that the matters which may be included in the Register prescribed by the Rules will extend to any highly sensitive or highly personal information about the person subject to the banning order. However, in some instances, such as where an individual or business has a common name, it may be necessary to include further information, to publish an amount of information that is sufficient to ensure people with disability and their carers can identify the person. This would not extend, for example, to the nature of the incident that prompted the making of the banning order. It may include, for example, a broad description of the town or area in which the banned person was providing services.[10]

1.24 While noting the explanation in the explanatory memorandum, the committee notes that there is nothing on the face of the bill which would prevent the inclusion of highly sensitive or highly personal information about persons on the Register. As a result, the committee notes that the potential disclosure of information regarding persons subject to banning orders will not be subject to the full range of parliamentary scrutiny inherent in bringing proposed changes in the form of an amending bill.

1.25 The committee therefore requests the minister's advice as to:

- **why it is necessary and appropriate to leave significant matters, such as what personal information can be included on the Register, to delegated legislation, noting the potential impact on a person's privacy; and**

9 Schedule 1, item 5, proposed subsection 73ZS(5A). The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(i) and (iv).

10 Explanatory memorandum, p. 2.

- **whether the bill can be amended to set out the information that can be included on the Register on the face of the primary legislation.**

Privacy Amendment (Public Health Contact Information) Bill 2020

Purpose	This bill seeks to amend the *Privacy Act 1988* to assist in preventing and controlling the entry, emergence, establishment or spread of the coronavirus known as COVID-19 into Australia or any part of Australia by providing specific privacy protections for users of the Commonwealth's COVIDSafe app and data collected through the app. The bill also seeks to elevate the provisions of the related determination into primary legislation and to introduce additional measures to strengthen privacy protections
Portfolio	Attorney-General
Introduced	House of Representatives on 12 May 2020

Significant penalties[11]

1.26 Item 2 of Schedule 1 to the bill seeks to insert new Part VIIIA into the *Privacy Act 1988* (Privacy Act). Division 2 of Part VIIIA (proposed sections 94D to 94H) establishes a series of offences relating to the COVIDSafe app and COVID app data. In this regard, Division 2 provides that the following forms of conduct would be punishable by 5 years' imprisonment, 300 penalty units ($63 000), or both:

- collecting, using or disclosing COVID app data, where the collection, use or disclosure is not permitted;[12]
- uploading COVID app data, or causing COVID app data to be uploaded, to the National COVIDSafe Data Store, without the consent of the COVIDSafe user or their parent, guardian or carer;[13]
- retaining COVID app data that has been uploaded to the National COVIDSafe Data Store on a database outside Australia;[14]
- disclosing COVID app data that has been uploaded to the National COVIDSafe Data Store to a person outside Australia;[15]

11 Schedule 1, item 2, proposed sections 94D, 94E, 94F, 94G and 94H. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

12 Proposed subsection 94D(1).

13 Proposed section 94E.

14 Proposed subsection 94F(1).

- decrypting COVID app data that is stored on a communications device;[16]
- requiring a person to download or use the COVIDSafe app, or requiring a person to consent to uploading COVID app data from a communications device to the National COVIDSafe Data Store;[17]
- taking specified forms action against a person, on the grounds that the person has not downloaded the COVIDSafe app, does not have the COVIDSafe app in operation, or has not consented to uploading COVID app data from a communications device to the National COVIDSafe Data Store.[18]

1.27 In relation to the offence in proposed subsection 94D(1), the explanatory memorandum states that:

> 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.[19]

1.28 The explanatory memorandum does not appear to contain an explanation as to the significance of the penalties in proposed sections 94E to 94H. However, the explanation provided in relation to subsection 94D(1) is relevant to those sections.

1.29 The committee acknowledges the importance of providing robust safeguards against the misuse of COVID app data and providing reassurance to the Australian community, and notes that other Commonwealth legislation imposes comparable penalties for offences relating to the use and disclosure of sensitive data.[20] However, given the significance of the penalties that may be imposed under proposed sections

---

15 Proposed subsection 94F(2). A person may disclose the COVID app data if they are employed by, or in the service of, a State or Territory health authority, and the disclosure is only for the purpose of undertaking contact tracing.

16 Proposed section 94G.

17 Proposed subsection 94H(1).

18 Proposed subsection 94H(2). Relevant actions include: refusing to enter into or continue a contract or arrangement with the person; taking adverse action against the person (within the meaning of the *Fair Work Act 2009*); refusing to allow the person to enter certain premises; refusing to allow the person to participate in an activity; refusing to receive goods or services from a person, or insisting the person offer goods or services at a discount; and refusing to provide goods or services from the person, or insisting that the person pay a premium.

19 Explanatory memorandum, p. 13.

20 For example, subsection 59(3) of the *My Health Records Act 2012* makes it an offence for a person to collect, use or disclose information contained in a healthcare recipient's My Health Record, where the person is unauthorised to do so.

94D to 94H, the committee would expect a comprehensive justification for the penalty in each of those provisions to be included in the explanatory memorandum.

1.30 In addition, the relevant penalties should be justified by reference to similar offences under Commonwealth law. This not only promotes consistency, but guards against the risk that the liberty of a person is unduly limited through the application of disproportionate penalties. In this respect, the committee notes that the *Guide to Framing Commonwealth Offences* states that a penalty 'should be consistent with penalties for existing offences of a similar kind or…seriousness. This should include a consideration of…other comparable offences in Commonwealth legislation'.[21]

1.31 As the explanatory memorandum does not appear to provide a sufficiently detailed justification as to why it is considered necessary and appropriate to impose significant penalties for the offences in proposed sections 94D to 94H, the committee requests the minister's detailed advice as to the justification for the significant penalties that may be imposed under those provisions, by reference to comparable Commonwealth offences and the requirements in the *Guide to Framing Commonwealth Offences*.

Reversal of evidential burden of proof[22]

1.32 Proposed subsection 94D(1) provides that it is an offence for a person to collect, use or disclose COVID app data, where collection, use or disclosure is not permitted under section 94D. Proposed subsection 94D(3) creates an exemption (offence-specific defence) to this offence, which provides that the offence does not apply to the collection of COVID app data, if:

- the collection of the COVID app data occurs as part of, or is incidental to, the collection, at the same time, of data that is not COVID app data (non-COVID app data); and
- the collection of the non-COVID app data is permitted under Australian law; and
- the COVID app data is deleted as soon as practicable after the person becomes aware that it has been collected, and is not otherwise accessed, used or disclosed by the person after it is collected.

1.33 Subsection 13.3(3) of the *Criminal Code Act 1995* provides that a defendant who wishes to rely on any exception, exemption, excuse, qualification or justification bears an evidential burden in relation to that matter.

---

21 Attorney-General's Department, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, p. 39.

22 Schedule 1, item 2, subsection 94D(3). The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(i).

1.34 At common law, it is ordinarily the duty of the prosecution to prove all elements of an offence. This is an important aspect of the right to be presumed innocent until proven guilty. Provisions that reverse the burden of proof and require a defendant to disprove, or raise evidence to disprove, one or more elements of an offence, interferes with this common law right.

1.35 In this instance, the defendant bears an evidential burden (requiring the defendant to raise evidence about the matter), rather than a legal burden (requiring the defendant to positively prove the matter). Nevertheless, the committee expects the reversal of the evidential burden of proof to be justified.

1.36 In relation to proposed subsection 94D(3), the explanatory memorandum states that:

> 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 data collection, and that in these circumstances, the collecting person can derive no benefit from that collection.[23]

1.37 The committee notes that the *Guide to Framing Commonwealth Offences* provides that a matter should only be included in an offence-specific defence where:

- it is peculiarly within the knowledge of the defendant; and
- it would be significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter.[24]

1.38 In this instance, it appears that the majority of the matters set out in subsection 94D(3) would meet the criteria set out in the *Guide*. However, it is not clear that all the matters in that subsection would meet those criteria. For example, it appears that whether the collection of data is permitted under Australian law is a factual matter, rather than a matter that would be peculiarly within the defendant's knowledge.

1.39 The committee draws its scrutiny concerns in relation to proposed subsection 94D(3), which reverses the evidential burden of proof, to the attention of senators.

---

23 Explanatory memorandum, p. 17.

24 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers,* September 2011, p. 50.

Privacy[25]

1.40 The bill sets out a series of measures relating to the COVIDSafe app[26] and to COVID app data. According to the explanatory memorandum, these measures provide stronger privacy protections for users of the app, and data collected through the app, than the protections that would otherwise apply under Australian law.[27] The relevant measures include new, targeted offences,[28] specific obligations relating to COVID app data and COVIDSafe,[29] and provisions which specify how general privacy protections elsewhere in the Privacy Act apply to COVIDSafe and COVID app data.[30]

1.41 In the view of the committee, these are important protections for individuals using the COVIDSafe app. However, the committee notes that certain terms in the bill—which are essential to the operation of the new measures—are broadly defined. From a scrutiny perspective, the committee is concerned that this may undermine the value of the measures as privacy safeguards.

Definition of 'COVID app data'

1.42 In particular, the committee is concerned that the scope of the information collected through the operation of the COVIDSafe app is unclear. In this regard, the bill defines 'COVID app data' as data relating to a person that:

- has been collected or generated (including before the commencement of Part VIIIA) through the operation of COVIDSafe; and
- is either registration data, or data that is, or has been, stored on a mobile communications device (including before Part VIIIA commenced).[31]

1.43 However, the bill does not specify the type of data that is collected or generated through the operation of the COVIDSafe app, nor does it define 'registration data'. The explanatory memorandum states that COVID app data includes data calculated or otherwise derived from within the COVIDSafe app on a

25 Schedule 1, item 2 proposed subsections 94D(5) and (6), definition of 'COVID app data' and 'contact tracing'. The committee draws senators' attention to these provision pursuant to Senate Standing Order 24(1)(a)(i).

