Chapter 1

New and continuing matters

1.1 This chapter provides assessments of the human rights compatibility of:

- bills introduced into the Parliament between 17 and 20 September 2018;[1]
- legislative instruments registered on the Federal Register of Legislation between 23 August and 18 September 2018 (consideration of 4 legislative instruments from this period has been deferred);[2] and
- bills and legislative instruments previously deferred.

Instruments not raising human rights concerns

1.2 The committee has examined the legislative instruments registered in the period identified above, as listed on the Federal Register of Legislation. Instruments raising human rights concerns are identified in this chapter.

1.3 The committee has concluded that the remaining instruments do not raise human rights concerns, either because they do not engage human rights, they contain only justifiable (or marginal) limitations on human rights or because they promote human rights and do not require additional comment.

1 See Appendix 1 for a list of legislation in respect of which the committee has deferred its consideration. The committee generally takes an exceptions based approach to its substantive examination of legislation.

2 The committee examines legislative instruments registered in the relevant period, as listed on the Federal Register of Legislation. See, https://www.legislation.gov.au/.

Response required

1.4 The committee seeks a response or further information from the relevant minister or legislation proponent with respect to the following bills and instruments.

Aged Care Quality and Safety Commission Bill 2018

Purpose	Establishes the Aged Care Quality and Safety Commission and sets out the Commission's functions, appointment processes for office holders, information sharing arrangements and other operational matters
Portfolio	Health
Introduced	House of Representatives, 12 September 2018
Rights	Right to privacy, criminal process rights
Status	Seeking additional information

Information disclosure powers

1.5 The bill seeks to establish a National Aged Care Quality and Safety Commission. Division 4 of Part 7 of the bill contains provisions regarding the use and disclosure of information, including protected information. 'Protected information' is defined in proposed subsection 60(2) of the bill as personal information, or information that relates to the affairs of an approved provider or a service provider of a Commonwealth funded aged care service, that is acquired under, or for the purposes of the, the Act or rules.

1.6 Proposed section 61 sets out the circumstances in which the National Aged Care Quality and Safety Commissioner (the Commissioner) may disclose protected information. These include:

- where the Commissioner determines, in writing, that it is necessary in the public interest to disclose the information in a particular case – to such persons and for such purposes as the Commissioner determines;[3]
- where the disclosure is made to a person who is, in the opinion of the Commissioner, expressly or impliedly authorised by the person or body to whom the information relates to obtain it;[4]
- where the disclosure is made to the Secretary to assist in the performance of their functions, or to the Chief Executive of Medicare for the purposes of payment subsidies under the *Aged Care Act 1997* (Aged Care Act);[5]

3 Section 61(1)(a).

4 Section 61(1)(b).

- where the Commissioner believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious risk to the safety, health or well-being of an aged care consumer, and the disclosure is made to such persons as the Commissioner determines, for the purpose of preventing or lessening the risk;[6]
- where the commissioner believes, on reasonable grounds, that a person's conduct breaches the professional conduct standards of a profession of which the person is a member, and the person should be reported to a body responsible for professional conduct standards, to maintain those standards;[7]
- where the disclosure is made to a person who has temporarily taken over the provision of care through a particular service to aged care consumers, to enable the person to properly provide that care;[8]
- where the Commissioner believes, on reasonable grounds, that disclosure of the information is necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or the protection of the public revenue, to an agency responsible for such enforcement or protection;[9]
- where the disclosure is made to the Aged Care Pricing Commissioner to assist in the performance of their functions under the Aged Care Act;[10] and
- where the disclosure is made to a person of a kind specified in the rules, for a purpose specified by the rules.[11]

1.7 Proposed section 60 makes it an offence punishable by two years' imprisonment for a person to make, use or disclose protected information obtained in the course of performing their functions, or exercising their powers, under or for the purposes of the Act or rules. Proposed section 62 makes it an offence punishable by two years' imprisonment for a person to record, use or disclose information that was disclosed to them under section 61 for a purpose other than that prescribed by section 61.

---

5 Section 61(1)(c), (d).

6 Section 61(1)(e).

7 Section 61(1)(f).

8 Section 61(1)(g).

9 Section 61(1)(h).

10 Section 61(1)(i).

11 Section 61(1)(j).

Compatibility of the measure with the right to privacy

1.8 The right to privacy includes the respect for private and confidential information, particularly the storing, use and sharing of such information, and the right to control the dissemination of information about one's private life.[12]

1.9 As acknowledged by the statement of compatibility,[13] the power to disclose protected information (including personal information) engages and limits the right to privacy. The right to privacy may be subject to permissible limitations which are provided by law and are not arbitrary. In order for a limitation not to be arbitrary, it must pursue a legitimate objective, and be effective to achieve (that is, rationally connected to) and proportionate to that objective.

1.10 The statement of compatibility provides limited information about the objective of the information sharing powers. However, the explanatory memorandum explains that:

> [Proposed section 61] sets out a number of situations where a disclosure of protected information by the Commissioner is authorised. There are a number of clauses under the permitted disclosures which are included to enable the Commissioner to ensure the safety of aged care consumers in certain circumstances. These provisions are in place so that action can be taken immediately when required and there are no delays to protect aged care consumers.
>
> To hamper the ability of the Commissioner to disclose protected information goes against the very purpose of the existence of the Commission. The safety and welfare of aged care consumers is at the heart of the Commission, and the Commissioner must have the ability to disclose protected information swiftly when an aged care consumer's safety, health or well-being is or may be at risk.[14]

1.11 In light of this information, it is possible that the measure pursues a legitimate objective under human rights law and is rationally connected to that objective.

1.12 In relation to proportionality, the statement of compatibility provides the following information regarding the availability of safeguards to protect against the disclosure of personal information:

> Part 7 of the Bill contains protections for personal information about individuals that is collected by staff of the Commission in the performance

12 See, article 17 of the International Covenant on Civil and Political Rights, article 22 of the Convention on the Rights of Persons with Disabilities (CRPD), and article 16 of the Convention on the Rights of the Child (CRC).

13 Statement of compatibility (SOC), pp. 3-4.

14 Explanatory statement (EM), p. 21.

of functions or the exercise of powers under the *Aged Care Quality and Safety Commission Act 2018* (once enacted).[15]

These provisions include a penalty of imprisonment for two years for the offence of making a record of, disclosing or otherwise using protected information except for permitted uses.

1.13 Such provisions, including proposed section 62 of the bill, are relevant safeguards to protect against unauthorised disclosure of personal information.

1.14 However, in order to be a proportionate limitation on the right to privacy, powers to disclose personal information must be sufficiently circumscribed and be only as extensive as is strictly necessary to achieve the objective of the measure.

1.15 In this regard, the statement of compatibility does not provide any information about what constitutes the 'public interest' for which information can be disclosed, nor does it clarify whether all persons and organisations to whom information may be disclosed under section 61 are subject to the *Privacy Act 1988* (Privacy Act). Further, the statement of compatibility does not provide any information as to the proposed power to disclose information pursuant to rules,[16] which raises additional questions as to whether the disclosure power is sufficiently circumscribed. It is not clear, for example, whether the rules will contain safeguards on the disclosure of personal information, such as requiring the consent of the person affected, or providing for review of the disclosure by an independent body. A copy of the proposed rules would assist in this respect.

Committee comment

1.16 The preceding analysis raises questions as to whether proposed section 61 of the bill is a proportionate limitation on the right to privacy.

1.17 The committee therefore seeks the advice of the minister as to whether the limitation on the right to privacy in proposed section 61 is proportionate, including:

- **what factors, if any, the Commissioner will have regard to in determining whether the disclosure of protected information is in the 'public interest' under proposed section 61(1)(a);**
- **whether, under proposed section 61, information may be disclosed to organisations that are not covered by the Privacy Act, and, if so, the sufficiency of other relevant safeguards to protect the right to privacy; and**

15 SOC, p. 3.

16 Section 61(1)(j) of the bill.

- **whether the power to disclose information pursuant to rules referred to in proposed section 61(1)(j) is sufficiently circumscribed and accompanied by adequate safeguards. The committee requests a copy of the proposed rules (or, if no copy is available, a detailed outline of the proposed rules as they relate to disclosure of information).**

Information sharing arrangements

1.18 Division 2 of part 7 of the bill contains provisions relating to information sharing between the Commissioner, secretary and minister.

1.19 Proposed section 56 provides that the Commissioner must give information to the secretary in accordance with the rules or at the secretary's request, where the secretary requires the information to perform their functions or exercise their powers. Section 57 similarly provides that the secretary must give information to the Commissioner at the Commissioner's request, where the information is available to the secretary, and the Commissioner requires the information to perform their functions.

1.20 Proposed section 58 provides that the minister may, by written notice, require the Commissioner to prepare a report or document about matters relating to the performance of the Commissioner's functions, and provide the report within the period specified by the notice. Subsection 58(4) provides that the minister may publish such a report or document on the internet or otherwise.

Compatibility of the measure with the right to privacy

1.21 The relevant principles relating to the right to privacy are outlined above at [1.8]. It is unclear whether the information that can be shared or published under Division 2 could include personal information, or whether Division 2 excludes the disclosure of such information because it is 'protected information'. To the extent that personal information might fall within the scope of 'information' prescribed by Division 2, questions arise as to whether the measure is a proportionate limitation on the right to privacy. This is particularly the case in relation to section 56, where the circumstances and the kind of information to be shared are to be specified in the rules. The statement of compatibility does not provide any information in this respect.

Committee comment

1.22 The preceding analysis indicates that, to the extent that personal information may be shared under Division 2 of part 7 of the bill, questions arise as to the proportionality of the measure in relation to the right to privacy.

1.23 The committee therefore seeks the advice of the minister as to:

- **whether personal information can be shared and published under division 2 of part 7, and, if so;**

- **whether the limitation on the right to privacy is proportionate to achieve the legitimate objective sought, including whether the circumstances in which personal information can be disclosed are sufficiently circumscribed, and the availability of any relevant safeguards.**

Reverse evidential burden of proof

1.24 Proposed subsection 60(1) of the bill would make it an offence for a person to record, use or disclose protected information, including personal information, to another person if they obtain such information in the course of performing functions or exercising powers under, or for the purposes of, the (proposed) Act or the rules.

1.25 Proposed subsection 60(3) provides that subsection 60(1) does not apply if:

- the person makes, uses or discloses the information in the course of performing their functions or exercising their powers under, or in relation to, the Act, the rules, the Aged Care Act or the Aged Care principles; or
- the conduct is authorised by the person or body to whom the information relates; or
- the conduct is otherwise authorised by the Act, the rules or any other Act.

1.26 Proposed subsection 60(4) provides that subsection 60(1) does not apply if the disclosure is to the person or body to whom the information relates or the disclosure is to the minister or the secretary.

1.27 For each of these defences, the defendant bears an evidential burden in relation to proving the relevant matters.

Compatibility of the measure with the right to be presumed innocent

1.28 Article 14(2) of the International Covenant on Civil and Political Rights protects the right to be presumed innocent until proven guilty according to law. Generally, consistency with the presumption of innocence requires the prosecution to prove each element of a criminal offence beyond reasonable doubt. 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, engage and limit this right.

1.29 Reverse burden offences will not necessarily be inconsistent with the presumption of innocence provided that they are within reasonable limits which take into account the importance of the objective being sought and maintain the defendant's right to a defence. In other words, such provisions must pursue a legitimate objective, be rationally connected to that objective and be a proportionate means of achieving that objective.

1.30 In accordance with *Guidance Note 1*, the committee's expectation is that where a reverse burden offence is introduced, the statement of compatibility will provide a human rights assessment of this measure. Further, the committee's *Guidance Note 2* sets out some of the key human rights compatibility issues in

relation to provisions that create offences (including reverse burden offences) in order to assist legislation proponents.

1.31 In relation to the defences in subsections 60(3) and (4), the defendant bears an evidential burden (requiring the defendant to raise evidence about the matter). However, the statement of compatibility does not identify that the reverse burden offences in the bill engage and limit the presumption of innocence, and therefore does not provide an assessment as to whether the limitation is permissible. Relevant information in this respect would include whether the matters for which the defendant is required to raise evidence include information that would be peculiarly within the knowledge of the defendant.