26 'COVIDSafe is defined in subsection 6(1) of the Privacy Act, as amended by item 1 of the bill, as an app that is made available or has been made available (including before the commencement of Part VIIIA), by or on behalf of the Commonwealth, for the purpose of facilitating contact tracing.

27 Explanatory memorandum, p. 2.

28 Division 2, Part VIIIA.

29 Division 3, Part VIIIA.

30 Division 4, Part VIIIA.

31 Paragraphs 94E(5)(a) and (b).

mobile communications device, and notes that the COVIDSafe app does not collect geolocation data.[32] However, there is nothing to this effect on the face of the bill.

1.44 In addition, the committee notes that where a user of the COVIDSafe app tests positive for COVID-19, and uploads decrypted records of their contacts over the previous 21 days, these decrypted records do not clearly fall within the definition of 'COVID app data'. This is because the decrypted records are not collected or generated from the operation of the app or stored on the user's device. It is also not clear that data transformed or derived from COVID app data by state or territory health officials falls within the definition of 'COVID app data'.

1.45 As the scope of 'COVID app data' is unclear, it is not apparent how such data would be deidentified, and whether the de-identification process would sufficiently protect individuals' privacy. For example, it is unclear whether data which has been de-identified could be reverse engineered, such that it could be used to identity users of the COVIDSafe app.

Definition of 'contact tracing' and 'in contact'

1.46 The bill defines 'contact tracing' as the process of identifying persons who have been 'in contact' with a person who has tested positive for the coronavirus known as COVID-19.[33] It also provides that a person has been 'in contact' with another person where the operation of COVIDSafe in relation to the person indicates that they may have been in the proximity of the other person.[34] The explanatory memorandum states that a person will only be considered to be 'in contact' with another person where they are both COVIDSafe users with the COVIDSafe app operating, and the COVIDSafe app detects the presence of another person 'within detectable proximity'.[35] However, it is unclear how close one telecommunications device with the COVIDSafe app must be to another before it is registered as being 'in contact'. Also unclear is the duration for which two communications devices with the COVIDSafe app must be in proximity to each other before one user's app registers the other as being 'in contact'.

1.47 The Privacy Impact Assessment indicates that where the COVIDSafe app detects another device with the app installed within its Bluetooth signal range, it will create a record ('digital handshake') of this contact every minute.[36] The Privacy

32 Explanatory memorandum, p. 18.

33 Subsection 94E(6). Subsection 6(1) of the Privacy Act, as amended by item 1 of the present Act, provides that a person has been 'in contact' with another person if the operation of COVIDSafe in relation to the person indicates that the person may have been in the proximity of the other person.

34 Subsection 6(1) of the Privacy Act, as amended by item 1 of the present Act.

35 Explanatory memorandum, p. 10.

36 Maddocks, *The COVIDSafe Application, Privacy Impact Assessment*, 24 April 2020, pp. 19-20.

Impact Assessment also states that, where a user consents, all digital handshakes will be uploaded to the National COVIDSafe Data Store.[37] This suggests that the scope of the data which may be collected and shared through the COVIDSafe app is broad, and may contradict the position that the app only collects data about other users who come within 1.5 metres, for at least 15 minutes.

Committee comment

1.48 These matters are significant for privacy purposes, because they provide an indication of the scope of the data that an individual may collect when they carry their mobile device, the scope data that may be shared, and the scope of the data that may be uploaded to the National COVIDSafe Data Store.

1.49 To clarify the nature and type of information that is collected under the bill, the committee requests the minister's detailed advice as to:

- **the scope of the information that is collected or generated through the COVIDSafe app, including whether 'COVID app data' includes:**
  - **decrypted records of a user's contacts over the previous 21 days, in circumstances where the user has tested positive for COVID-19; or**
  - **data transformed or derived from COVID app data by state or territory health officials; and**
- **when the COVIDSafe app will make a record of a 'digital handshake' between users of the app, and upload that record to the National COVIDSafe Data Store, including:**
  - **how close users must be to each other in order for the app to record a 'digital handshake'; and**
  - **how long users must be in proximity to each other for the app to record a 'digital handshake'.**

1.50 The committee also requests the minister's advice as to how COVID app data will be de-identified, and how the de-identification process will protect the privacy of individuals.

Privacy[38]

1.51 As noted above, proposed subsection 94H(1) provides that it is an offence to require a person to download the COVIDSafe app to a communications device, to have the app in operation on a communications device, or to upload data to the

37 Maddocks, *The COVIDSafe Application, Privacy Impact Assessment*, 24 April 2020, pp. 19-20.

38 Schedule 1, item 2, section 94H. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(i).

National COVIDSafe Data Store. Proposed subsection 94H(2) provides that it is an offence for a person to take proscribed actions against a person, on the grounds that the person has not downloaded, or is not using, the COVIDSafe app, or has not consented to uploading data to the National COVIDSafe Data Store.[39]

1.52 The explanatory memorandum states that:

> The purposes of these offences taken together is to ensure that no person can require, coerce, or otherwise oblige (whether directly or indirectly) another person to install or have COVIDSafe operating on their communications device, or to upload…data from a communications device to the National COVIDSafe data store.[40]

1.53 In addition, the statement of compatibly indicates that the offences in proposed section 94H are intended to safeguard individuals' privacy, by ensuring individuals are given a free and informed choice as to whether to download and use COVIDSafe. It also states that the offences provide strong incentives against requiring individuals to download and use the app.

1.54 The offences in proposed section 94H appear to provide strong deterrents against requiring individuals to download and use COVIDSafe, or to upload data to the National COVIDSafe data store. However, it is unclear whether these offences as currently drafted would capture attempts to incentivise individuals to undertake these activities. Additionally, it is unclear whether the offences as currently drafted would capture persons who indirectly incentivise the downloading of the app by placing additional requirements or conditions on individuals who have not downloaded it (for example, where a restaurant has a general requirement that patrons must provide their contact details, but this requirement is waived for those patrons who have downloaded the app). The explanatory memorandum is silent on these matters.

1.55 The committee is concerned that the failure to include the provision of financial incentives as conduct that is prohibited under proposed section 94H may undermine the value of that provision as a privacy safeguard.

1.56 The committee requests the minister's advice as to whether the offences in section 94H of the Act would apply to making discounts, payments and other incentives (including placing additional requirements or conditions on individuals who have not downloaded the app) contingent on a person downloading or using the COVIDSafe app, or uploading COVID app data to the National COVIDSafe Data Store.

---

39 The proscribed actions include taking adverse action against the person (within the meaning of the *Fair Work Act 2009*); refusing to allow the person to enter premises; and refusing to provide good or services to the person.

40 Explanatory memorandum, p. 21.

No requirement to table or publish reports[41]

1.57 Proposed section 94ZA requires the Health Minister to cause reports to be prepared on the operation and effectiveness of COVIDSafe and the National COVIDSafe Data Store during the six-month period starting on the commencement of Part VIIIA of the Act, and during each subsequent six-month period.

1.58 Proposed section 94ZB similarly requires the Information Commissioner to cause reports to be prepared on the performance of the Commissioner's function, and the exercise of the Commissioner's powers, during the six-month period starting on the commencement of Part VIIIA, and during each subsequent six-month period.

1.59 The explanatory memorandum indicates that the reports prepared under proposed sections 94ZA and 9ZB are intended to inform and reassure the public about the operation of Part VIIIA (that is, the Part relating to the COVIDSafe app and COVID app data). In this respect, it states that:

> [Reports prepared under section 94ZB are] 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…performance of functions and exercise of powers.[42]

1.60 However, the bill does not appear to require the report prepared by the Health Minister under section 94ZA to be published online, and does not appear to require the report prepared by the Commissioner to be tabled in Parliament.

1.61 Tabling documents in Parliament is important to parliamentary scrutiny, as it alerts parliamentarians to the existence of documents and provides opportunities for debate that are not available where documents are not made public or are only published online. Making documents related to the performance of Commonwealth entities and programs available online promotes transparency and accountability. Consequently, where a bill does not require the tabling or publication of documents associated with review processes, the committee would expect an appropriate justification to be included in the explanatory memorandum.

1.62 In this instance, the explanatory memorandum does not provide an explanation as to why reports prepared by the Health Minister are not required to be published online, or why reports prepared by the Commissioner are not required to be tabled in Parliament.

---

41 Schedule 1, item 2, sections 94ZA and 94ZB. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(v).

42 Explanatory statement, p. 36.

1.63 Noting that there may be impacts on parliamentary scrutiny where reports associated with the operation of regulatory schemes are not available to the Parliament or published online, the committee requests the minister's advice as to:

- **why the bill does not require reports prepared by the Health Minister under proposed section 94ZA to be published online; and**
- **why the bill does not require reports prepared by the Information Commissioner under proposed section 94ZB to be tabled in Parliament.**

Treasury Laws Amendment (2020 Measures No. 3) Bill 2020

Purpose	This bill seeks to: • authorise the Minister to enter into loan agreements with the International Monetary Fund and other countries; • allow certain entities to be deductible gift recipients under income tax law; • extend the instant asset write-off and reduce the GDP adjustment factor for the 2021-21 income year to nil; and • clarify payments made under the Coronavirus Economic Response Package
Portfolio	Treasury
Introduced	House of Representatives on 12 June 2020

Parliamentary scrutiny[43]

Authorising loan agreements with the IMF

1.64 Items 2 and 4 of Schedule 1 to the bill seek to amend the *International Monetary Agreements Act 1947* (IMA Act) to:

- authorise the minister, on behalf of Australia, to enter into loan agreements with the International Monetary Fund (IMF); and
- allow Australia to meet its future funding obligations under these loan agreements without the need for either primary legislation or delegated legislation by:
  - inserting a new standing appropriation in proposed section 8CAB to fund Australia's obligations to pay amounts to the IMF under a loan agreement; and
  - inserting a new paragraph 6(1)(d) which would authorise the Treasurer to borrow amounts that Australia is required to pay because of its obligations under a loan agreement.

1.65 In relation to entering into the loan agreements, the explanatory memorandum states that:

43 Schedule 1. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(v).

> These changes ensure that Australia can enter into other loan agreements with the IMF without legislation being required to implement the decision after it has been entered in to. It is expected that the new legislative framework will be used to authorise the next round of bilateral borrowing agreements with the IMF...
>
> This approach is consistent with other provisions in the IMA Act relating to agreements that the Minister is authorised to enter in to.[44]

1.66 In relation to meeting the funding obligations under the loan agreements, the explanatory memorandum states that:

> The Consolidated Revenue Fund is appropriated for the purposes of payments by Australia under an agreement authorised by these amendments...
>
> This approach is consistent with all other appropriations covered by the IMA Act…Appropriations of this kind ensure that Australia is able to comply with any international obligations that it has to make payments under an agreement.[45]

1.67 The explanatory memorandum also notes that where a loan agreement also constitutes a treaty action, the decisions to enter into those agreements are subject to Australia's domestic treaty making procedures, including consideration by the Joint Standing Committee on Treaties (JSCOT).

New Arrangements to Borrow

1.68 The New Arrangements to Borrow is a multilateral borrowing agreement between the IMF and a number of its members that allows the IMF to borrow from those members, when supplementary resources are required to address an impairment of the international monetary system. Australia is a founding member of the New Arrangements to Borrow and has participated since it formally commenced in 1998.[46]

1.69 Items 1 and 3 of Schedule 1 to the bill seek to amend the IMA Act to remove the requirement for primary legislation to give force of law to amendments to the New Arrangements to Borrow, including amendments that increase or decrease the quantum of Australia's commitment to the IMF and trigger the existing standing appropriation under section 8B.

1.70 Unlike the new provisions in relation to entering into loan agreements with the IMF referred to above, the amendments in relation to New Arrangements to Borrow retain some level of parliamentary oversight through delegated legislation.

---

44 Explanatory memorandum, p. 10.

45 Explanatory memorandum, p. 10.

46 Explanatory memorandum, p. 7.

Proposed subsection 8B(3) would allow the Treasurer to give notice, by legislative instrument, of an amendment or renewal of the New Arrangements to Borrow.

1.71 The explanatory memorandum states that:

> This allows the terms of the New Arrangements to Borrow to be updated to reflect future changes without the need for legislative amendments to be passed by the Parliament. This approach is consistent with other provisions in the IMA Act...[47]

1.72 A legislative instrument giving notice of an amendment or renewal of the New Arrangements to Borrow would commence after the disallowance period for the instrument has passed. The explanatory memorandum notes that 'this deferred commencement ensures that the Parliament can consider and deal with any amendment to the New Arrangements to Borrow before they take effect in the IMA Act.'[48] In addition, any amendments to the New Arrangements to Borrow which also constitute a treaty action, would be subject to Australia's domestic treaty making procedures, including consideration by JSCOT.

Committee comment

1.73 If passed, the bill would:

- allow Australia to meet its future funding obligations under loan agreements entered into with the IMF, without the need for either primary legislation or delegated legislation, by inserting a new standing appropriation into the IMA Act and authorising the Treasurer to borrow relevant amounts;[49] and
- remove the requirement for primary legislation to give force of law to amendments to the New Arrangements to Borrow, including amendments that increase or decrease the quantum of Australia's commitment to the IMF.[50]

1.74 These proposed amendments would limit the opportunity for Parliament to review and scrutinise Australia's future commitments to the IMF. While the committee notes the explanation that such an approach has been adopted in other similar contexts, from a scrutiny perspective, the committee does not generally consider consistency with existing provisions to be sufficient justification for limiting parliamentary oversight. In addition, while the committee notes that treaty actions may be subject to scrutiny through JSCOT, and the Treasurer is required to give notice, by legislative instrument, of an amendment or renewal of the New

47 Explanatory memorandum, p. 11.

48 Explanatory memorandum, p. 11.

49 Schedule 1, items 2 and 4.

50 See proposed sections 5 and 5A of the IFC Act.

Arrangements to Borrow, the committee does not consider that such scrutiny is a substitute for the level of scrutiny inherent in the passage of a bill through both Houses of the Parliament.

1.75 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of limiting the opportunity for Parliament to review and scrutinise Australia's future commitments to the International Monetary Fund.

Bills with no committee comment

1.76 The committee has no comment in relation to the following bills which were introduced into the Parliament between 10 – 12 June 2020:

- Aged Care Legislation Amendment (Financial Transparency) Bill 2020
- Broadcasting Services Amendment (Regional Commercial Radio and Other Measures) Bill 2020
- Commonwealth Electoral Amendment (Ensuring Fair Representation of the Northern Territory) Bill 2020
- Education Legislation Amendment (2020 Measures No. 1) Bill 2020
- Electoral Legislation Amendment (Miscellaneous Measures) Bill 2020
- Health Insurance Amendment (Continuing the Office of the National Rural Health Commissioner) Bill 2020

Commentary on amendments and explanatory materials

Tertiary Education Quality and Standards Agency Amendment (Prohibiting Academic Cheating Services) Bill 2020

1.77 On 12 June 2020 the Assistant Minister to the Deputy Prime Minister (Mr Hogan) presented an addendum to the explanatory memorandum, and the bill was read a third time.

1.78 The committee thanks the assistant minister for tabling this addendum to the explanatory memorandum which includes key information previously requested by the committee.

1.79 The committee has no comment on amendments made or explanatory material relating to the following bills:

- Australian Sports Anti-Doping Authority Amendment (Enhancing Australia's Anti-Doping Capability) Bill 2019;[51]
- National Radioactive Waste Management Amendment (Site Specification, Community Fund and Other Measures) Bill 2020;[52]
- Paid Parental Leave Amendment (Flexibility Measures) Bill 2020;[53] and
- Treasury Laws Amendment (2019 Measures No. 3) Bill 2019.[54]

51 On 11 June 2020 the Senate agreed to one Opposition amendment, and the bill was read a third time. On 12 June 2020 the House of Representatives agreed to the Senate amendment.

52 On 11 June 2020 the House of Representatives agreed to 3 Government amendments, and the bill was read a third time.

53 On 11 June 2020 the Senate agreed to 7 Government amendments, the bill was read a third time, and the House of Representatives agreed to the Senate amendments.

54 On 12 June 2020 the Senate agreed to 2 Centre Alliance amendments, and the bill was read a third time.

Chapter 2

Commentary on ministerial responses

2.1 This chapter considers the responses of ministers to matters previously raised by the committee.

Telecommunications Legislation Amendment (International Production Orders) Bill 2020

Purpose	This bill seeks to provide the legislative framework for Australia to give effect to future bilateral and multilateral agreements for cross-border access to electronic information and communications data
Portfolio	Home Affairs
Introduced	House of Representatives on 5 March 2020
Bill status	Before the House of Representatives

Trespass on personal rights and liberties—international production orders[1]

2.2 In *Scrutiny Digest 5 of 2020* the committee requested the minister's advice as to:

- why it is necessary and appropriate to allow international production orders (IPOs) to be issued by members of the Administrative Appeals Tribunal (AAT);
- whether the bill could be amended to include a national Public Interest Monitor scheme so that Public Interest Monitors may make submissions in relation to all IPO applications;
- whether the bill could be amended to require that, for all IPOs, the relevant decision maker must be satisfied that an IPO would be 'likely to *substantially* assist' with the relevant purpose for which the IPO is sought, rather than merely 'likely to assist';
- whether the 3 month period in subclause 81(1) of proposed Schedule 1 to the TIA Act could be reduced, to provide the Ombudsman with more immediate oversight of the issuing of control order IPOs;

1 Proposed Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(i).

- whether clause 144 of proposed Schedule 1 to the TIA Act could be amended to provide that the Ombudsman may obtain relevant information from officers and members of staff if the Ombudsman has 'reasonable grounds to *suspect*' that the officer or member of staff is able to give the relevant information, rather than 'reasonable grounds to *believe*'.[2]

Minister's response[3]

2.3 The minister advised:

Issuing of IPOs by members of the AAT

The Bill provides for a range of independent decision-makers to authorise international production orders for disclosure of intercepted communications, stored communications and telecommunications data. To assist the Committee, a table setting out which decision-makers are able to authorise different types of orders under the Bill and the TIA Act currently is set out at **Annexure A**.

Administrative Appeals Tribunal (AAT) members, judges, magistrates, and the Attorney-General, all play a critical role as independent decision-makers in authorising investigatory powers domestically in the current regimes under the *Telecommunications (Interception and Access) Act 1979* (TIA Act). In accordance with this current domestic approach, the Bill recognises the value of having an independent decision-maker with the skillset of being a qualified legal practitioner given the complexity of the decision-making involved in authorising investigatory powers internationally and the inherent balancing of law enforcement or national security powers with affected individuals' privacy and other rights and liberties required.