Committee comment

1.32 The committee draws to the attention of the minister its *Guidance Note 2* which sets out information specific to reverse burden offences.

1.33 The committee requests the advice of the minister as to the compatibility of the reverse burden provisions with the right to be presumed innocent. In particular:

- **whether the reverse burden offence is aimed at achieving a legitimate objective for the purposes of international human rights law;**
- **how the reverse burden is effective to achieve (that is, rationally connected to) that objective; and**
- **whether the limitation is a reasonable and proportionate measure to achieve the stated objective.**

Crimes Legislation Amendment (Police Powers at Airports) Bill 2018

Purpose	Seeks to amend the *Crimes Act 1914* to introduce new powers at major airports, including the power for constables and protective service officers to give directions to persons to provide identification, move-on, or stop.
Portfolio	Home Affairs
Introduced	House of Representatives, 12 September 2018
Rights	Multiple rights
Status	Seeking additional information

Increased police powers at airports

1.34 The bill seeks to amend the *Crimes Act 1914* (Crimes Act) to expand the powers of police and protective service officers (PSO)[1] at the premises[2] of major airports.[3]

Directions to provide identity information at airports

1.35 Currently, section 3UM of the Crimes Act provides that a constable may request a person provide evidence of their identity where the constable reasonably

1 'protective service officer' means an Australian Federal Police (AFP) employee (other than a member) who has been declared by the Commissioner of the AFP to be a protective service officer of the AFP. The Commissioner may make such a declaration if the Commissioner is satisfied that the employee meets competency and qualification requirements specified in a determination: see sections 40EA and 40EB of the *Australian Federal Police Act 1979.* A 'member' of the Australian Federal Police means the Commissioner of Police, Deputy Commissioner of Police or an AFP employee in respect of whom a declaration under section 40B (which relates to employees other than protective service officers) is in force: see section 4 of the *Australian Federal Police Act 1979*.

2 'airport premises' is defined in section 239 of the *Airports Act 1996* to be a reference to (a) an airport site, if there is an airport lease for the airport; or (b) a building or other structure on such a site; and includes a part of any such premises.

3 'major airport' is defined in proposed section 3UL to mean (a) a Commonwealth aerodrome; (b) an airport in a Territory; or (c) an airport determined by the minister under proposed section 3UM. 'Commonwealth aerodrome' is defined in section 3 of the *Crimes (Aviation) Act 1991* to mean (a) an area of land or water in Australia that is owned by the Commonwealth and used, or intended for use, either wholly or partly, for, or in connection with, the arrival, departure or other movement of aircraft; or (b) a 'core regulated airport' as defined in section 7 of the *Airports Act 1996*; and includes any building, structure, installation or equipment in that area, or on the land that forms the core regulated airport, that is provided for use in connection with the operation of that area or land as an aerodrome or airport.

suspects the suspect has committed, is committing or intends to commit an offence against a law of the Commonwealth, or a law of a State or Territory, punishable by imprisonment for 12 months or more.

1.36 The bill seeks to introduce additional bases on which the powers can be exercised and additional persons who can exercise these powers. Proposed section 3UN provides that a constable or a PSO may direct a person to give the constable or PSO evidence of the person's identity (identification direction).[4] An identification direction may be issued if the constable or PSO:

- suspects on reasonable grounds that the person has committed, is committing, or intends to commit an offence against a law of the Commonwealth, or a law of a State having a federal aspect, punishable by imprisonment for 12 months or more; or
- considers on reasonable grounds that it is necessary to give the direction to safeguard 'aviation security'.[5] 'Aviation security' is defined in the bill to include the 'good order and safe operation' of a major airport and its premises, and flights to and from a major airport.[6]

Move-on directions at airports

1.37 Proposed section 3UO provides that a constable or PSO may give a direction to a person (a move-on direction) not to take a specified flight, or any flight, to or from that airport, or any specified major airport, for a specified period of no more than 24 hours after the direction is given.[7] A move-on direction may also direct a person to leave the airport premises as soon as practicable, and not enter those premises, or the premises of any specified major airport, for a specified period of no more than 24 hours after the direction is given .[8]

4 Evidence of a person's identity includes a government photographic identity document or, if the person does not produce such a document, another identity document or, if so directed, 2 different identity documents. If the person does not produce any of these identity documents the person may give the constable or officer the person's name, address and date of birth: see item 5 of Schedule 1 of the bill, proposed section 3UN(2).

5 See item 5 of Schedule 1 of the bill, proposed section 3UN(1).

6 See item 2 of Schedule 1 of the bill, proposed insertion into section 3UL.

7 See item 5 of Schedule 1 of the bill, proposed section 3UO(3).

8 See item 5 of Schedule 1 of the bill, proposed section 3UO(3).

1.38 A move-on direction may be given where:

- the constable or PSO considers on reasonable grounds that the person has contravened an identification direction or a direction to stop or do anything else pursuant to section 3UQ (discussed further below), and the constable or PSO is not reasonably satisfied of the person's identity;
- the constable or PSO suspects on reasonable grounds that it is necessary to give the direction to prevent or disrupt relevant criminal activity[9] occurring on the premises of any major airport, or in relation to a flight to or from any major airport; or
- the constable or PSO considers on reasonable grounds that it is necessary to give the direction to safeguard aviation security.

1.39 A move-on direction covering a period of more than 12 hours must be given, or authorised, by a senior police officer.[10] There are restrictions on repeated directions within seven days of the first move-on direction, such that no more than one later direction (the second direction) can be given within that period; the second move-on direction can only be given if: another assessment is made that the requirements to issue a move-on direction are satisfied; the second direction is given or authorised by a senior police officer; and the second period of exclusion from the airport premises would end no later than seven days after the first direction was given.[11]

Stop and ancillary directions powers at airports

1.40 Proposed section 3UQ provides that a constable or PSO may direct a person to stop or 'do anything else the constable considers on reasonable grounds to be necessary' to facilitate the direction to give identity information or the move-on direction.[12] A constable or PSO may give this direction if it is given on the premises of a major airport and the constable or PSO considers on reasonable grounds that it is necessary to give the direction to facilitate the exercise of the power to give a direction to give identity information or a move-on direction.[13]

---

9 'relevant criminal activity' is criminal activity involving the commission of an offence that is punishable by imprisonment for 12 months or more, against either the law of the Commonwealth or a law of the State having a federal aspect: see item 5 of Schedule 1 of the bill, proposed section 3UO(2).

10 A senior police officer is a constable having the rank of sergeant or an equivalent rank, or higher; or performing the duties of a constable having such a rank.

11 See item 5 of Schedule 1 of the bill, proposed section 3UO(6).

12 See item 5 of Schedule 1 of the bill, proposed section 3UQ(2).

13 See item 5 of Schedule 1 of the bill, proposed section 3UQ(1).

Compatibility of the measures with multiple rights

1.41 The identification, move-on and stop and ancillary directions powers introduced by the bill engage and may limit several human rights including:

- the right to privacy;
- the right to freedom of movement and the right to liberty;
- the right to freedom of expression and freedom of assembly; and
- the right to equality and non-discrimination.[14]

1.42 Each of these rights is discussed further below.

Compatibility of the measures with the right to privacy

1.43 Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary or unlawful interferences with an individual's privacy, family, correspondence or home. As acknowledged in the statement of compatibility,[15] the bill engages and may limit the right to privacy as it requires a person to produce evidence of their identity to a constable or PSO if certain circumstances exist. The right is also engaged by the stop and ancillary directions powers, as a person may be directed to do anything the constable considers on reasonable grounds to be necessary to facilitate the exercise of an identification direction.[16]

1.44 The right to privacy may be subject to permissible limitations which are provided by law and are not arbitrary. In order for limitations not to be arbitrary, the measure must pursue a legitimate objective and be rationally connected and proportionate to that objective.

1.45 The statement of compatibility describes the objective of the measures as follows:

> The purpose of these directions is to enhance safety and security in airports in a context where aviation remains a high-profile, high-impact

14 In the context of the stop, search and seize powers in Division 3A of Part IAA of the Crimes Act (which relate to powers in relation to terrorist acts and terrorism offences), the committee has previously stated that other human rights that may be engaged by such powers include the right to a fair trial and fair hearing and the right to be treated with humanity and dignity: see the committee's analysis of the Counter-Terrorism Legislation Amendment (No.1) Bill 2018 in Parliamentary Joint Committee on Human Rights, *Report 10 of 2018* (18 September 2018) pp.45-53; *Report 6 of 2018* (26 June 2018) pp.21-29. See also the committee's analysis of stop, search and seize powers in the committee's consideration of the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 in Parliamentary Joint Committee on Human Rights, *Fourteenth Report of the 44th Parliament* (28 October 2014); *Nineteenth Report of the 44th Parliament* (3 March 2015); *Thirtieth Report of the 44th Parliament* (10 November 2015).

15 Statement of compatibility (SOC) p. 22.

16 SOC, p. 22.

> target for terrorists. Airports are also a focal point for gang-related activities such as illicit drug trafficking, as well as other serious and organised crime. In light of these threats, and the fact that identity check directions can only be issued where there is a reasonable link between the direction and addressing criminal behaviour or aviation security concerns (ancillary orders are similarly confined), these directions are issued for the legitimate purpose of preserving national security, public order and the rights and freedoms of others.[17]

1.46 The statement of compatibility also explains that the new powers are aimed at addressing the following pressing and substantial concern:

> These powers seek to close a gap in existing Commonwealth law that allows people to scope potential vulnerabilities in security apparatus, where there is currently no ability for police to appropriately engage with individuals that are acting suspiciously on airport *premises*. In many cases, suspicious conduct may not necessarily lead to a suspicion that a person is involved in a particular offence – for example, a person may not be travelling on an aircraft or picking up or dropping off a passenger but are regularly observed in the airport precinct for no clear reason. Without specific intelligence that an offence has been, is being, or will be committed, AFP officers have reported that, under the current framework, they are unable to assess potential threats within airports by directing a person to provide evidence of their identity.[18]

1.47 Based on the information provided in the statement of compatibility, the stated objectives of enhancing safety and security in airports, and of preserving national security, public order and the rights and freedoms of others, are likely legitimate objectives for the purposes of international human rights law.

1.48 Directing a person to provide identification where it is necessary to safeguard aviation security, or where a person is suspected on reasonable grounds to have committed, be committing or be intending to commit particular offences, appears to be rationally connected to these objectives. However, it is not clear based on the information provided how the power to 'do anything else' necessary to facilitate the exercise of the identification directions power would necessarily be effective to achieve the objective, as the concept is extremely broad. Further information from the minister as to what ancillary directions would be included in the concept of 'do[ing] anything else' would assist in determining whether this aspect of the measures is rationally connected to the stated objective.

1.49 As to proportionality, the statement of compatibility states that the identification directions 'have a minimal impact on a person's privacy'.[19] This is

17 SOC, pp. 22-23.

18 SOC, p. 23.

19 SOC, p. 23.

relevant to determining whether the limitation on the right to privacy is proportionate.[20]

1.50 However, in order to be a proportionate limitation on the right to privacy, a limitation must be sufficiently circumscribed to ensure that it is only as extensive as is strictly necessary to achieve the objective. Here, questions arise as to whether the ability of the constable or PSO to issue an identification direction where they consider on 'reasonable grounds' that it is 'necessary' to give the direction to 'safeguard aviation security' is sufficiently circumscribed. In this respect, the statement of compatibility states that an identification direction issued to safeguard 'aviation security' is proportionate because:

> …the terms 'reasonable' and 'necessary' will ensure that the direction will be appropriate and proportionate to the activity it is seeking to prevent or disrupt, and will be implemented based on information available to police or an objective fact.[21]

1.51 While the requirements that a constable or PSO must have 'reasonable grounds' to consider it 'necessary' to issue an identification direction are important safeguards, concerns remain insofar as 'aviation security' is defined broadly to include the 'good order and safe operation' of major airports, their premises and flights to and from such airports. In particular, 'good order' is not defined in the bill, and it is unclear whether the concept would capture a broader range of conduct than is strictly necessary to fulfil the legitimate objectives of the bill. It is unclear, for example, whether a peaceful protest in a major airport would be conduct capable of disrupting the 'good order' of the airport so as to enliven the power to give an identification direction.[22]

1.52 Similarly, there are also concerns as to the breadth of the ancillary directions power to direct a person to 'to do anything else' considered on reasonable grounds to be necessary to facilitate the identification direction power. It is not clear, for example, whether this could require a person to remove an item of clothing (such as a facial covering) for the constable or PSO to ascertain a person's identification. This raises concerns that the measure may be insufficiently circumscribed. Further information as to what is envisaged by the ancillary power to require a person to 'do anything else' considered necessary to facilitate the identification direction power would assist in determining whether the measure is proportionate.