The ability for nominated AAT members to authorise the use of investigatory powers is not new. For example, nominated AA T members have played an independent decision-maker role in investigatory powers legislation, including in relation to interception and stored communication warrants under the TIA Act since 1998. Nominated AAT members also issue surveillance device warrants and computer access warrants under the *Surveillance Devices Act 2004*. The skill and experience of AAT members make them ideal candidates to assess applications for international production orders and make independent decisions on their compliance with the legislative requirements. In addition, the framework and principles under which AAT members operate safeguard the functional independence of their decisions.

---

2 Senate Scrutiny of Bills Committee, *Scrutiny Digest 5 of 2020*, pp. 24-28.

3 The minister responded to the committee's comments in a letter dated 18 May 2020. A copy of the letter is available on the committee's website: see correspondence relating to *Scrutiny Digest 7 of 2020* available at: www.aph.gov.au/senate_scrutiny_digest

The skill, competence, and independence of AAT members makes them suitable to assess applications for international production orders and to make independent decisions in accordance with the legal requirements under the Bill. AAT members undertake this independent decision-maker role in their personal capacity. AAT members must consent to being made an independent decision-maker under specific regimes of the TIA Act (including the Bill) and the Attorney-General must nominate them. Providing a wide range of independent decision-makers (e.g. AAT members, judges and magistrates) ensures there is a sufficient pool of available decision-makers to authorise orders sought by agencies. This is particularly important given all law enforcement agencies across Australia utilise the TIA Act to obtain these kinds of investigatory powers.

In terms of international production orders that relate to national security, this will be limited to nominated AAT Security Division members only after the consent of the Attorney-General has been received. This ensures there is a rigorous process of independent scrutiny with ASIO being required to satisfy both the Attorney-General (as the First Law Officer with a longstanding role in approving ASIO's intelligence collection powers) and a nominated member of the AAT, that the legislative thresholds have been met before an international production order can be issued. The Inspector-General of Intelligence and Security will also provide oversight of ASIO's use of powers under the legislation.

For the above reasons, the Government sees the utilisation of AAT members in their personal capacity as independent decision-makers as appropriate, necessary and critical to the effective operation of the TIA Act and the Bill.

Public Interest Monitors

In accordance with the current approach to domestic law enforcement interception warrants under the TIA Act, the Bill aligns international production orders for interception to ensure that, where Public Interest Monitors are available in relation to domestic interception warrants, they will also be available for interception international production orders.

At present, Public Interest Monitors only exists within Victoria and Queensland. Public Interest Monitors perform a broad oversight role over their jurisdiction's law enforcement agencies including when applying for certain types of warrants, such as interception warrants. Consistent with current practices, the Bill intentionally gave the ability to facilitate the role of the Public Interest Monitors for international production orders relating to interception.

Other Australian States and Territories have not legislated for this office within their jurisdictions. Consequently, the Bill only provides for the Public Interest Monitors in Victoria and Queensland. These Offices were established in Victoria under the *Public Interest Monitor Act 2011* (Vic), and various pieces of legislation in Queensland, including the *Police*

Powers and Responsibilities Act 2000 (Qld) and the *Crime and Corruption Act 2001* (Qld).

Consistency of safeguards

This Government considers that *'likely to assist*' is the appropriate threshold, as set out in the Bill. The threshold of '*likely to assist*' applies for all warrants under the TIA Act other than control order warrants. In terms of the Bill, this threshold applies to both intelligence and law enforcement agencies for international production orders to authorise intercept live communications as well as for stored communications and telecommunications data. When applying for any of these international production orders, agencies are required to demonstrate that the use of the warrant would be likely to assist in connection with those purposes.

The issuing authority must be satisfied that the information to be gathered would be '*likely to assist*' in meeting the purpose of the warrant. This criterion is then balanced alongside a range of other factors decision-makers must take into account, such as having regard to privacy interference and the gravity of conduct (for law enforcement warrants).

Replacing the threshold of '*likely to assist*' with the threshold of '*likely to substantially assist*' may have the effect of preventing law enforcement and intelligence agencies from accessing overseas information likely to assist in the investigation of serious crime or matters relating to national security. During the early stages of an investigation, it would be extremely difficult for agencies to demonstrate in advance of reviewing the information that the information will be '*likely to substantially assist*' the investigation. For example, telecommunications data, such as account details and IP addresses, are often collected during the early stages of an investigation. When seeking an order, agencies need to demonstrate that this information is likely to assist the investigation, for example by determining a link between an account and the suspected criminal activity or offender and thereby identifying further lines of inquiry.

One of the policy objectives of this legislation is the recognition that the digital communications landscape has changed dramatically in the last decade, with communications technology providing a plethora of communications options on any given device – from traditional telecommunications and SMS through to social media and encrypted communications applications – each provided by a separate communications provider and each requiring a separate international production order. In many cases it would not be possible to know ahead of receiving the information if the data provided by any given communications provider will be the information that would 'substantially assist' an investigation. A higher threshold could therefore be detrimental to investigations by removing a critical line of inquiry during the early stages of an investigation.

For completeness, the Government notes that monitoring powers within the TIA Act that relate to control orders are subject to the threshold of

'substantially assist'. The imposition of a higher threshold for monitoring powers is appropriate because control orders have a protective or preventative purpose by facilitating monitoring of the person's compliance with the requirements of the control order, and the person is not necessarily suspected of involvement in further criminal activity since the control order was imposed. Accordingly, the Government has applied the exact same thresholds to international production orders relating to control orders.

Oversight by the Commonwealth Ombudsman

The inclusion of a three month period in subclause 81 (1) of the Bill reflects advice from the Commonwealth Ombudsman that given this is a new scheme whose frequency of use is not yet known, a period of three months would be more appropriate to facilitate timely oversight. This is already a marked reduction from current regimes. Both the *Crimes Act 1914* and the TIA Act establish a six month notification period.

The Commonwealth Ombudsman conducts its inspections of agencies' use of covert and intrusive powers retrospectively, with records generally assessed after the relevant warrant, authorisation or order has ceased to be in force. As such, inspections of records regarding control order international production orders are likely to occur some months after the Commonwealth Ombudsman has been notified of a control order international production order being issued. However, it is likely to significantly assist the Commonwealth Ombudsman to schedule and allocate resources for inspections, especially as it is anticipated that the use of the international production order regime will likely increase compared to current levels.

Possible amendments

Clause 144 was drafted to mirror the same oversight powers of the Commonwealth Ombudsman contained within section 87 of the TIA Act. This is also consistent with other Commonwealth legislation, such as the *Crimes Act 1914*. Accordingly, amending the '*reasonable grounds to believe*' threshold to '*reasonable grounds to suspect*' threshold, would require broader consideration across not only the TIA Act, but other Commonwealth legislation. The Government views that amending only the TIA Act (or parts of the TIA Act) would lead to considerable confusion as to what thresholds apply under different pieces of legislation despite the oversight role of the Commonwealth Ombudsman being broadly consistent across Commonwealth legislation.

Committee comment

The committee thanks the minister for this response.

Allowing IPOs to be issued by members of the AAT

2.4 The committee notes the minister's advice that AAT members have played a decision-making role in investigatory powers legislation since 1998—including in relation to the issue of interception and stored communication warrants under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and surveillance device and computer access warrants under the *Surveillance Devices Act 2004*.

2.5 The committee also notes the minister's advice that the skills and experience of AAT members make them ideal candidates to assess applications for IPOs and make independent decisions on compliance with applicable legislative requirements. In addition, the committee notes the advice that the framework and principles under which AAT members operate safeguard the functional independence of their decisions.

2.6 While acknowledging the minister's advice, the committee does not consider consistency with other laws, or the fact that AAT members have been authorised to issue interception warrants in the past, to be sufficient justification for allowing AAT members to approve IPOs under the framework proposed by the bill. The committee is also concerned that the bill would permit full-time senior members of the AAT with no experience as a legal practitioner, and part-time senior and general members with only five years' legal experience, to issue IPOs. It is not apparent that these AAT members would have the skills and expertise of an independent judicial officer. Consequently, from a scrutiny perspective, the committee remains of the view that allowing AAT members to issue IPOs may not adequately protect individuals' rights and liberties—particularly the right to privacy.

2.7 The committee reiterates its longstanding view that the power to issue warrants or orders relating to the use of intrusive powers should only be conferred on judicial officers. This is particularly important where the use of such powers may involve access to significant amounts of personal information.

2.8 Finally, the committee notes that, in determining whether to issue an interception IPO, the relevant decision-maker must have regard to whether intercepting communications would be the method that is likely to have the least interference with any person's privacy.[4] However, this requirement does not appear to apply to other IPOs. The committee considers that the requirement to consider potential interference with privacy should apply to all IPOs, and not only those relating to interception.

2.9 From a scrutiny perspective, the committee considers that the bill should be amended to provide that the power to issue IPOs be limited to judicial officers or, at a minimum, to judicial officers and a President or Deputy President of the AAT with at least five years' experience as a legal practitioner.

4 Proposed paragraph 60(5)(f).

2.10 The committee also considers that the bill should be amended to specify that, in relation to all IPOs, the issuing officer must have regard to whether the relevant method of surveillance would be the method that is likely to have the least interference with any person's privacy.

2.11 The committee otherwise draws its scrutiny concerns to the attention of senators, and leaves to the Senate as a whole the appropriateness of allowing members of the AAT to issue IPOs.

Public interest monitors

2.12 The committee notes the minister's advice that the bill aligns the IPO regime with the regime for domestic interception warrants. The committee also notes the minister's advice that the bill intentionally provides for the involvement of public interest monitors only in relation to IPOs for interception.

2.13 The committee also notes the minister's advice that public interest monitor arrangements only exist in Victoria and Queensland. Consequently, the bill only provides for public interest monitors for interception IPOs in those jurisdictions.