---

20 See, *Reyntjens v Belgium,* European Court of Human Rights Application No.1810/90, Decision on Admissibility (9 September 1992) p. 152.

21 SOC, p. 23.

22 This also raises related concerns in relation to the right to freedom of expression, discussed further below.

Committee comment

1.53 The preceding analysis raises questions as to the compatibility of the measures with the right to privacy.

1.54 The committee therefore seeks the further advice of the minister as to this matter, including:

- **whether the power in proposed section 3UQ(2)(b) of the bill to direct a person 'to do anything else' the constable or PSO considers on reasonable grounds to be necessary to facilitate the exercise of a power under proposed section 3UN is rationally connected to achieving the stated objective (including information as to what ancillary directions would be included in the scope of this power);**
- **whether the power to issue an identification direction under section 3UN(1)(b) is proportionate to the stated objective of the bill (including whether the power in proposed section 3UN(1)(b)(ii) to direct a person to provide identification where a constable or PSO considers on reasonable grounds it is necessary to give the direction to safeguard 'aviation security' is sufficiently circumscribed and accompanied by adequate safeguards); and**
- **whether the ancillary power in section 3UQ(2)(b) to direct a person to 'do anything else' the constable or PSO considers on reasonable grounds to be necessary to facilitate the exercise of a power under proposed section 3UN is proportionate (including whether the measure is sufficiently circumscribed and accompanied by adequate safeguards).**

Compatibility of the measures with the right to freedom of movement and the right to liberty

1.55 Article 12 of the ICCPR protects freedom of movement. The right to freedom of movement includes the right to move freely within a country for those who are lawfully within the country, and also includes the right to leave a country. The right to leave a country encompasses both the legal right and practical ability to leave a country, and therefore it applies not just to departure for permanent emigration but also for the purpose of travelling abroad. There can be limitations on the right to leave a country, including where it is necessary and proportionate to achieve the objectives of protecting the rights and freedoms of others, national security, public health or morals, and public order.

1.56 As acknowledged in the statement of compatibility, the right to freedom of movement is engaged by the bill in several respects. First, it is engaged by the move-on directions, which are capable of limiting the movement of a person in and out of major airports (including preventing them from leaving the country).[23] It is also

23 SOC, p. 19.

engaged and limited by the ancillary directions powers to direct a person to stop or to do anything else the constable considers on reasonable grounds to be necessary to facilitate the move-on powers.[24]

1.57 The statement of compatibility states that the move-on and ancillary directions serve a legitimate objective because the directions powers:

> …are designed to protect national security by preventing terrorist acts and to uphold the public order by preventing the commission of crime. These directions also protect the rights and freedoms of other persons at airports who may be affected by the behaviour of a person subject to a direction.[25]

1.58 The statement of compatibility also explains that while there are limited powers under the Commonwealth law to direct a person to move on from the premises of airports,[26] the existing powers are limited to safeguarding against unlawful interference with aviation rather than 'disruptive behaviour more generally'.[27] It also explains that there is a suite of move-on powers under state and territory legislation, but that these vary between the jurisdictions. Therefore the move-on directions powers in the bill 'will ensure police have access to consistent and targeted powers across Australia to exclude a person from the aviation environment in order to prevent and/or disrupt criminal or security threats'.[28]

1.59 Preventing or disrupting criminal or security threats may be capable of constituting legitimate objectives in the context of the move-on directions power, in light of the explanation in the statement of compatibility regarding the inadequacy of existing laws. However, in relation to the ancillary directions power, which would require a person to stop or do anything else necessary to facilitate the exercise of the identification or move-on directions powers, the statement of compatibility does not address why current laws are insufficient such as to warrant this additional power. Further information as to how the ancillary directions power addresses a pressing and substantial concern, including why current powers are insufficient, would assist in determining whether this measure pursues a legitimate objective for the purposes of international human rights law.

1.60 Directing a person to move-on by not taking a specified flight or leaving the airport premises would appear to be rationally connected to the stated objective.[29]

---

24 SOC, p. 19.

25 SOC, pp. 19-20.

26 One existing power is in section 86 of the *Aviation Transport Security Act 2004,* which allows law enforcement officers to move people on from a prescribed airport, security controlled airport or designated area or zone if they reasonably suspect a person is committing or has committed an offence under that Act: see SOC, p. 17.

27 SOC, p. 17.

28 SOC, p. 17.

29 See SOC, pp. 20-21.

However, as discussed above in relation to the right to privacy, it is not clear based on the information provided how the power to 'do anything else' necessary to facilitate the exercise of the move-on or identification directions power would be effective to achieve the objective, as the concept is very broad.

1.61 In relation to the proportionality of move-on directions, the statement of compatibility states that the measure takes the least rights restrictive approach on the following basis:

> …it allows an officer to determine the scope of the move-on direction and the duration of the exclusion period depending on what is reasonable and necessary in the circumstances. Furthermore, even if these directions limit a person's liberty of movement, they can be viewed as a less intrusive means than taking a person into detention or arresting them.[30]

1.62 The statement of compatibility also states that the requirement that the constable or PSO must suspect or consider on reasonable grounds that the move-on direction is necessary to achieve the permissible purposes also ensures that these directions will be used in a proportionate manner.[31]

1.63 The statement of compatibility states that the measures are necessary because:

> Allowing move-on directions to be issued in these instances is necessary to ensure that the central purpose of these orders, namely to facilitate early detection of dangerous or illegal activity, cannot be frustrated by a person simply refusing to abide by them.
>
> If a constable or PSO is not permitted to issue a move-on direction in these circumstances, a person who refuses to abide by the identity check or ancillary orders will be permitted to remain within a major airport or to take a flight to or from these airports, causing a potential considerable risk to aviation security or public order.[32]

1.64 However, the consequence of a move-on direction, including a requirement not to take a flight for a period of time, could be significant for a person. For example, a person directed not to take their flight when traveling with their family could be separated from their family as a result of the move-on direction.[33] Further, as discussed in relation to the right to privacy at [1.51] above, the breadth of the definition of 'aviation security' (including 'good order and safe operation' of major airports) raises questions as to whether the power would apply to a broader range of conduct than is strictly necessary to fulfil the legitimate objectives of the bill. This

30 SOC, p. 20.

31 SOC, p. 20.

32 SOC, p. 21.

33 This may also engage and limit the rights of the child and the right to protection of the family.

raises questions as to whether the move-on directions power to safeguard aviation security is sufficiently circumscribed.

1.65 In relation to the ancillary directions powers, the statement of compatibility states that while an ancillary directions order (such as an order to stop) may impede a person's freedom of movement, 'it remains necessary and proportionate as a constable or PSO must have reasonable grounds that the direction is necessary before it can be issued'.[34] The statement of compatibility also states that the phrase 'reasonable grounds' means that the constable or PSO 'must choose the least intrusive means to ensure that an identity check or move-on direction can be facilitated, as a more excessive option is unlikely to be found to be necessary on reasonable grounds'.[35]

1.66 However, there remain concerns as to whether this power is sufficiently circumscribed and accompanied by adequate safeguards in circumstances where it is not clear what the power to direct a person 'to do anything else' to facilitate the exercise of the identification and move-on directions powers entails. It is not clear, for example, whether it could require a person to sit in a separate room in the airport until the specified flight departs or the person's identity can be ascertained. It is also unclear whether there is any limitation to the duration of time in which a person can be stopped pursuant to an ancillary direction. This raises concerns that the measures may also not be accompanied by adequate safeguards.

1.67 Additionally, the ability to direct a person to stop for an undefined period of time coupled with a power to direct a person to 'do anything else' raises additional questions as to whether the measure may engage and limit the right to liberty. The right to liberty in Article 9 of the ICCPR prohibits state parties from depriving a person of their liberty except in accordance with the law, and provides that no one shall be subject to arbitrary detention. It applies to deprivations of liberty, rather than mere restrictions on whether a person can freely move around. However, a restriction on a person's movement may be to such degree and intensity that it would constitute a 'deprivation' of liberty, particularly if an element of coercion is present.[36] The statement of compatibility does not address whether the power to

---

34 SOC, p. 21.

35 SOC, p. 21.

36 United Nations Human Rights Committee, *General Comment No.27: Article 12 (Freedom of Movement)*, CCPR/C/21/Rev.1/Add.9 (2 November 1999) [7]; see also United Nations Human Rights Council, *Report of the Working Group on Arbitrary* Detention, A/HRC/22.44 (22 December 2012) [55] and [57]; *Foka v Turkey,* European Court of Human Rights Application No.28940/95, Judgment (24 June 2008) [78]; *Gillan and Quinton v United Kingdom,* European Court of Human Rights Application No.4158/05, Judgment (12 January 2010) [54]-[57]; *Austin v United Kingdom,* European Court of Human Rights Application Nos. 39692/09, 40713/09 and 41008/09, Grand Chamber, (15 March 2012) [57]; *Gahramanov v Azerbaijan*, European Court of Human Rights Application No.26291/06, Judgment (15 October 2013) [38]-[45].

direct a person to 'stop' or 'do anything else' may engage and limit the right to liberty.

Committee comment

1.68 The preceding analysis indicates that the measures in the bill engage and limit the right to freedom of movement. The committee seeks the further advice of the minister as to the compatibility of the measures with this right, in particular:

- **whether there is reasoning or evidence that establishes that the stated objective addresses a pressing or substantial concern or whether the proposed changes are otherwise aimed at achieving a legitimate objective (including how current laws are insufficient to address this objective);**
- **how the measures are effective to achieve (that is, rationally connected to) that objective; and**
- **whether the limitation is a proportionate limitation on the right to freedom of movement, including whether:**
  - **the power to issue a move-on and ancillary direction where a constable or PSO considers on reasonable grounds it is necessary to give the direction to safeguard 'aviation security' is sufficiently circumscribed and accompanied by adequate safeguards; and**
  - **the ancillary power to direct a person to stop or 'do anything else' the constable or PSO considers on reasonable grounds to be necessary to facilitate the exercise of the move-on or identification direction is sufficiently circumscribed and accompanied by adequate safeguards.**

1.69 The preceding analysis also indicates the ancillary powers to require a person to stop or 'do anything else' to facilitate the exercise of the identification and move-on directions powers may engage and limit the right to liberty. The committee therefore seeks the further advice of the minister as to the compatibility of the measures with this right.

Compatibility of the measures with the right to equality and non-discrimination

1.70 The right to equality and non-discrimination provides that everyone is entitled to enjoy their rights without discrimination of any kind, and that all people are equal before the law and entitled without discrimination to the equal and non-discriminatory protection of the law.[37] Equality before the law provides that law must not be applied by law enforcement authorities or the judiciary in an arbitrary or discriminatory manner.

37 See Articles 2 and 26 of the International Covenant on Civil and Political Rights; Articles 2, 4, 5 and 7 of the International Convention on the Elimination on All Forms of Racial Discrimination.

1.71 'Discrimination' is defined as a distinction based on a personal attribute (for example, race, sex or religion)[38], which has either the purpose ('direct' discrimination), or the effect ('indirect' discrimination), of adversely affecting human rights.[39] The UN Human Rights Committee has explained indirect discrimination as 'a rule or measure that is neutral on its face or without intent to discriminate', which exclusively or disproportionately affects people with a particular personal attribute.[40] Where a measure impacts on particular groups disproportionately, it establishes *prima facie* that there may be indirect discrimination.