2.14 While acknowledging this advice, there does not appear to be anything that would prevent the bill from establishing public interest monitor or similar arrangements for IPOs at a national level.

2.15 Further, the committee does not consider consistency with existing legislation to be sufficient justification for restricting the involvement of public interest monitors to applications for interception IPOs. In this regard, the committee emphasises that the involvement of public interest monitors is an important safeguard against arbitrary or unlawful interference with privacy.

2.16 The committee therefore reiterates its scrutiny view that the bill should be amended to allow public interest monitors to make submissions, and appear at hearings, in relation to all IPO applications—regardless of whether they relate to interception or involve the law enforcement agencies of a particular jurisdiction.

2.17 From a scrutiny perspective, the committee considers that the bill should be amended to establish a national public interest monitor scheme so that monitors may make submissions, and appear at hearings, in relation to all applications for international production orders, regardless of whether the order relates to interception or involves the law enforcement agencies of a particular jurisdiction.

2.18 The committee otherwise draws its scrutiny concerns to the attention of senators, and leaves to the Senate as a whole the appropriateness of restricting the involvement of public interest monitors to applications for IPOs relating to interception involving the law enforcement agencies of Queensland and Victoria.

Consistency of safeguards

2.19 The committee notes the minister's advice that replacing the threshold of 'likely to assist' with 'likely to *substantially* assist' may prevent law enforcement and intelligence agencies from accessing overseas information that is likely to assist in the investigation of serious crime and matters relating to national security.

2.20 In this regard, the committee notes the minister's advice that, during the early stages of an investigation, it would be extremely difficult for an agency to demonstrate that information is 'likely to substantially assist' the investigation before viewing the information. The committee notes the advice that telecommunications data—such as account details and IP addresses—is often collected during the early stages of an investigation. When seeking an IPO, agencies must demonstrate that this information is likely to assist the investigation—for example by determining a link between an account and suspected criminal activity. This identifies further lines of inquiry. The minister advised that the higher threshold of 'likely to substantially assist' could be detrimental to investigations by removing critical lines of inquiry.

2.21 In relation to the higher threshold of 'likely to substantially assist' being applied only to IPOs relating to control orders, the committee notes the minister's advice that this is appropriate because control orders have a protective or preventative purpose, and the person to whom the order applies is not necessarily suspected of involvement in further criminal activity.

2.22 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.23 In light of the information provided by the minister, the committee makes no further comment on this matter.

Oversight by the Commonwealth Ombudsman—clause 81

2.24 The committee notes the minister's advice that the inclusion of a three-month period in subclause 81(1) of the bill reflects the Ombudsman's advice that such a notification period is appropriate, given that the IPO scheme is a new scheme whose frequency of use is not yet known. The committee also notes the minister's advice that this is a marked reduction from other regimes. The committee notes the advice that both the *Crimes Act 1914* and the TIA Act establish a six-month notification period. The committee further notes the minister’s advice that the Ombudsman conducts inspections of agencies' use of covert and intrusive powers retrospectively, with records generally assessed after the relevant warrant, authorisation or order ceases to be in force.

2.25 The committee acknowledges that the three-month notification period reflects advice from the Ombudsman, and that this period is substantially shorter

than similar notification periods under other Commonwealth legislation. However, given the significant consequences that may flow from the issue of an IPO, from a scrutiny perspective, the committee remains concerned that a three-month notification period (rather than a shorter period of time) may still limit the Ombudsman's ability to provide effective and responsive oversight. The committee is also concerned that the bill does not appear to impose specific consequences for a failure to comply with the requirements in proposed section 81. It only provides that a failure to comply with those requirements does not affect the validity of an IPO.

2.26 In addition, the minister's advice regarding how the Ombudsman conducts inspections indicate that shortening the notification period in relation to IPOs may permit the Ombudsman to spend additional time scheduling and allocating resources before starting an inspection. Ideally, this would result in a more comprehensive inspection process and improved compliance outcomes. The committee therefore considers that an agency should be required to notify the Ombudsman that a control order IPO has been issued, and provide the Ombudsman with a copy of the IPO, as soon as reasonably practicable after the IPO is issued.

2.27 In this regard, the committee notes that this does not seek to alter the time required for the Ombudsman to complete an inspection. Instead, it would ensure that the Ombudsman has access to the information needed to commence an inspection as soon as possible.

2.28 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.29 From a scrutiny perspective, the committee considers that the bill should be amended to require the chief officer of a control order IPO agency to notify the Commonwealth Ombudsman that an IPO has been issued, and give the Ombudsman a copy of the IPO, as soon as reasonably practicable after the IPO is issued.

2.30 The committee otherwise draws its scrutiny concerns to the attention of senators, and leaves to the Senate as a whole the appropriateness of providing that the chief officer of a control order IPO agency may notify the Commonwealth Ombudsman that an IPO has been issued, and give the Ombudsman a copy of the IPO, up to three months after the IPO is issued.

Oversight by the Commonwealth Ombudsman—clause 144

2.31 The committee notes the minister's advice that clause 144 was drafted to mirror the oversight powers of the Ombudsman in section 87 of the TIA Act, and is consistent with other Commonwealth legislation. The committee notes the advice that changing 'reasonable grounds to believe' to 'reasonable grounds to *suspect*'

would require broader consideration not only across the TIA Act, but other Commonwealth laws.

2.32 The committee also notes the minister's advice that the government considers that amending only the TIA Act would lead to considerable confusion as to the thresholds that apply under different laws, despite the oversight role of the Ombudsman being broadly consistent across Commonwealth legislation.

2.33 While the committee acknowledges that the bill was drafted to mirror the oversight powers of the Ombudsman in section 87 of the TIA Act, the committee does not consider consistency with existing legislation alone to be sufficient justification for providing that the Ombudsman may obtain information when the Ombudsman has 'reasonable grounds to *believe*' an officer is able to give information, rather than the lower threshold of 'reasonable grounds to *suspect*'. In this regard, the committee notes that concerns about consistency in relation to the oversight role of the Ombudsman across Commonwealth legislation could be addressed by providing that the Ombudsman's power to obtain information is engaged when the Ombudsman has 'reasonable grounds to *suspect*' across the Commonwealth statute book.

2.34 From a scrutiny perspective, the committee considers that clause 144 of proposed Schedule 1 to the TIA Act should be amended to provide that the Ombudsman has the power to obtain relevant information from officers and members of staff if the Ombudsman has 'reasonable grounds to *suspect*' that the officer or member of staff is able to give the relevant information, rather than the higher threshold of 'reasonable grounds to *believe*'.

2.35 The committee otherwise draws its scrutiny concerns to the attention of senators, and leaves to the Senate as a whole the appropriateness of providing that the Ombudsman may only obtain information when the Ombudsman has 'reasonable grounds to *believe*' an officer is able to give information, rather than the lower threshold of 'reasonable grounds to *suspect*'.

Delegation of administrative powers—applications for international production orders[5]

2.36 In *Scrutiny Digest 5 of 2020* the committee requested the minister's advice as to:

- why it is necessary and appropriate to allow a broad range of persons to make an application for an international production order;
- whether the bill could be amended to:

5 Schedule 1, item 43, clause 22. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(ii).

- limit the persons who can make an application for an international production order to the heads of relevant agencies and members of the senior executive service (SES) (or equivalent); or
- at a minimum, require that the relevant agency head be satisfied that persons authorised to apply for an IPO have the relevant qualifications and expertise to do so.[6]

Minister's response

2.37 The minister advised:

Broad delegation of administrative powers

The Bill allows for an appropriate range of Commonwealth, State and Territory agencies to make an application for an international production order. This is primarily to reduce the burden on the current mutual legal assistance regime through providing an alternative investigative pathway and to ensure that investigations of serious crime and national security, and the monitoring of control orders, are able to be undertaken in a timely and effective manner.

The agencies and people within those agencies that can make an application for an international production order is intended to mirror the current arrangements under the TIA Act. The same agencies who can access this information domestically can do so internationally, in order to ensure they can successfully investigate serious crime, national security matters, and monitor control orders. Chief Officers of relevant agencies can delegate their powers to appropriate persons within their agencies to streamline processes to assist the relevant agency to enact and discharge its functions. Law enforcement and national security officers will receive training on the legislative requirements for making applications and will be supported by their legal areas to ensure that applications are of a high quality, and meet legislative requirements.

In terms of limiting who within agencies can make an application, please see response to 1.110 below for response.

Possible amendments

Consistent with the TIA Act regime, the Bill gives certain officers within agencies the ability to delegate the power to apply for an international production order. Independent of this consistency with domestic regimes, the separate policy reasoning for this is two-fold. Firstly, given the potential high volume of international production orders from Australian agencies, requiring agency heads or members of the senior executive service to make each application for an international production order would significantly reduce the speed with which agencies can request data

6 Senate Scrutiny of Bills Committee, *Scrutiny Digest 5 of 2020*, pp. 28-29.

under the international production order scheme and thereby significantly impair its utility. Secondly, agencies will be best placed to determine which officers are sufficiently qualified and across the factual circumstances of the investigations to ensure that independent decision-makers have before them sufficient opportunities to query facts forming the foundation of the application. In many cases, this may be the relevant investigating officer in charge of an investigation, rather than agency heads or members of the senior executive service.

Australia's law enforcement and national security agencies provide all officers with high levels of training and apply appropriate levels of oversight to officers when making warrant applications and authorisations through clearance chains and, in the case of law enforcement, the chain of command. Similar training and oversight will apply in respect of officers dealing with international production orders. Training often includes the legislative requirements for making applications, as well as outlining any support officers would receive from their respective legally qualified staff. This ensures that applications are of a high quality, and meet legislative requirements set by the Australian Parliament.