1.72 The statement of compatibility states that the proposed identity check, move-on and ancillary directions will apply equally to all persons within a major airport regardless of age, gender, ethnicity, religious background or other status.[41] However, there are questions as to whether the powers to issue directions where a constable or PSO considers on reasonable grounds that a person has committed, is committing, or intends to commit certain offences, or that it is necessary to safeguard aviation security, may engage this right. This is because, unless there are sufficient safeguards, the directions powers introduced by the bill have the potential, in practice, to be applied in a manner which may target, for example, persons with certain physical characteristics or of particular national or ethnic origins. Where this kind of targeting occurs, without objective or reasonable justification, it will be incompatible with the right to equality and non-discrimination.[42] That is, it may result in the law being applied in ways that are discriminatory, and may have a disproportionate or unintended negative impact on particular groups based on race or religion and therefore be potentially indirectly discriminatory. This form of targeting is often referred to as racial profiling.

1.73 Differential treatment (including the differential effect of a measure that is neutral on its face) will not constitute unlawful discrimination if the differential treatment is based on reasonable and objective criteria such that it serves a

---

38 The prohibited grounds are race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Under 'other status' the following have been held to qualify as prohibited grounds: age, nationality, marital status, disability, place of residence within a country and sexual orientation.

39 United Nations Human Rights Committee, *General Comment No.18: Non-Discrimination* (1989).

40 *Althammer v Australia,* UN Human Rights Committee Communication No.998/01 (2003) [10.2].

41 SOC, p. 18.

42 *Williams Lecraft v Spain,* UN Human Rights Committee Communication No.1493/2006 (2009) [7.2]-[7.4]. See also United Nations Human Rights Council, *Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance,* A/HRC/29/46 (20 April 2015).

legitimate objective, is effective to achieve that legitimate objective and is a proportionate means of achieving that objective.

1.74 The statement of compatibility states that the 'reasonable grounds' requirement for each of the powers 'ensures that directions are based on actionable intelligence relevant to aviation security or criminal conduct' and that this requirement prevents a direction being issued 'solely on the basis of a person's age, ethnicity or religious background'.[43] The statement of compatibility further states in this respect that:

> Commonwealth officers exercising these powers are also bound by Commonwealth anti-discrimination legislation including the *Racial Discrimination Act 1975, the Sex Discrimination Act 1984, the Disability Discrimination Act 1992 and the Age Discrimination Act 2004*. State and territory officers are also bound by similar legislation within their own jurisdictions.
>
> Police officers are also bound by professional standards that preclude them from using their powers in a discriminatory fashion. The AFP Code of Conduct, for example, requires all AFP appointees to act without discrimination or harassment in the course of AFP duties. A breach of this Code may lead to disciplinary action, including termination.
>
> Constables and PSOs also receive specialist training to identify potential threats in a non-discriminatory manner. Members of the AFP, for example, are appropriately trained in Behavioural Assessment and Security Questioning to identify known behavioural traits displayed by people who are about to commit a criminal act, and to ask targeted questions of persons of interest, without prejudice or discrimination.[44]

1.75 The statutory frameworks relating to anti-discrimination are important safeguards, as is the requirement that a constable or PSO has 'reasonable grounds' before issuing a direction. However, as discussed above, the power to issue a direction on reasonable grounds is framed broadly, arising where a constable or PSO considers on reasonable grounds that exercising the power is necessary to safeguard aviation security (including 'good order', which is not defined), or where he or she suspects that a person 'intends to commit an offence'. The conferral of this widely framed power to an officer gives rise to a risk of arbitrariness or a risk that the power may be misused in a manner incompatible with the right to equality and non-discrimination.[45]

---

43 SOC, pp. 18-19.

44 SOC, p. 19.

45 See *Gillan and Quinton v United Kingdom,* European Court of Human Rights Application No.4158/05, Judgment (12 January 2010) [85].

1.76 The Committee on the Elimination of Racial Discrimination has stated that the fulfilment of the non-discrimination provisions of the International Convention on the Elimination of All Forms of Racial Discrimination requires national law enforcement officials who exercise police powers to receive intensive training to ensure that in the performance of their duties they respect as well as protect human dignity and maintain and uphold the human rights of all persons without distinction as to race, colour or national or ethnic origin.[46] In this respect, the AFP Code of Conduct and the Behavioural Assessment and Security Questioning are also relevant safeguards. However, further information as to how these professional standards apply in practice is required to assess whether such practices provide an adequate safeguard against the laws operating in a discriminatory manner. It is also not clear from the information provided the extent to which those frameworks will apply to PSOs, who are not members of the AFP.[47]

Committee comment

1.77 The preceding analysis indicates that the measures in the bill may engage and limit the right to equality and non-discrimination.

1.78 **The committee therefore seeks the advice of the minister as to the compatibility of the measures with this right, including:**

- **whether the measures in the bill are sufficiently circumscribed and accompanied by adequate safeguards to ensure that the powers in the bill are exercised in a non-discriminatory manner; and**
- **a copy of the AFP Code of Conduct, further information relating to the Behaviour Assessment and Security Questioning, and any other relevant information as to the professional standards and training that applies to AFP members and protective services officers to ensure that the powers in the bill will be exercised in a non-discriminatory manner.**

Compatibility of the measures with the right to freedom of expression and the right to freedom of assembly

1.79 The right to freedom of expression requires the state not to arbitrarily interfere with freedom of expression, particularly restrictions on political debate. It protects all forms of expression and the means of their dissemination, including spoken, written and sign language and non-verbal expression. The right to peaceful assembly is the right of people to gather as a group for a specific purpose.

1.80 As discussed above, due to the breadth of the definition of 'aviation security' (and in particular the words 'good order') it is unclear whether a peaceful protest in a

46 Committee on the Elimination of Racial Discrimination, *General Recommendation 13 on the training of law enforcement officials in the protection of human rights* (1993) [2].

47 See the definition of PSOs in sections 40EA and 40EB of the *Australian Federal Police Act 1979.*

major airport would be conduct capable of disrupting the 'good order' of the airport so as to enliven the power to give an identification, move-on or ancillary powers direction because the constable or PSO considers on reasonable grounds it is necessary to 'safeguard aviation security'. If this were the case, the measures would engage and may limit the right to freedom of expression and the right to freedom of assembly. These rights may be subject to permissible limitations where the measure pursues a legitimate objective, and is rationally connected to, and proportionate to achieving, that objective. However, the statement of compatibility does not acknowledge that this right is engaged and limited, so does not provide an assessment as to whether the limitation is justifiable under international human rights law.

Committee comment

1.81 The preceding analysis indicates the measures may engage and limit the right to freedom of expression and the right to freedom of assembly. The statement of compatibility does not acknowledge these rights may be engaged and limited by the bill. The committee therefore seeks the advice of the minister as to the compatibility of the measures with this right, including:

- **whether there is reasoning or evidence that establishes that the stated objective addresses a pressing or substantial concern or whether the proposed changes are otherwise aimed at achieving a legitimate objective;**
- **whether there is a rational connection between the limitation and that objective; and**
- **whether the limitation is a reasonable and proportionate measure for the achievement of that objective.**

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Purpose	Seeks to amend various Acts in relation to telecommunications, computer access warrants and search warrants to: introduce new provisions to allow law enforcement and security agencies to secure assistance from key providers in the communications supply chain both within and outside Australia; increase agencies' ability to use a range of measures, including to obtain computer access warrants, to covertly collect evidence from electronic devices, and to request a search warrant to be issued in respect of a person for the purposes of seizing a computer or data storage device.
Portfolio	Home Affairs
Introduced	House of Representatives, 20 September 2018
Rights	Multiple rights
Status	Seeking additional information

Technical assistance notices, technical capability notices and technical assistance requests

1.82 Schedule 1 of the bill seeks to amend the *Telecommunications Act 1997* (Telecommunications Act) to grant certain persons with the power to give a 'designated communications provider'[1] (provider) technical assistance notices, technical assistance requests, and technical capability notices, for the purposes of assisting law enforcement and intelligence agencies with performing certain functions and discharging certain powers relevant to crime, national security, and other objectives.

Technical assistance notice

1.83 Section 317L provides that the Director-General of Security (who leads the Australian Security Intelligence Organisation, ASIO) or the chief officer of an

1 Proposed section 317C in Schedule 1 of the bill defines 'designated communications providers' by reference to 15 circumstances in which a person is a designated communications provider.

'interception agency'[2] may give a provider a notice that requires the provider to do one or more specified 'acts or things' in connection with any or all of the 'eligible activities'[3] of the provider (technical assistance notice). Prior to giving the notice, the Director-General or chief officer giving the notice must be satisfied that doing so is reasonable, proportionate, practicable and technically feasible.[4] The 'act or thing' specified in the technical assistance notice must be by way of giving help to either ASIO or the interception agency in relation to the performance of a function or the exercise of a power relevant to the objectives of: enforcing the criminal law and laws imposing pecuniary penalties, or assisting the enforcement of the criminal laws in a foreign country, or safeguarding national security.[5]

Technical capability notice

1.84 Section 317T gives the Attorney-General the power to issue a 'technical capability notice' requiring a provider to do an 'act or thing' which must be directed towards ensuring that the provider is capable of giving 'listed help', or be by way of giving help, to ASIO or an interception agency, in relation to performance of a function or exercise of a power insofar as it relates to a 'relevant objective'. 'Relevant objective' means enforcing the criminal law and laws imposing pecuniary penalties, or assisting the enforcement of the criminal laws in a foreign country, or safeguarding national security. Help will constitute 'listed help' if it consists of a listed act or thing, or one or more acts or things of a kind determined by legislative instrument.[6]

Technical assistance request

1.85 Section 317G of the bill provides for the giving of 'technical assistance requests', which operate similarly to technical assistance notices and technical capability notices, except that compliance with a technical assistance request is

2 Proposed section 317B in Schedule 1 of the bill defines 'interception agency' to mean the Australian Federal Police; the Australian Commission for Law Enforcement Integrity; the Australian Crime Commission; the Police Force of a State or the Northern Territory; the Independent Commission Against Corruption of New South Wales; the New South Wales Crime Commission; the Law Enforcement Conduct Commission of New South Wales; the Independent Broad-based Anti-corruption Commission of Victoria; the Crime and Corruption Commission of Queensland; the Independent Commissioner Against Corruption (SA); or the Corruption and Crime Commission (WA).

3 Proposed section 317C defines 'eligible activities' in broad terms, by reference to 15 types of eligible activities.

4 Proposed section 317P in Schedule 1 of the bill.

5 Proposed section 317L(2) in Schedule 1 of the bill.

6 See proposed section 317T(4) in Schedule 1 of the bill.

voluntary.[7] A provider that decides to comply with the request is not subject to civil liability in relation to an 'act or thing' done in accordance with the technical assistance request, or in good faith purportedly with the request.[8] In addition, the Director-General of the Australian Secret Intelligence Service (ASIS) and the Director-General of the Australian Signals Directorate (ASD) may also make a technical assistance request, as well as ASIO and interception agencies. Further, the 'act or thing' specified in the technical assistance request may 'be directed towards ensuring that the designated communications provider is capable of giving help' to ASIO, ASD, ASIS or the interception agency. In addition to seeking assistance in relation to the functions performed or powers exercised for enforcing criminal laws, imposing pecuniary penalties and assisting the enforcement of foreign criminal laws, technical assistance requests can also be made to procure assistance with functions performed or powers exercised in relation to 'the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being'.[9]

Listed acts or things

1.86 The 'acts or things' that may be specified in a technical assistance notice, technical capability notice or technical assistance request include, but are not limited to, 'listed acts or things'.[10] Listed acts or things include, for example:

- removing one or more forms of electronic protection;[11]
- installing, maintaining, testing or using software or equipment;[12]
- ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format;[13]
- facilitating access to customer equipment, software or a service;[14] and
- assisting with the testing, modification, development or maintenance of a technology or capability.[15]

---

7 There is also a requirement in the bill that the relevant Director-General or chief officer of an intelligence agency advise the recipient of a technical assistance request that compliance is voluntary: see proposed section 317HAA in Schedule 1 of the bill.

8 Proposed section 317G(1) in Schedule 1 of the bill.

9 Proposed section 317G(5)(c) in Schedule 1 of the bill.

10 Proposed sections 317L(3), 317T(4), 317T(7), and 317G(6) in Schedule 1 of the bill.

11 Proposed section 317E(1)(a) in Schedule 1 of the bill.

12 Proposed section 317E(1)(c) in Schedule 1 of the bill.

13 Proposed section 317E(1)(d) in Schedule 1 of the bill.

14 Proposed section 317E(1)(e) in Schedule 1 of the bill.

15 Proposed section 317E(1)(f) in Schedule 1 of the bill.

1.87 It also includes an act or thing done to conceal the fact that any thing has been done covertly.[16]

Limitations on technical assistance notices and technical capability notices

1.88 The bill also provides that a technical assistance notice or technical capability notice must not have the effect of requiring a provider to implement or build a systemic weakness or a systemic vulnerability into a form of electronic protection, or prevent a provider from rectifying such a weakness or vulnerability.[17] This includes implementing or building a new decryption capability in relation to a form of electronic protection, or one or more actions that would render systemic methods of authentication or encryption less effective.[18]

1.89 Further, the bill provides that technical assistance notices and technical capability notices have no effect to the extent that they would require a provider to do a thing for which a warrant or authorisation under the *Telecommunications (Interception and Access) Act 1979* (TIA Act), the *Surveillance Devices Act 2004* (SD Act), the *Crimes Act 1914* (Crimes Act), the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), the *Intelligence Services Act 2001* (IS Act) or equivalent State and Territory laws would be required.[19]

Compatibility of the measures with multiple rights

1.90 As acknowledged in the statement of compatibility, the technical assistance notices and requests and technical capability notices engage and may limit a number of human rights including the right to privacy, the right to freedom of expression, and the right to an effective remedy. Each of these rights is discussed further below.

Compatibility of the measures with the rights to privacy and freedom of expression

1.91 The statement of compatibility identifies that the measures engage the rights to privacy and freedom of expression, but states that they represent permissible limitations on those rights.[20]

1.92 The right to privacy protects against arbitrary and unlawful interference with an individual's privacy, and includes the right to respect for private and confidential information, particularly the storing, use and sharing of such information and the right to control the dissemination of information about one's private life. As noted in the statement of compatibility, the measures engage the right to privacy because, as a consequence of such notices, 'communications providers may facilitate law

16 Proposed section 317E(1)(j) in Schedule 1 of the bill.

17 Proposed section 317ZG(1) in Schedule 1 of the bill.

18 Proposed section 317ZG(2) and (3) in Schedule 1 of the bill.

19 Proposed section 317ZH in Schedule 1 of the bill.

20 Statement of compatibility (SOC), pp. 9-14.

enforcement, security and intelligence agencies' access to private communications and data where an underlying warrant or authorisation is present'.[21]

1.93 The right to freedom of expression in article 19(2) of the International Covenant on Civil and Political Rights (ICCPR) includes the freedom to seek, receive and impart information and ideas of all kinds, either orally, in writing or print, in the form of art, or through any other media of an individual's choice. As acknowledged in the statement of compatibility, the measures may engage the right to freedom of expression 'by indirectly making some people more reluctant to use communications services' because:

> It is plausible that a person may minimise their use of communications services if they believe government agencies can ask providers to facilitate access to communications carried through these service, for example by removing forms of electronic protection applied to their communications if they are capable of doing so.[22]

1.94 The right to freedom of expression, as the statement of compatibility identifies,[23] may only be subject to restrictions provided by law that are necessary for the protection of national security or of public order or of public health or morals. The right to privacy may be subject to permissible limitations which are provided by law and are not arbitrary. That is, for each of these rights, the measures must pursue a legitimate objective and be rationally connected and proportionate to achieving that objective.

Legitimate objective

1.95 The statement of compatibility states that 'the bill pursues the legitimate objective of protecting national security and public order by addressing crime and terrorism',[24] specifically referring to 'terrorism, espionage, acts of foreign interference and serious and organised crime'.[25]

1.96 In general terms, protecting national security and public order is capable of constituting a legitimate objective for the purposes of international human rights law. However, a measure will only pursue a legitimate objective (capable of justifying a proposed limitation on human rights) where there is a reasoned and evidence-based explanation of why the measure addresses a pressing or substantial concern, and does not simply seek an outcome which is convenient or desirable. The statement of compatibility does not identify a pressing and substantial concern to be addressed by the relevant measures. However, the explanatory memorandum

21 SOC, p. 9 [8].

22 SOC, p. 14 [40].

23 SOC, p. 14 [39].

24 SOC, p. 11 [16].

25 SOC, p. 11 [21].

indicates that the measures are directed towards addressing the 'challenges associated with encrypted communications', explaining that:

> Secure, encrypted communications are increasingly being used by terrorist groups and organised criminals to avoid detection and disruption. Over 90% of telecommunications information being lawfully intercepted by the Australian Federal Police now uses some form of encryption…
>
> The increasing use of encryption has significantly degraded law enforcement and intelligence agencies' ability to access communications and collect intelligence, conduct investigations into organised crime, terrorism, smuggling, sexual exploitation of children and other crimes, and detect intrusions into Australian computer networks.[26]

1.97 The committee's usual expectation is that this information would be included in the statement of compatibility to enable assessment of whether the measures pursue a legitimate objective.[27] However, even taking this information into account, further information is required to establish a pressing and substantial concern for the purposes of international human rights law. For example, it is not clear from the information provided why the measures are necessary, as opposed to desirable or convenient, to address the majority of information legally intercepted by ASIO being encrypted. It is also not clear whether the aspects of the measures that do not appear on their face to relate to decryption address a pressing or substantial concern.

1.98 Further, as noted in the statement of compatibility, 'national security' and 'public order' represent permissible grounds on which the right to freedom of expression may be restricted.[28] However, there are questions as to whether aspects of technical assistance requests restrict the right on these grounds, insofar as a request may be given in relation to the objective of 'the interest of Australia's foreign relations or Australia's economic well-being'.[29] These grounds are broader than those on which the right to freedom of expression can be validly restricted, and the statement of compatibility does not address if they are relevant to a valid ground. Further information from the minister as to how the power to request technical assistance in relation to the performance of functions or exercise of powers in relation to the interest of Australia's foreign relations or economic well-being relates to a permissible ground on which the right to freedom of expression can be

---

26 Explanatory memorandum (EM), p. 2 [3]-[4].

27 In accordance with the committee's *Guidance Note 1,* the committee's expectation is that statements of compatibility read as stand-alone documents, as the committee relies on the statement as the primary document that sets out the legislation proponent's analysis of the compatibility of the bill with Australia's international human rights obligations.

28 SOC, p. 14 [43], see also ICCPR article 19(3).

29 Proposed section 317G(5) in Schedule 1 of the bill.

restricted would assist with this analysis. This would also assist in determining whether this aspect of the measure is rationally connected to its objective.

Rational connection

Power to give technical assistance notices or requests, or technical capability notices

1.99 Empowering ASIO to obtain technical assistance in relation to the performance of its functions or exercise of powers related to safeguarding national security or crime appears to be rationally connected to the objectives of the bill. So, too, does granting such powers to some interception agencies such as the Australian Federal Police. However, the definition of 'interception agency' is very broad and includes state-based anti-corruption agencies. It is not clear how empowering these agencies, which do not appear to discharge functions relevant to safeguarding national security and addressing the type of crime contemplated in the statement of compatibility,[30] is effective to achieve the objectives of the bill (namely, protecting national security and public order). The statement of compatibility does not explicitly address this issue. Further information from the minister – namely, how granting each of the agencies that fall within the definition of 'interception agency' the power to give technical assistance notices or requests, or technical capability notices, is effective to achieve the objectives of the bill – would assist in assessing whether the measures are rationally connected to a legitimate objective.

'Acts or things' compelled by a technical assistance notice or technical capability notice, or requested by a technical assistance request

1.100 A question arises as to whether all of the 'acts or things' that may be specified in a technical assistance notice or request, or technical capability notices, are rationally connected to the stated objectives of the measures. The statement of compatibility provides an example, that 'a technical assistance notice may ask a provider to decrypt information that would otherwise be unintelligible if the provider has the ability to do so'.[31] This appears to be rationally connected with the objectives of protecting national security and public order in circumstances where 'encryption is increasingly being used by terrorist groups and organised criminals'.[32] Other 'listed acts or things', such as ensuring information obtained in connection

30 For example, section 2A of the *Independent Commission against Corruption Act 1988* (NSW) (Act), provides that the principal objects of the Act are 'to promote the integrity and accountability of public administration by constituting an Independent Commission Against Corruption as an independent and accountable body… to investigate, expose and prevent corruption involving or affecting public authorities and public officials'. Section 13 of the Act sets out the principal functions of the Commission, which are numerous but largely all relate to investigating and preventing 'corrupt conduct'.

31 SOC, p. 10 [15].

32 EM, p. 2 [3].

with a warrant is given in a particular format,[33] also would appear to be an effective means to achieve the objectives of the bill.

1.101 However, the statement of compatibility otherwise does not specifically address how each of the listed acts or things a provider may be required to do in compliance with a technical assistance notice or request, or technical capability notice, is rationally connected to the objectives of the bill. It is not clear, for example, how modifying a service provided by a provider,[34] or requiring a provider to install software,[35] would be effective to achieve the objectives of protecting national security and public order by addressing crime and terrorism. In relation to technical capability notices, the statement of compatibility states that capabilities built as a result of acts or things done pursuant to a technical capability notice 'may' assist agencies to access private communications for investigative purposes,[36] but does not elaborate as to how. Further information from the minister as to how each of the listed acts or things are rationally connected with the stated objectives of the bill would assist for the purposes of this analysis.

1.102 Further, the 'acts or things' that a provider can be compelled or requested to do is not limited to 'listed acts or things'.[37] As the list of acts or things that can be compelled or requested is non-exhaustive, it is difficult to assess whether the measures as a whole are rationally connected with the objectives of the bill. Further information from the minister as to how requesting or compelling a provider to do any act or thing beyond the 'listed acts or things' in the bill is effective to achieve the objectives of the measures would assist with this analysis.

Proportionality

Power to give technical assistance notices or requests, or technical capability notices

1.103 As to proportionality, measures that restrict the right to privacy and freedom of expression must be no more extensive than is strictly necessary to achieve their stated objective. While the statement of compatibility addresses the features of the measures and relevant safeguards, it does not explain why existing powers available under the warrant and authorisation scheme are insufficient to address the stated objectives, and therefore why the measures are strictly necessary. Nor does it consider whether the measures represent the least rights restrictive approach, compared with, for example, amending the relevant warrant and authorisation regimes.

---

33 Proposed section 317E(d) in Schedule 1 of the bill.

34 Proposed section 317E(h) in Schedule 1 of the bill.

35 Proposed section 317E(c) in Schedule 1 of the bill.

36 SOC, p. 12 [27].

37 Proposed section 317L(3) in Schedule 1 of the bill.

1.104 While the stated objective of the measures is 'protecting national security and public order by addressing crime and terrorism',[38] the proposed power to give technical assistance notices or requests, or technical capability notices, is not limited in this way and may be broader in scope. Specifically, the statement of compatibility does not explain why it is necessary for the purposes of safeguarding national security and addressing crime to seek assistance from providers in relation to 'enforcing laws that attract a pecuniary penalty' or, in relation to technical assistance requests, 'the interests of Australia's foreign relations or the interests of Australia's national economic well-being'.[39] The terms 'foreign relations' and 'national economic well-being' are not defined in the bill, and could apply to a broad range of conduct not necessarily involving crime and terrorism. This raises concerns that the measures as framed may be overly broad with respect to its stated objectives.

1.105 The power to give a technical assistance notice or request is restricted to senior executive staff in all agencies,[40] and the power to give a technical capability notice is restricted to the Attorney-General.[41] The statement of compatibility concludes that 'accordingly, requests will only be issued by persons with the appropriate seniority and expertise who are in a position to effectively determine the proportionality, reasonableness, practicability and technical feasibility of any request'.[42] In relation to technical assistance notices and technical capability notices, this may be a relevant safeguard for the purposes of proportionality in terms of ensuring that the power is exercised in a way that is not arbitrary.

1.106 However, there are questions as to whether this is a relevant safeguard in relation to technical assistance notice, the giving of which does not require the Director-General or chief officer of an interception agency to determine that it is proportionate, reasonable, practicable or technically feasible. Given that technical assistance requests, if fulfilled by a provider, would appear to impact rights in the same way as technical assistance notices and technical capability notices, further information from the minister as to safeguards relevant to the decision to issue technical assistance requests that prevent the power from being exercised arbitrarily would be useful for the purposes of this analysis.