It is anticipated that before an agency may apply for an international production order under the Bill, the Australian Designated Authority will first examine the capabilities of the agency and offer training on the international production order framework to that agency's relevant personnel. If the Australian Designated Authority is satisfied of the agency's ability to comply with the requirements of the international production order regime, the Australian Designated Authority may certify that agency as eligible to seek communications data through the channels established by the Bill and the relevant designated international agreement. As part of that certification process, the agency will need to demonstrate that persons authorised to apply for an international production order are appropriately qualified.

While there is flexibility to determine who is best placed to make an application for each individual agency or department, other safeguards such as orders only being issued by an independent decision maker (e.g. an eligible judge or nominated AAT member) stand as a guard for insufficient or poor applications. Comprehensive oversight arrangements by the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security will also create accountability for how agencies approach the application process. For the above reasons, the Government does not think it is necessary to limit who can apply for an international production order.

Committee comment

2.38 The committee thanks the minister for this response. The committee notes the minister's advice that chief officers of relevant agencies may delegate their powers to appropriate persons within their agencies to streamline processes and

support the effective exercise of powers and functions. The committee notes the advice that law enforcement and national security officers will receive training on the legislative requirements for making applications, and will be supported by their legal areas to ensure that applications are high quality and meet legislative requirements.

2.39 The committee also notes the minister's advice that law enforcement and national security agencies apply appropriate levels of oversight to officers dealing with warrant applications through clearance chains and, in the case of law enforcement agencies, the chain of command. The committee notes the advice that similar levels of oversight will apply in respect of officers dealing with IPOs.

2.40 The committee further notes the minister's advice that it is anticipated that, before an agency may apply for an IPO, the Australian Designated Authority will examine the capabilities of the agency and offer training on the IPO framework to the agency's relevant personnel. As part of this process, the agency will need to demonstrate that persons authorised to apply for IPOs are appropriately qualified.

2.41 In relation to whether the bill could be amended to restrict the categories of persons who may apply for an IPO, the committee notes the minister's advice that the powers of delegation in the bill are consistent with the broader TIA Act regime.

2.42 The committee also notes the minister's advice that, given the potentially high volume of applications from Australian agencies, requiring agency heads and members of the SES to make each application for an international production order would significantly reduce the speed with which agencies can request data under the IPO scheme and thereby significantly impair the scheme's utility.

2.43 Finally, the committee notes the minister's advice that although there is flexibility to determine who is best-placed to make an application for an IPO on behalf of an agency, there are a number of general safeguards against insufficient or poor-quality applications. These include the requirement that IPOs only be issued by an independent decision-maker, and comprehensive oversight arrangements by the Ombudsman and the Inspector-General of Intelligence and Security.

2.44 The committee acknowledges that the circumstances of particular investigations may make it necessary to delegate the power to apply for IPOs to persons who are not members of the SES (or equivalent) in certain cases. However, the committee remains of the view that the power to apply for IPOs should only be delegated to persons with appropriate skills, training and expertise. This is to ensure that applications for IPOs are only made in appropriate circumstances, noting the potentially very significant trespass on personal rights and liberties flowing from the issue of an IPO. It is not apparent to the committee that such a requirement would interfere with the effective administration of the IPO scheme. Rather, the minister's advice indicates that such a requirement would simply codify existing practice.

2.45 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic

material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.46 From a scrutiny perspective, the committee considers that the bill should be amended to require that the relevant agency head must be satisfied that persons authorised to apply for IPOs possess the appropriate skills, training and expertise.

2.47 The committee otherwise draws its scrutiny concerns to the attention of senators, and leaves to the Senate as a whole the appropriateness of allowing a broad range of persons to apply for IPOs, in the absence of any legislative requirement that such persons possess appropriate skills, training and expertise.

No-invalidity clause[7]

2.48 In *Scrutiny Digest 5 of 2020* the committee requested the minister's advice as to the rationale for including a no-invalidity clause in relation to requirements to notify the Ombudsman about the issuing of control order IPOs or where the chief officer of an agency has contravened paragraph 114(1)(d).[8]

Minister's response

2.49 The minister advised:

> The notification requirement in clause 81 facilitates Commonwealth Ombudsman oversight of agency use of the international production order regime as it relates to control orders. This additional notification requirement in respect of control order international production orders is necessary given the extraordinary nature of the control order monitoring powers. Sub clause 81(3) seeks to clarify that if an agency fails to comply with the administrative requirements in sub clauses (1) or (2), the validity of the order remains unaffected. The purpose of this clause is to ensure that an administrative oversight does not result in the potential for invalidity.
>
> Control order international production order agencies are required to comply with their reporting obligations in this clause and more broadly throughout the Bill. However, sub clause 81(3) ensures that where an administrative reporting obligation is included and contravened, the contravention would not undermine the validity of the order, which could result in perverse outcomes eventuating, for instance the inability to obtain information relevant to preventing a terrorist attack or subsequent prosecution relating to that potential attack.

---

7 Schedule 1, item 43, clause 81. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a) (i) and (iii).

8 Senate Scrutiny of Bills Committee, *Scrutiny Digest 5 of 2020*, pp. 29-30.

> Control order international production order agencies will be subject to strict oversight by the Commonwealth Ombudsman, as is the case for existing agencies that can apply for a control order warrant. Failure to comply with obligations in clause 81 may result in the investigation and public reporting on agency practices. This is consistent with current practices under the TIA Act for domestic control order warrants.

Committee comment

2.50 The committee thanks the minister for this response, and notes the minister's advice that the no-invalidity clause was included in subclause 81(3) to ensure that administrative oversight does not result in the invalidity of a control order IPO. In this respect, the committee notes the advice that if a failure to comply with the relevant administrative requirements did mean that an IPO is invalid, this could result in perverse outcomes such as the inability to obtain information relevant to preventing a terrorist attack or prosecution relating to that potential attack.

2.51 The committee further notes the minister's advice that control order IPO agencies will be subject to strict oversight by the Commonwealth Ombudsman and that failure to comply with the obligations in clause 81 may result in the investigation and public reporting on agency practices.

2.52 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.53 In light of the information provided by the minister, the committee makes no further comment on this matter.

Delegation of administrative powers—functions of the Ombudsman[9]

2.54 In *Scrutiny Digest 5 of 2020* the committee requested the minister's advice as to:

- why it is necessary to allow most of the Ombudsman's powers and functions to be delegated to APS employees at any level; and
- whether the bill could be amended to:
  - provide some legislative guidance as to the scope of powers that might be delegated, or the categories of people to whom those powers might be delegated; or

9 Schedule 1, clause 148. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(ii).

- at a minimum, require that the Ombudsman be satisfied that persons performing delegated functions and exercising delegated powers have the expertise appropriate to the function or power delegated.[10]

Minister's response

2.55 The minister advised:

> *Delegation of administrative powers*
>
> The broad delegation power allows the Commonwealth Ombudsman to determine how best to allocate resources and who the most appropriate officers will be when executing the functions or powers of the Commonwealth Ombudsman. This position is consistent with existing powers to delegate under the TIA Act.
>
> This provision, and the provision at clause 149 regarding immunity from suit, replicate long standing provisions contained in the *Ombudsman Act 1976* (subsections 33 and 34) and mirror similar provisions contained in the oversight and accountability regimes established in the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* (Part 6), and the *Crimes Act 1914* (Part IAB).
>
> The purpose of the delegation provision is to ensure that the staff of the office of the Commonwealth Ombudsman can perform the functions of the Commonwealth Ombudsman as required. It is important that the Commonwealth Ombudsman be able to determine the most efficient, effective and appropriate means of operationalising his functions as between himself and his staff cognisant of the powers involved and the expertise required to exercise them. In practice exercise of these functions and powers is limited to members of the team within the office of the Commonwealth Ombudsman responsible for conducting inspections of covert and intrusive powers by agencies.
>
> *Possible amendments*
>
> The choice of delegate is largely a matter to be determined by the person making the delegation. However, the Government expects that where delegation is appropriate and permitted by domestic law, the original decision-maker will consider the appropriateness and the expertise required to perform that delegation effectively and in line with Australian community expectations.

Committee comment

2.56 The committee thanks the minister for this response. The committee notes the minister's advice that the purpose of the delegation provisions is to ensure the Office of the Commonwealth Ombudsman can perform the Ombudsman's functions

10 Senate Scrutiny of Bills Committee, *Scrutiny Digest 5 of 2020*, pp. 30-31.

as required. The committee also notes that the provisions are consistent with other provisions in the TIA Act, as well as provisions relating to oversight and accountability in other Commonwealth legislation.

2.57 The committee acknowledges the minister's advice that it is important for the Ombudsman to be able to determine the most efficient, effective and appropriate means of operationalising his functions as between himself and his staff—cognisant of the powers involved and the expertise required to exercise them. The committee further notes the advice that, in practice, the exercise of the relevant functions and powers is limited to members of the team within the Office of the Commonwealth Ombudsman responsible for conducting inspections of covert and intrusive powers by agencies.

2.58 While noting this advice, the committee remains concerned that the bill would permit the Commonwealth Ombudsman to delegate functions and powers to a broad range of persons—including APS employees responsible to the Ombudsman and other persons with similar roles—without any guidance on the face of the bill as to how the powers of delegation are to be exercised.

2.59 In addition, the committee does not consider operational efficiency—or consistency with other laws—to be sufficient justification for permitting the delegation of significant functions and powers to APS officers at any level. In this respect, the committee acknowledges that it may be necessary for a range of APS officers to undertake work on the Ombudsman's behalf. However, the committee considers it important that the Ombudsman, or sufficiently qualified and senior staff, remain accountable for the exercise of the Ombudsman's powers.

2.60 The committee therefore considers that the bill should specify that the Ombudsman's powers and functions may only be delegated to certain persons or positions or, at a minimum, specify that the Ombudsman must be satisfied that persons performing delegated functions or exercising delegated powers possess appropriate training, qualifications and expertise. The minister's advice regarding how powers of delegation are exercised in practice indicates that such a requirement would not interfere with the effective administration of the Office of the Commonwealth Ombudsman. Rather, the requirement would only codify existing practice.

2.61 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.62 From a scrutiny perspective, the committee considers that the bill should be amended to restrict the delegation of the Commonwealth Ombudsman's powers under the international production orders scheme to specific persons or roles or, at a minimum, require that the Ombudsman be satisfied that persons

exercising delegated functions and powers possess the expertise appropriate to the relevant function or power.

2.63 The committee otherwise draws its scrutiny concerns to the attention of senators, and leaves to the Senate as a whole the appropriateness of allowing the Commonwealth Ombudsman to delegate functions and powers to Commonwealth APS officers at any level, and to persons with equivalent functions in other jurisdictions, in the absence of any legislative requirement that persons exercising delegated functions and powers possess appropriate skills, training and expertise.

Immunity from liability[11]

2.64 In *Scrutiny Digest 5 of 2020* the committee requested the minister's advice as to why it is necessary to provide the Ombudsman, an inspecting officer, or a person acting under an inspecting officer's direction or authority with immunity so that affected persons have their right to bring an action to enforce their legal rights limited to situations where lack of good faith is shown.[12]

Minister's response

2.65 The minister advised:

> As mentioned above, clause 149 ensures the Commonwealth Ombudsman and staff with the office of the Commonwealth Ombudsman are able to perform their inspection functions under Part 10 without being impeded by the possibility of legal action. This provision is fundamental to enabling the Commonwealth Ombudsman and their staff to carry out their functions and powers freely and independently within the confines of the law. This immunity only applies if the inspection functions are being carried out in good faith. Immunity provisions of this kind are long-standing safeguards afforded to the Commonwealth Ombudsman and staff of the office of the Commonwealth Ombudsman, and similar immunities are contained elsewhere, such as section 33 of the *Ombudsman Act 1976*.

Committee comment

2.66 The committee thanks the minister for this response. The committee notes the minister's advice that the proposed immunity is fundamental to enabling the Commonwealth Ombudsman and their staff to carry out their functions and powers freely and independently within the confines of the law. The committee also notes the advice that the immunity only applies if the relevant functions are being carried out in good faith.

---

11 Schedule 1, clause 149. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(i).

12 Senate Scrutiny of Bills Committee, *Scrutiny Digest 5 of 2020*, pp. 31.

2.67 The committee further notes the minister's advice that immunity provisions of this kind are long-standing safeguards afforded to the Ombudsman and staff of their office, and similar immunities are contained elsewhere—such as in section 33 of the *Ombudsman Act 1976.*

2.68 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.69 In light of the information provided by the minister, the committee makes no further comment on this matter.

Evidentiary certificates[13]

2.70 In *Scrutiny Digest 5 of 2020* the committee requested the minister's advice as to whether the bill can be amended to provide that an evidentiary certificate made under clause 161 will be prima facie evidence rather than conclusive evidence of the matters stated in the certificate.[14]

Minister's response

2.71 The minister advised:

> Both prima facie and conclusive evidentiary certificates continue to be vital to the functioning of the TIA Act, and indeed, the effective administration of justice. Since the early 1990s, the TIA Act has included a framework for the use of evidentiary certificates. Consistent with existing provisions in the TIA Act, evidentiary certificates issued by designated communication providers are to be received into evidence in proceedings as conclusive evidence of the matters stated in the certificate, and evidentiary certificates issued by law enforcement are to be received into evidence in proceedings as prima facie evidence of the matters stated in the certificate.
>
> The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide) sets out best practice in terms of the application of whether evidentiary certificate provisions are prima facie or conclusive evidence of the matters stated within. The Guide also notes evidentiary certificate provisions may specify that certificates are conclusive evidence of the matters stated in it where they cover technical matters that are sufficiently removed from the main facts at issue.

13 Schedule 1, item 43, clause 161. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(i).

14 Senate Scrutiny of Bills Committee, *Scrutiny Digest 5 of 2020*, pp. 32.

> As noted by the Committee, the evidentiary certificates under clause 161 are to be treated in proceedings as conclusive evidence of the matters stated within from foreign designated communications providers. The policy objective here is the recognition of the inherent difficulties associated with having to have persons from those providers attend court to give witness testimony on matters that are merely technical or formal matters the provider had undertaken to comply with the international production order. These difficulties are likely to be compounded by the expected numbers of international production orders that will be focused on a few large foreign designated communications providers.
>
> These evidentiary certificates will not cover matters in dispute or matters that go to questions of legality. The provision of conclusive evidentiary certificates that apply to the technical or formal matters will ensure that courts have complete information before them to assist in the administration of justice.

Committee comment

2.72 The committee thanks the minister for this response. The committee notes the minister's advice that both *prima facie* and conclusive evidentiary certificates are vital to the functioning of the TIA Act, and to the administration of justice generally. In this respect, the committee notes the advice that evidentiary certificates issued under clause 161 are consistent with existing provisions in the TIA Act.

2.73 The committee also notes the minister's advice that certificates issued under clause 161 recognise inherent difficulties associated with requiring persons from foreign communications providers to attend court to give testimony on matters that are merely technical or formal. The committee notes the advice that these difficulties are likely to be compounded by the expected numbers of IPOs that will be focussed on a few large foreign communications providers. The committee further notes the minister's advice that evidentiary certificates issued under clause 161 will not cover matters in dispute or go to questions of legality.

2.74 The committee appreciates that the proposal to allow communications providers to issue conclusive evidentiary certificates under clause 161 recognises the difficulties associated with requiring the providers to attend court to give evidence. In addition, the committee notes that the *Guide to Framing Commonwealth Offences* states that conclusive certificates may be appropriate in limited circumstances where they cover technical matters that are sufficiently removed from the main facts at issue. The Guide points to subsection 18(2) of the TIA Act as an example of where the use of conclusive certificates may be appropriate.[15] Clause 161 of the bill is similar to subsection 18(2) of the TIA Act.

---

15 Attorney-General's Department, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers,* September 2011, p. 55.

2.75 However, the Guide also states that evidentiary certificates should generally only be used to settle formal or technical matters, and asserts that evidentiary certificate provisions should generally specify that certificates are prima facie evidence of the matters to which they relate, and allow an opportunity for evidence of contrary matters to be adduced. In relation to conclusive certificates, the Guide also asserts that requiring courts to exclude contrary evidence can destroy any reasonable chance to place complete facts before the court.[16]

2.76 The committee will have significant scrutiny concerns about the use of conclusive evidentiary certificates, and considers that any proposal to allow the use of such certificates should be accompanied by a detailed explanation as to why the certificates are appropriate. This should include an explanation of why it is necessary for the certificate to be conclusive evidence of the matters to which it relates rather than prima facie evidence. In this instance, while the minister's response explains why it is considered necessary use evidentiary certificates generally, it does not provide a clear explanation of why *conclusive* certificates are appropriate.

2.77 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.78 The committee otherwise draws its scrutiny concerns to the attention of senators, and leaves to the Senate as a whole the appropriateness of allowing designated communications providers to issue written certificates as conclusive evidence of the matters to which the certificates relate (rather than *prima facie* evidence), in the absence of a clear justification as to why the use of conclusive evidentiary certificates is appropriate.

Trespass on personal rights and liberties

Lack of parliamentary oversight

Privacy[17]

2.79 In *Scrutiny Digest 5 of 2020* the committee requested the minister's advice as to why it is considered necessary and appropriate to allow information held in Australia to be accessed by foreign governments, in circumstances where existing legislative protections for the accessing of information have been removed and no

16 Attorney-General's Department, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers,* September 2011, p. 55.

17 Schedule 1, item 43, clauses 168 and 169. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i), (iv) and (v).

safeguards are provided on the face of the bill to ensure a designated international agreement contains sufficient safeguards regarding the circumstances in which information can be accessed.

2.80 The committee also requested the minister's advice as to whether the bill can be amended to:

- set out minimum protections and safeguards related to privacy that must be included in designated international agreements;
- specify that designated international agreements must be tabled in the Parliament; and
- provide that any regulation that specifies the name of a designated international agreement does not commence until after the Parliament has had the opportunity to scrutinise the designated international agreement.[18]

Minister's response

2.81 The minister advised:

> The Bill facilitates Australia entering into international cross-border access to data agreements with like-minded foreign governments who share Australia's commitment to combating serious crime, rule of law principles, and who strive for electronic surveillance laws that respect the balance between the needs of law enforcement and national security with protecting their communities from arbitrary and unlawful interference to their privacy. Whilst the Bill provides the mechanism for these agreements to be designated by regulation (clause 3), before getting to this point agreements will be subject to considerable parliamentary and public scrutiny, such as:
>
> 1. The Australian Government will conduct a thorough assessment of the privacy regime of the foreign country before entering into, and during, any agreement negotiations.
> 2. The Attorney-General and the Minister for Foreign Affairs will approve any proposed agreement before it is signed. Both Ministers have unique responsibilities for both domestic and international privacy matters.
> 3. Copies of the Treaty text will be tabled in parliament. The Department of Home Affairs will prepare a National Interest Analysis.
> 4. Any agreement will be referred to the Joint Standing Committee on Treaties (JSCOT) for consideration. Stakeholders and members of the public will be able to make submissions to JSCOT indicating any privacy concerns that JSCOT will take into account before providing its recommendations.