1.107 In relation to safeguards to prevent the arbitrary exercise of the power to issue technical capability notices, the statement of compatibility states that 'prior to a notice being issued, there is a mandatory 28 day consultation period with the relevant provider' and that 'this will ensure that the powers are not exercised

38 SOC, p. 12 [16].

39 Proposed section 317G(5)(c) in Schedule 1 of the bill.

40 SOC, p. 11 [19].

41 Proposed section 317T in Schedule 1 of the bill.

42 SOC, p. 11 [19].

arbitrarily'.[43] However, there are questions as to whether the mandatory 28 day consultation period would function as a safeguard to prevent the power from being exercised arbitrarily for the purposes of human rights law. This is because it appears that the Attorney-General is not required to take into account any concerns raised by the relevant provider, and in any event those concerns may not necessarily be relevant to the impact a technical capability notice may have on human rights.

1.108 Also relevant to proportionality is the extent to which the measure interferes with other rights. In this respect, concerns arise from the extent to which the measures can be used to obtain assistance from a provider with the enforcement of criminal laws in force in a foreign country.[44] The committee has previously raised concerns regarding the human rights implications of Australia's mutual legal assistance scheme.[45] These concerns are relevant to the bill insofar as any requests for assistance from foreign countries would be governed by Australia's mutual legal assistance scheme. Further discussion of the interactions between the bill and the mutual legal assistance scheme are discussed further below at [1.202]-[1.203].

1.109 Another relevant factor in assessing whether a measure is proportionate is whether there is the possibility of oversight and the availability of review.[46] The power to give a technical assistance notice or request, or technical capability notice, is not exercised by a judge, nor does a judge supervise its application. Section 317ZFA provides a discretionary power to a court, in relation to proceedings before it, to make such orders as the court considers appropriate in relation to the disclosure, protection, storage, handling or destruction of technical assistance information, if the court is satisfied that it is in the public interest. The bill does not otherwise provide for court involvement in the process of giving a technical assistance notice or request, or technical capability notice. The bill additionally seeks to amend the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act) to exclude decisions under Part 15 of the Telecommunications Act (which would include a decision to issue a technical assistance notice or request, or technical capability notice) from judicial review under the ADJR Act.[47] In these circumstances, further information from the minister as the adequacy of the safeguards in terms of

43 SOC, p. 13 [32].

44 See proposed section 317L(2)(c)(ii) in Schedule 1 of the bill.

45 See, for example, Parliamentary Joint Committee on Human Rights, *Report 2 of 2017*, (21 March 2017) pp. 3-9; *Report 4 of 2017* (9 May 2017) pp. 70-73 and 90-98; *Twenty-second report of the 44th Parliament* (13 May 2015), pp. 108-110; *Sixth report of 2013* (15 May 2013), pp. 149-167; *Tenth Report of 2013* (26 June 2013), pp. 56-75.

46 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (addressing the use of encryption and anonymity in digital communications), 30 January 2018, A/HRC/29/32, 11 [32].

47 Proposed section 1 in Schedule 1 of the bill.

oversight and review would assist in determining the proportionality of the measures.

'Acts or things' compelled by a technical assistance notice or technical capability notice, or requested by a technical assistance request

1.110 There are also concerns as to the proportionality of the measures as they relate to the 'acts or things' the providers would be compelled to do in compliance with a technical assistance notice or technical capability notice, or could agree to do in relation to a technical assistance request. In this respect, the statement of compatibility indicates that the limitation on human rights 'would not be arbitrary because a technical assistance request or notice may only be issued for a specified list of acts or things'.[48] However, the language of the bill is broader, such that the acts or things that may be specified in a technical assistance notice or request 'include (but are not limited to) listed acts or things', and for the purposes of a technical capability notice, 'listed help' may also include acts or things determined by the minister in a legislative instrument.[49]

1.111 In terms of safeguards relating to the disclosure of private information, it is relevant that section 317ZH provides that 'a provider cannot be asked to provide the content of a communication or private telecommunications data… without an existing warrant or authorisation' under the TIA Act, SD Act, Crimes Act, ASIO Act, the IS Act and their state and territory equivalents,[50] and that there is an express prohibition in section 317ZG on compelling a provider to implement or build a systemic weakness or vulnerability into a form of electronic protection,[51] also known as a 'back door'.[52] However, these safeguards appear to apply only to technical assistance notices and technical capability notices, and not technical assistance requests.[53] There is also a question as to whether variations to technical assistance notices or technical capability notices would be subject to this safeguard. To assess the proportionality of these measures, further information from the minister is required as to whether a technical assistance request (or variation to a technical assistance notice or technical capability notice) could be used to request or compel information to be provided for which a warrant would ordinarily be required, or to request or compel a provider to build a 'back door'.

1.112 In relation to whether section 317ZH provides a safeguard to protect the disclosure of personal information, the section states that a notice has 'no effect' to

48 SOC, p. 10 [11].

49 Proposed section 317T(4)(c)(ii) and (5) in Schedule 1 of the bill.

50 SOC, p. 10 [12]; see proposed section 317ZH in Schedule 1 of the bill.

51 Proposed sections 317ZG in Schedule 1 of the bill.

52 SOC, p. 11 [20].

53 Proposed sections 317ZG and 317ZH in Schedule 1 of the bill.

the extent it seeks to compel a provider to do an act or thing for which a warrant would be required. While sections 317P and 317V prevent a relevant decision maker from issuing a notice unless satisfied of certain things (namely that the requirements it sets are reasonable and proportionate, and compliance with the notice is practicable and technically feasible),[54] it appears that a decision maker can still issue a notice even if it seek to compel a provider to do an act or thing for which a warrant would be required. It therefore appears that it would be for the provider receiving the notice to determine if the relevant notice seeks to compel the provider do an act or thing for which a warrant is required. There are questions as to how a provider, especially smaller or unsophisticated providers, are expected to know whether or not what has been requested or compelled requires a warrant, and therefore how to respond accordingly. Further information is required as to how this will operate as a relevant safeguard, including whether it would be possible to amend the decision-making criteria to state that a notice must not be issued unless the decision-maker is satisfied it does not seek to compel a provider to do an act or thing for which a warrant is required.

1.113 In any case, whether a warrant or authorisation scheme will function as an effective safeguard turns upon the extent to which the warrant and authorisation scheme constitutes a proportionate limitation on the right to privacy. In relation to the warrant or authorisation powers under the TIA Act, as that Act was legislated prior to the establishment of the committee, the scheme has never been required to be subject to a foundational human rights compatibility assessment in accordance with the terms of the *Human Rights (Parliamentary Scrutiny) Act 2011.*[55] It is therefore difficult to assess whether the warrant or authorisation scheme in the TIA Act would operate as a sufficient safeguard. The same concern arises in relation to the warrant and authorisation scheme under the SD Act.

---

54 See also sections 317RA and 317ZAA, which set out whether requirements imposed by a notice are reasonable and proportionate.

55 The committee has considered proposed amendments to the TIA Act on a number of previous occasions: See, Parliamentary Joint Committee on Human Rights, Law Enforcement Integrity Legislation Amendment Bill 2012, *Fifth Report of 2012* (October 2012) pp. 21-21; Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *Fifteenth Report of the 44th Parliament* (14 November 2014) pp. 10-22; *Twentieth report of the 44th Parliament* (18 March 2015) pp. 39-74; and *Thirtieth report of the 44th Parliament* (10 November 2015) pp. 133-139; the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015, *Thirty-second report of the 44th Parliament* (1 December 2015) pp. 3-37 and *Thirty-sixth report of the 44th Parliament* (16 March 2016) pp. 85-136; the Law Enforcement Legislation Amendment (State Bodies and Other Measures) Bill 2016, *Report 9 of 2016* (22 November 2016) pp. 2-8 and *Report 1 of 2017* (16 February 2017) pp. 35-44; and the Telecommunications (Interception and Access – Law Enforcement Conduct Commission of New South Wales) Declaration 2017 [F2017L00533], *Report 7 of 2017* (8 August 2017) pp. 30-33.

1.114 The committee has previously noted in relation to the TIA Act, however, that while the warrant regime may assist to ensure that access to private communications is sufficiently circumscribed, questions arise as to the proportionality of the broad access that may be granted in relation to 'services' or 'devices' under the relevant chapters of the TIA Act.[56] This would be particularly relevant in the context of this bill given the broad scope of 'acts or things' that may be done to 'services' or 'devices' pursuant to a technical assistance notice. Further information from the minister in relation to the human rights compatibility of the warrant and authorisation scheme of the TIA Act insofar as it interacts with the bill would assist the human rights assessment of the proposed measures.

1.115 In relation to the warrant or authorisation powers under other legislative schemes referred to in the statement of compatibility, there are also questions as to the extent to which the enabling legislation of 'interception agencies', such as state-based commissions charged with investigating corruption and misconduct, functions as a sufficient safeguard, given the broad investigative powers afforded to such bodies. Such investigative powers are exercised pursuant to warrant and authorisation regimes which may operate without judicial oversight.[57]

1.116 Further, while section 317ZG is intended to operate to prevent notices from being used to compel providers to implement or build systemic weaknesses or vulnerabilities, there are questions as to whether this functions as a sufficient safeguard for the purposes of international human rights law. The bill itself does not define systemic weakness or vulnerability and therefore appears to leave this determination to the person that gives the notice. In this respect the statement of compatibility provides that:

> While systemic weaknesses cannot be built into services or devices, a technical assistance notice can require the selective deployment of a weaknesses [sic] or vulnerability in a particular service, device or software on a case-by-case basis. Deployment of this kind is necessary to access protected information of suspect individuals and gather intelligence or evidence in the course of an investigation. This will ensure that the powers achieve legitimate, national security and law enforcement objectives without unduly jeopardising the legitimate privacy and information security interests of innocent parties.[58]

---

56 See Parliamentary Joint Committee on Human Rights, *Report 9 of 2016* (22 November 2016) p. 5; *Report 1 of 2017* (16 February 2017) pp. 35-44.

57 See, for example, the investigative powers conferred on the NSW Independent Commission Against Corruption by the *Independent Commission Against Corruption Act 1988* (NSW): section 21 (power to obtain information); section 22 (power to obtain documents etc.); section 23 (power to enter public premises); section 40(2)-(3) (search warrants).

58 SOC, p. 11 [20].

1.117 The statement of compatibility does not elaborate as to how weaknesses or vulnerabilities in a particular service, device or software can be 'selectively deployed' in a way that is limited to matters in relation to individuals under investigation, and in a manner that will not unnecessarily intrude into the private life of the person under investigation or third persons. This raises concerns under international human rights law in circumstances where it has been observed that the exploitation of a weakness or vulnerability in encryption may weaken security systems more generally.[59] Further information from the minister as to how the scheme will be limited to avoid broader effects on the users of a provider's service or device would assist with the analysis of the proportionality of the measure.

Committee comment

1.118 The preceding analysis raises questions about the compatibility of technical assistance notices, technical capability notices and technical assistance requests with the rights to privacy and freedom of expression.

1.119 The committee therefore seeks the advice of the minister as to the compatibility of the measures with these rights, including:

- **an explanation of the pressing and substantial concern that gives rise to the need for the measures (including how aspects of the measures that do not on their face relate to decryption are directed towards addressing the stated objective of the measures);**
- **whether the power to give a technical assistance request in relation to 'the interests of Australia's foreign relations or the interests of Australia's national economic well-being', relates to a permissible ground on which the right to freedom of expression can be restricted;**
- **whether granting each of the agencies that fall within the definition of 'interception agency' the power to give technical assistance notices or requests is rationally connected to (that is, effective to achieve) the stated objectives of the measures;**
- **whether each of the listed acts or things specified in proposed section 317E is rationally connected to (that is, effective to achieve) the stated objectives of the measures;**
- **whether the measures are proportionate to the stated objectives, including:**
    - **why the current warrant and authorisation schemes are insufficient to address the stated objectives of the bill, and whether the measures**

59 See for example, Office of the Australian Information Commissioner, *Submission to the Department of Home Affairs on the consultation draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (12 September 2018) pp. 5-6.

therefore represent the least rights restrictive approach to addressing the objectives of the bill;

- **safeguards relevant to the decision to issue technical assistance requests;**
- **safeguards in terms of oversight and review of the measures and whether these are adequate for the purposes of ensuring the proportionality of the measures;**
- **the human rights compatibility of the warrant and authorisation scheme of the *Telecommunications (Interception and Access) Act 1979* insofar as it interacts with the measures;**
- **the adequacy of the safeguards to ensure that notices and requests will not be used to obtain personal information for which a warrant would be required (including whether it would be possible to amend the decision-making criteria to state that a notice must not be issued unless the decision-maker is satisfied it does not seek to compel a provider to do an act or thing for which a warrant is required);**
- **whether a technical assistance request could be used to request a provider to do a thing for which a warrant or authorisation under the *Telecommunications (Interception and Access) Act 1979*, the *Surveillance Devices Act 2004*, the *Crimes Act 1914*, the *Australian Security Intelligence Organisation Act 1979*, the *Intelligence Services Act 2001* or equivalent State and Territory laws would be required, and if so, the relevant safeguards that would apply;**
- **whether a technical assistance request could be used to request or compel a provider to implement or build a systemic weakness or vulnerability, and if so, the relevant safeguards that would apply;**
- **whether it would be feasible to amend sections 317ZG and 317ZH to also apply to technical assistance requests, and to expressly refer to variations to technical assistance notices and technical capability notices;**
- **whether it would be feasible to define 'systemic vulnerability' and 'systemic weakness', and if not, whether the scheme will be sufficiently circumscribed so as to avoid broader effects on the users of a provider's service or device; and**
- **any other information relevant to determining the proportionality of compatibility of the measures with the rights to privacy and expression.**

Compatibility of the measures with the right to an effective remedy

1.120 Article 2(3) of the ICCPR protects the right to an effective remedy for any violation of rights and freedoms recognised by the ICCPR, including the right to have such a remedy determined by competent judicial, administrative or legislative authorities or by any other competent authority provided for by the legal system of the state. While limitations may be placed in particular circumstances on the nature of the remedy provided (judicial or otherwise), state parties must comply with the fundamental obligation to provide a remedy that is effective.[60]

1.121 The statement of compatibility acknowledges that the bill may engage the right to an effective remedy insofar as an individual's rights are infringed by compliance with a notice, because the bill does not provide for merits review of decision making and excludes judicial review under the ADJR Act.[61] The statement of compatibility suggests, however, that individuals will still be entitled to an effective remedy as Australian courts will retain jurisdiction for judicial review of a decision of an agency head to issue a technical assistance notice or the Attorney-General's decision to issue a technical capability notice (presumably by way of prerogative writ).[62] However, it is not clear how a natural person could pursue judicial review of a decision to issue a technical assistance notice or technical capability notice in circumstances where they may not be aware that a notice has been issued.[63] Further information from the minister as to how this ensures the right to an effective remedy would assist with this analysis.

1.122 Technical assistance requests also engage the right to an effective remedy because they provide immunity from civil liability for any act or thing done by a provider in compliance with a technical assistance request. If the act or thing involves a breach of human rights, this could raise concerns about the availability of an effective remedy for victims in these circumstances. However, the statement of compatibility does not address the right to an effective remedy in relation to technical assistance requests and accordingly no assessment was provided as to the compatibility of this measure with this right.

Committee comment

1.123 The preceding analysis raises questions as to the compatibility of technical assistance notices, technical capability notices and technical assistance requests

60 See UN Human Rights Committee, *General Comment No.29: States of Emergency (Article 4)* (2001) [14].

61 SOC, p. 14 [44].

62 SOC, p. 14 [45].

63 Division 6 of Schedule 1 of the bill imposes criminal penalties for the disclosure of information that is technical assistance notice information, technical capability notice information, technical assistance request information, or obtained in accordance with such orders or requests.

with the right to an effective remedy. In relation to technical assistance notices and technical compatibility notices, this was not fully addressed in the statement of compatibility. In relation to technical assistance requests, this was not addressed at all in the statement of compatibility.

1.124 The committee therefore seeks the advice of the minister as to the compatibility of the measures with this right.

Computer access warrant scheme in the Surveillance Devices Act

1.125 The SD Act currently governs the use of optical surveillance devices, listening devices, data surveillance devices and tracking devices by law enforcement agencies. Schedule 2 of the bill introduces a computer access warrant scheme into the SD Act, as well as several related and additional orders and authorisations relating to accessing data held on computers. A computer access warrant enables officers to search a computer[64] remotely or physically and access content on that computer.[65]

Computer access warrants

1.126 Proposed section 27A provides that computer access warrants can be sought in a number of different circumstances, including:

- in relation to investigations into the commission of 'relevant offences'[66] or where there has been a 'mutual assistance authorisation'[67] where the law enforcement officer suspects on reasonable grounds that access to data[68] held in a computer[69] (the 'target computer')[70] is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the

64 Computer is defined in proposed section 6(1) of the SD Act in Schedule 2 of the bill to mean 'all or part of (a) one or more computers; or (b) one or more computer systems; (c) one or more computer networks; or (d) any combination of the above'.

65 There are additional human rights issues raised in relation to the power to access computers remotely discussed below in relation to measures introduced in Schedules 3 and 4.

66 'Relevant offence' is defined broadly in section 6 of the SD Act, and includes an offence against the law of the Commonwealth that is punishable by a maximum term of imprisonment of 3 years or more or for life.

67 A mutual assistance authorisation means an authorisation under subsection 15CA(1) of the MA Act. For the proposed amendments to the MA Act, see further below.

68 Data is defined in proposed section 6(1) of the SD Act in Schedule 2 of the bill to include information in any form; and any program (or part of a program).

69 'Data held in a computer' is defined in proposed section 6(1) of the SD Act in Schedule 2 of the bill to include (a) data held in any removable data storage device for the time being held in a computer; and (b) data held in a data storage device on a computer network of which the computer forms a part.

70 'target computer' may be a particular computer, a computer on particular premises, or a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known): see proposed section 27A(15) of the SD Act in Schedule 2 of the bill.

commission of the relevant offences, or the identity or location of the relevant offenders;

- where a recovery order[71] is in force and where the law enforcement officer suspects on reasonable grounds that access to data held in a target computer may assist in the location and safe recovery of the child to whom the recovery order relates;
- where an 'integrity authority'[72] is in effect authorising an integrity operation in relation to an offence committed by a staff member of a target agency and the officer suspects on reasonable grounds that access to data held in a target computer will assist the conduct of the integrity operation in specified ways; and
- where a 'control order' is in force in relation to a person and the officer suspects on reasonable grounds that access to data held in a target computer to obtain information relating to the person would be likely to substantially assist in specified matters, including determining whether the control order or any succeeding control order has been or is being complied with.

1.127 Proposed section 27C provides that a computer access warrant is issued by an eligible Judge or a nominated AAT member (decision maker).[73] To issue a computer access warrant, the decision maker must be satisfied of various matters including that there are reasonable grounds for the suspicion founding the application for a warrant. The decision maker must also 'have regard to' various other matters including the nature and gravity of the alleged offence (where applicable), the extent to which the privacy of any person is likely to be affected, the existence of any alternative means of obtaining the evidence or information sought to be obtained, and the likely evidentiary or intelligence value of evidence or information obtained.

1.128 A computer access warrant authorises specified things to be done in relation to a target computer that the decision maker considers appropriate in the circumstances, including:

- entering premises;
- using the target computer for the purpose of obtaining access to data held on the target computer in order to determine whether the relevant data is covered by the warrant;

---

71 A recovery order means an order under section 67U of the *Family Law Act 1975* or an order for the apprehension or detention of a child under the *Family Law (Child Abduction Convention) Regulations 1986*.

72 'Integrity authority' is defined in section 6 of the SD Act.

73 'Eligible Judge' and 'nominated AAT member' are defined in section 12 of the SD Act.

- adding, copying, deleting or altering other data in the target computer for certain purposes;
- using any other computer to access the relevant data (if, having regard to other methods of obtaining access to the relevant data which are likely to be as effective, it is reasonable to do so);
- removing a computer or other thing from premises to do any thing specified in the warrant;
- intercepting a communication passing over a telecommunications system, if the interception is for the purpose of doing any thing specified in the warrant;[74] and
- any other thing reasonably incidental to any of the above.[75]

1.129 There are also concealment of access powers[76] and provisions which compel persons to provide assistance to law enforcement to allow the officer to access data,[77] discussed in further detail below.

1.130 In addition to these matters, the computer access warrant must authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant.[78] Orders can also be made that a person not be required to disclose information in proceedings that would reveal details of computer access technologies or methods in certain circumstances.[79]

Additional measures in relation to computer access warrants for control orders

1.131 Proposed section 65A(2) in Schedule 2 of the bill provides that a person is not criminally liable for any actions done under a control order access warrant issued on the basis of an interim control order where the interim control order is subsequently declared to be void. Further, if a court declares an interim order is void, any information obtained under the control order access warrant can be used, communicated or published if the person reasonably believes that doing so is necessary for preventing or reducing the risk of the commission of a terrorist act or serious harm to a person or property, or if the person does so for certain purposes including in relation to a matter arising under a preventative detention order.[80]

---

74 This interception power is similar to that introduced into the ASIO Act in Schedule 2 of the bill and is discussed further below.

75 See proposed section 27E(2) of the SD Act in Schedule 2 of the bill.

76 See proposed section 27E(7) of the SD Act in Schedule 2 of the bill.

77 See proposed sections 64A((2),(3),(4),(5),(6) and(7) of Schedule 2 of the bill.

78 See proposed section 27E(6) of the SD Act in Schedule 2 of the bill.

79 See proposed section 47A of the SD Act in Schedule 2 of the bill.

80 See proposed section 65B(1)(a)(ia) of the SD Act in Schedule 2 of the bill, and section 65B of the SD Act.

Emergency authorisation for access to data held in a computer

1.132 Additionally, the bill seeks to amend the SD Act to provide that a law enforcement officer may apply to an 'appropriate authorising officer'[81] for an emergency authorisation for access to data held in a target computer[82] in certain circumstances where the matters are of such urgency that access to data held in the target computer is necessary, and it is not practicable in the circumstances to apply for a computer access warrant.[83] The appropriate authorising officer may give the emergency authorisation if satisfied of certain matters, including that there are reasonable grounds for the suspicion founding the application.[84]

1.133 Within 48 hours after giving an emergency authorisation, the person who gave the authorisation must apply to an eligible Judge or nominated AAT member for approval of the giving of the emergency authorisation. The Judge or eligible AAT member may give the approval if satisfied of certain matters.[85] In making this decision, the decision-maker considering the application must, in particular, and 'being mindful of the intrusive nature of accessing data held in a target computer',[86] consider several factors. These factors include the nature of the risk which provided the basis for the emergency authorisation, the extent to which issuing a computer access warrant would have helped reduce or avoid the risk, and the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk.[87]

Compatibility of the measures with the right to privacy

1.134 The measures in the new computer access warrant scheme in the SD Act engage and limit a number of rights, in particular the right to privacy. The relevant principles relating to the right to privacy are discussed above.

---

81 'appropriate authorising officer' is defined in section 6A of the SD Act and includes senior members of federal law enforcement agencies and state and territory enforcement agencies (for example in the context of the AFP: (a) the Commissioner of Police; or (b) a Deputy Commissioner of Police; or (c) a senior executive AFP employee the chief officer properly authorised).

82 'target computer' may be a particular computer, a computer on particular premises, or a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known): proposed section 28(1B) of the SD Act in Schedule 2 of the bill.

83 Proposed amendments to the SD Act in Schedule 2 of the bill in sections 28(1A) (in relation to the course of an investigation into a relevant offence), section 29(1B) (in relation to a recovery order) and section 30(1A) (in relation to the loss of evidence).