18 Senate Scrutiny of Bills Committee, *Scrutiny Digest 5 of 2020*, pp. 33-35.

5. Before Australia can ratify an Agreement, Regulations will be made under the TIA Act to declare the agreement as a 'designated international agreement'. Such Regulations will be subject to the normal disallowance periods in parliament, and to oversight by parliamentary committees such as the Parliamentary Joint Committee on Human Rights.

Accordingly, there will be considerable opportunities for the Australian Parliament and the Australian community to scrutinise proposed agreements that go to facilitating efficient and effective access to electronic data to combat serious crime.

A thorough assessment will be conducted of applicable domestic laws and policies of the foreign government before entering into any agreement. This will be supported by a range of safeguards and restrictions to reflect in those agreements Australian values such as rule of law, privacy considerations and that electronic surveillance powers be exercised under a purported agreement where it is necessary, proportionate and reasonable.

Privacy

Our collective safety and security depends on the ability of Australian agencies to maintain lawful and efficient access to electronic evidence. The Bill creates a framework for ensuring that Australia can enter into international cross-border access to data agreements with trusted foreign countries while respecting privacy interests and foreign sovereignty. However, the benefits of allowing Australian law enforcement agencies and ASIO to be able to directly issue orders on foreign providers, cross-border arrangements and agreements would need to be reciprocal.

For example, in order for Australia to be a qualifying foreign government that is able to enter into an agreement under the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act, it must ensure the removal of blocking statutes. Blocking statutes are laws that would prevent the United States Government from issuing legal process directly on Australian providers to access electronic information held in Australia. Accordingly, it was necessary that amendments be made to the *Telecommunications Act 1997* to clarify that disclosures would be authorised by law for the purposes of the *Privacy Act 1988* so as to ensure that Australian providers were legally able to comply with such legal process.

The Bill sets the outer framework for these agreements, whilst the treaty negotiation process and the agreements themselves will provide flexibility for Australia to ensure that individual agreements reflect appropriate safeguards and restrictions, and the changing technological environment. Agreements negotiated will have a range of safeguards and restrictions to ensure respect for privacy and civil liberties, rule of law, requirements for appropriate thresholds, and independent authorisation processes, to ensure orders are reasonable, necessary and proportionate. These necessary safeguards set an important foundation for future negotiations

of cross-border access to data agreements with like-minded foreign governments.

Possible amendments

The Government considers that the current framing of the Bill permits sufficiently strong protections and safeguards to be agreed on between governments when negotiating cross-border access to data agreements. Australia's treaty-making process requires that all treaties be subject to Parliamentary scrutiny, including tabling in Parliament. Ordinarily, the treaty text is tabled before the Parliament to ensure transparency and allow for Parliamentary scrutiny processes to occur. Please refer to the response under 1.131 detailing the available opportunities that the Australian Parliament would have to scrutinise any cross-border access to data agreements that the Government pursues.

Committee comment

2.82 The committee thanks the minister for this response.

Trespass on personal rights and liberties

2.83 The committee notes the minister's advice that the bill creates a framework for ensuring that Australia can enter into international cross-border access to data agreements with trusted foreign countries, while respecting privacy interests and foreign sovereignty. This includes allowing Australian law enforcement agencies and ASIO to issue orders on foreign providers. The committee notes the advice that the benefits conferred on Australia under such agreements would need to be reciprocal and, as a consequence, it was necessary to dis-apply certain Australian privacy laws to ensure Australian providers can comply with requests by foreign governments.

2.84 The committee also notes the minister's advice that the bill sets the legal framework for entering into the relevant agreements, while treaty negotiation processes and the agreements themselves provide flexibility for Australia to ensure individual agreements include appropriate safeguards and reflect the changing technological environment. In this respect, the committee notes the advice that the relevant agreements will contain a range of safeguards and restrictions to ensure that personal rights and liberties are adequately protected.

2.85 The committee further notes the minister's advice that, before an agreement is made, the Australian Government will conduct a thorough assessment of the privacy regime of the foreign country—noting that it will be the laws of the foreign country that will establish the safeguards which apply when a foreign government requests information from Australian providers. The committee also notes the advice that the ministers responsible for domestic and international privacy matter (that is, the Attorney-General and the Minister for Foreign Affairs) must approve any proposed agreement before it is signed.

2.86 The committee welcomes the advice that the government will undertake a thorough assessment of the privacy regime of the relevant foreign country before

entering into such agreements, including approval by the Attorney-General and Minister for Foreign Affairs. However, the committee remains concerned that the bill provides no guidance as to what must be included in reciprocal agreements between Australia and foreign governments, no guidance as to how the issue of orders or the making of requests will occur, and no guidance as to the persons or entities which constitute 'competent authorities'. Further, while noting that an assessment of the privacy regime of the relevant foreign country may occur in practice, the committee remains concerned that there is nothing on the face of the bill that would *require* such an assessment to be conducted, or require the relevant minister or ministers to be satisfied that the laws of the foreign country provide adequate privacy protections.

2.87 Additionally, while noting the minister's advice that agreements will have a range of safeguards to ensure respect for personal rights and liberties, there is no requirement on the face of the bill that the relevant minister(s) be satisfied that the relevant foreign country has appropriate legal and democratic processes in place, and that these processes are underpinned by the rule of law and the separation of powers.

2.88 The committee therefore remains of the view that, as currently drafted, these provisions have the potential to significantly trespass on personal rights and liberties.

Parliamentary oversight

2.89 In relation to the oversight mechanisms that apply to access to data agreements, the committee notes the minister's advice that copies such agreements will be tabled in Parliament and will be referred to the Joint Standing Committee on Treaties for consideration. In addition, the committee notes the minister's advice that, before Australia can ratify an agreement, the name of the agreement must be specified in regulations. The committee notes the advice that such regulations will be subject to disallowance, and to oversight by parliamentary committees such as the Parliamentary Joint Committee on Human Rights.

2.90 While noting this advice, given the significant nature of the agreements and associated powers and the potential trespass on personal rights and liberties, the committee considers that the bill should be amended to provide that any regulation that specifies the name of a designated international agreement does not come into effect until it has been approved by resolution of each House of the Parliament.[19]

2.91 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic

19 For an example of this approach, see section 10B of the *Health Insurance Act 1973*.

material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.92 The committee considers that the provisions of the bill as currently drafted have the potential to significantly trespass on personal rights and liberties, particularly in circumstances where access to information held in Australia may be given to foreign jurisdictions whose governance structures are not underpinned by respect for the rule of law and the separation of powers.

2.93 The committee considers that the bill should be amended to:

- **specify minimum protections and safeguards related to privacy that must be included in designated international agreements;**
- **require that, before the Australian Government signs a designated international agreement with a foreign government:**
    - **the Australian Government must conduct a publicly-available assessment of the laws and the legal and democratic processes of the relevant foreign country, to ensure that there are adequate safeguards in place against undue trespass on personal rights and liberties, including but not limited to undue trespass on the right to privacy; and**
    - **the ministers responsible for domestic and international privacy and human rights matters must approve the proposed agreement.**

2.94 In addition, from a scrutiny perspective, the committee considers that the bill should be amended to provide that any regulation that specifies the name of a designated international agreement does not come into effect until it has been approved by resolution of each House of the Parliament.

2.95 The committee otherwise draws its scrutiny concerns to the attention of senators, and leaves to the Senate as a whole the appropriateness of dis-applying Australian privacy laws in relation to requests by foreign governments for access to information held in Australia under designated international agreements, in the absence of safeguards on the face of the bill to ensure that the information is only accessed in appropriate circumstances, or express requirements that designated international agreements be subject to appropriate parliamentary oversight.

Chapter 3

Scrutiny of standing appropriations

3.1 Standing appropriations enable entities to spend money from the Consolidated Revenue Fund on an ongoing basis. Their significance from an accountability perspective is that, once they have been enacted, the expenditure they involve does not require regular parliamentary approval and therefore escapes parliamentary control. They are not subject to approval through the standard annual appropriations process.

3.2 By allowing the executive government to spend unspecified amounts of money for an indefinite time into the future, provisions which establish standing appropriations may, depending on the circumstances of the legislation, infringe on the committee's terms of reference relating to the delegation and exercise of legislative power.

3.3 Therefore, the committee has determined that, as part of its standard procedures for reporting on bills, it should draw Senators' attention to bills that establish or amend standing appropriations or establish, amend or continue in existence special accounts.[1] It will do so under provisions 1(a)(iv) and (v) of its terms of reference, which require the committee to report on whether bills:

> (iv) inappropriately delegate legislative powers; or
>
> (v) insufficiently subject the exercise of legislative power to parliamentary scrutiny.[2]

3.4 The committee draws the following bills to the attention of Senators:

- **Education Legislation Amendment (2020 Measures No. 1) Bill 2020** — Schedule 2, item 1, clause 5; and Schedule 2, item 2, clause;
- **Treasury Laws Amendment (2020 Measures No. 3) Bill 2020** — Schedule 1 item 4, subsection 8CAB(2).

Senator Helen Polley
Chair

---

1 The Consolidated Revenue Fund is appropriated for expenditure for the purposes of special accounts by virtue of section 80 of the *Public Governance, Performance and Accountability Act 2013*.

2 For further detail, see Senate Standing Committee for the Scrutiny of Bills *Fourteenth Report of 2005*.