84 See section 28(4),29(3) and 30(3) of the SD Act.

85 Proposed section 35A of the SD Act in Schedule 2 of the bill.

86 See proposed section 34(4) of the SD Act in Schedule 2 of the bill.

87 Proposed section 34(1A), 34(2A), 34(4) of the SD Act in Schedule 2 of the bill.

1.135 The statement of compatibility acknowledges that the new computer access warrant scheme engages the right to privacy 'insofar as accessing a person's personal information held in a computer is inherently privacy intrusive'.[88] It states that the measures pursue the following objective:

> The measure is directed towards the legitimate purpose of ensuring that law enforcement agencies have appropriate powers to investigate serious crimes. Computer access is a valuable in the current digital environment because it allows officers to access data held on a device in an unencrypted state. The ability to execute computer access remotely limits interference with property and limits the risk of harm to law enforcement officers.[89]

1.136 The statement of compatibility also states that the measures pursue the objectives of protecting national security and public order, and that the amendments address advances in technology which enable serious criminals to conduct activities and communicate anonymously.[90] While this may be capable of constituting a legitimate objective for the purposes of international human rights law, further information is required as to the substantial and pressing concern each of the measures seeks to address. That is, while the statement of compatibility states that advances in technology have enabled criminals to conduct activities and communicate anonymously, more information is needed to conclude that this creates a substantial and pressing national security or public order concern, so as to give rise to a legitimate objective justifying the limitation of human rights. Further, it is not clear how some aspects of the computer access warrant regime, such as the proposed use of force provision, are rationally connected to the achievement of any such national security or public order objective.[91] Further information as to the substantial and pressing concern each of the measures seeks to address, and how each of the measures is rationally connected to the achievement of the relevant objectives, would assist with this analysis.

1.137 The statement of compatibility states that the measures include 'a range of safeguards to ensure that the limitation on privacy is reasonable, proportionate and necessary'.[92] These safeguards include, in relation to computer access warrants, that:

- a law enforcement officer must have reasonable grounds to suspect that access to data held on a particular computer is necessary to investigate a federal offence which carries a maximum penalty of at least three years imprisonment;

88 SOC, p. 17 [70].

89 SOC, pp. 17-18 [71].

90 SOC, pp. 18 [84].

91 Proposed section 27E(6) of the SD Act in Schedule 2 of the bill.

92 SOC, p. 18 [72].

- the chief officer of the law enforcement agency to which the computer access warrant was issued must revoke the warrant if it is no longer required to obtain evidence of the offence, and also has an obligation to ensure that access to data is discontinued;
- a Judge or nominated AAT member is responsible for issuing a computer access warrant, and in all cases, the Judge or AAT member must have regard to the extent to which the privacy of any person is likely to be affected and the existence of any alternative means of obtaining the evidence or information sought to be obtained;
- a computer access warrant does not authorise activities likely to cause material loss or damage to other persons lawfully using a computer,[93] except where necessary for concealment (discussed further below); and
- the chief officer of a law enforcement agency must report to the Attorney-General on every computer access warrant issued, and agencies must report annually on the number of warrants applied for and issued during the year and the number of emergency authorisations.[94]

1.138 These safeguards are relevant to determining the proportionality of the limitation on the right to privacy.

1.139 The statement of compatibility also identifies that there are restrictions on the use of information obtained under a computer access warrant in the SD Act, including offences relating to unauthorised disclosure. It also notes that the use, recording and communication of information obtained in the course of intercepting a communication in order to execute a computer access warrant is also restricted, because where an agency wants to gain intercept material for its own purpose, it must apply for, and be issued with, an interception warrant under Chapter 2 of the TIA Act.[95]

1.140 However, as the committee has previously stated, the SD Act was legislated prior to the establishment of the committee, and has therefore not been subject to a foundational human rights compatibility assessment in accordance with the *Human Rights (Parliamentary Scrutiny) Act 2011*. It is difficult to assess the human rights compatibility of measures which extend or amend the existing legislation, or make an assessment as to whether the existing safeguards in the SD Act are sufficient, without the benefit of a foundational human rights assessment.[96]

---

93 See proposed section 27E(5) of the SD Act in Schedule 2 of the bill.

94 SOC, pp. 18-19.

95 SOC, p. 18 [79].

96 See, for example Parliamentary Joint Committee on Human Rights, *Report 12 of 2017* (28 November 2017) pp. 84-88.

1.141 Further, a number of the measures raise concerns from the perspective of proportionality that are not sufficiently addressed in the statement of compatibility. In order to constitute a proportionate limitation on the right to privacy, measures must only go so far as is strictly necessary to achieve the stated objectives of the measures. However, computer access warrants authorise a number of measures which may significantly interfere with a person's privacy, including entering a premises, using a computer, adding or deleting data to a computer, and removing a computer. In particular, computer access warrants can authorise entering third party premises and using 'any other computer' to access relevant data.[97] This is, of its nature, very intrusive and may occur in circumstances where the owner of the third party computer or premises may not be suspected of committing any criminal offence or any of the other bases on which a warrant can be granted (such as being the subject of recovery order). While the use and manipulation of data in another computer is subject to the requirement that it be reasonable in the circumstances and that the relevant decision maker consider other methods of obtaining access that are likely to be effective,[98] it is not clear these safeguards are sufficient in light of the very substantial interference with the right to privacy associated with these measures. This is particularly the case given the broad definition of computer, such that many types of devices may be caught within the scope of these measures, including mobile phones and communications devices which use computers or computing technology as their functional basis (such as security systems, internet protocol cameras and digital video recorders).[99] This raises concerns that the measure may not be sufficiently circumscribed to constitute a proportionate limitation on the right to privacy.

1.142 Further, the statement of compatibility does not address the proportionality of the emergency authorisations. As noted earlier, an emergency authorisation allows access to data held in a target computer without a computer access warrant in certain circumstances of urgency. While a Judge or AAT member is required to approve the emergency authorisation, this is not required until up to 48 hours after the authorisation is originally given, during which time the data could be obtained. The statement of compatibility does not, for example, provide any information as to the compatibility with the right to privacy of the treatment of information where a decision maker does not subsequently approve the emergency authorisation. The explanatory memorandum states that in such circumstances the decision maker may make certain orders (including issuing a computer access warrant for subsequent access) but that the decision maker may not authorise the destruction of relevant information because 'such information, while improperly obtained may still be

97 See proposed section 27E(2)(a),(b) and (e) of the SD Act in Schedule 2 of the bill.

98 See proposed section 27E(2)(e) of the SD Act in Schedule 2 of the bill.

99 EM, p. 88 [421]-[423].

required for a permitted purpose such as an investigation'.[100] There would appear to be less rights restrictive approaches available, including the destruction of information and obtaining a new warrant for an investigation. Further information as to the proportionality of the emergency authorisations, including whether such authorisations are sufficiently circumscribed, are the least rights restrictive approach, and are accompanied by adequate safeguards, would assist in determining the proportionality of these measures.

Committee comment

1.143 The preceding analysis indicates that the proposed computer access warrant scheme in Schedule 2 of the bill engages and limits the right to privacy.

1.144 The committee therefore seeks the advice of minister as to the compatibility of the measures with this right, including:

- **having regard to the matters discussed in the preceding analysis, whether there is reasoning or evidence that establishes that each of the measures addresses a pressing or substantial concern, or whether the proposed changes are otherwise aimed at achieving a legitimate objective;**
- **how the measures are effective to achieve (that is, rationally connected to) the stated objective;**
- **whether the measures are a proportionate limitation on the right to privacy, including:**
    - **whether the measures are sufficiently circumscribed (including in relation to the proposed powers to be able to enter third party premises and use third party computers);**
    - **whether the emergency authorisations are proportionate, including whether such authorisations are sufficiently circumscribed, are the least rights restrictive approach, and are accompanied by adequate safeguards;**
    - **whether the existing safeguards in the *Surveillances Devices Act 2004* are sufficient insofar as those safeguards interact with the measures in the bill; and**
    - **any other information relevant to determining the proportionality of the measures in Schedule 2 of the bill.**

Compatibility of the measures with the right to a fair trial and fair hearing

1.145 As noted earlier, Schedule 2 of the bill also provides that information relating to computer access technologies and methods may be prohibited from disclosure in

100 See proposed section 35A(5) and (6) of the SD Act in Schedule 2 of the bill; EM, p. 108 [579]-[580].

proceedings.[101] As noted in the statement of compatibility, this engages the right to a fair trial and fair hearing because the result of this provision is 'that there may be circumstances where a defendant will not have a chance to review material that the relevant Judge has decided warrants capability protection'.[102]

1.146 The right to a fair trial in Article 14 of the ICCPR provides that in the determination of any criminal charge against a person, that person shall be entitled to certain minimum guarantees including the right to be informed of the charge and to understand the nature of the cause of the charge, and to have adequate time and facilities to prepare a defence. Limitations on the right to a fair trial are permissible where the measures pursue a legitimate objective and are rationally connected with and proportionate to that objective.

1.147 The statement of compatibility describes the objective of the measure as follows:

> Preventing the release of sensitive operational information into the public domain is essential for the protection of the public and for national security. Releasing such information has inevitable harmful consequences for the ability of law enforcement to conduct future operations.[103]

1.148 In general, these objectives are capable of being legitimate objectives for the purposes of international human rights law. However, while such objectives may be legitimate in relation to *public* disclosure of sensitive information, it is not clear whether it is legitimate to preclude a defendant from accessing such information which may be relevant to their case. In this respect it is also not clear how precluding a defendant from reviewing such material is rationally connected to this objective.

1.149 In relation to proportionality, the statement of compatibility states:

> To the extent the right to a fair trial is limited, the limitation is necessary and proportionate. Safeguards include that the presiding officer of the proceeding must make a determination whether the disclosure of the information is necessary for the fair trial of the defendant. It is anticipated that agencies will use computer access powers to gather such material as is necessary to enable other powers to collect evidentiary material, where it is possible to do so. For example, an agency may use a computer access power to gather such intelligence as to enable the application for search warrants under the Crimes Act to be made for a number of suspects. The Crimes Act search warrant would collect such evidence as would be presented in a relevant proceeding. Section 47A does not engage with the

101 See proposed section 47A of the SD Act in Schedule 2 of the bill.

102 SOC, p. 20 [92].

103 SOC, p. 20 [95].

right to be informed in detail, in a language the defendant understands, as it only takes effect after charges have been laid.[104]

1.150 These are relevant safeguards and assist with the proportionality of the measure. However, further information as to whether there may be other less rights restrictive means available (such as allowing for disclosure to a defendant subject to certain conditions, or allowing for disclosure to a defendant's legal counsel), would assist in determining the proportionality of the measure.

Committee comment

1.151 The preceding analysis indicates that the power to prohibit disclosure of information relating to computer access technologies and methods engages and limits the right to a fair trial and fair hearing.

1.152 The committee seeks the further advice of the minister in relation to the compatibility of the measures with this right, including:

- **whether precluding a defendant from accessing information as a consequence of proposed section 47A pursues a legitimate objective;**
- **whether this measure is rationally connected to (that is, effective to achieve) the stated objective; and**
- **whether the measure is proportionate (including whether there are other less rights restrictive measures available).**

Compatibility of the use of force power with multiple rights

1.153 As noted earlier, the 'use of force' provisions in proposed section 27E(6) of the SD Act require computer access warrants to authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant and, if the warrant authorises entering premises, state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.

1.154 Use of force provisions engage multiple human rights. The provisions engage the right to privacy insofar as using force to enter a premises can interfere with a person's right to a private life. Empowering authorised persons to use force against persons may also engage and limit the right to life, as force may be used in a manner that could lead to a loss of life. Empowering persons to use force against other persons may engage the rights to freedom from torture, cruel, inhuman and degrading treatment or punishment, as force may be used in such a way that causes pain (physical or mental) in such a way that it amounts to a violation of these rights.

1.155 The statement of compatibility does not acknowledge that the use of force provisions engage any of these rights. In relation to the right to privacy and the right

104 SOC, p. 20 [93].

to life, limitations may be permissible if it is demonstrated that the measure addresses a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective. The prohibition on torture, cruel, inhuman and degrading treatment or punishment is absolute and can never be justified in any circumstances, regardless of the objective sought to be achieved. Further information from the Minister would therefore assist in determining the compatibility of the use of force provision with these rights.

Committee comment

1.156 The use of force provisions in proposed section 27E(6) of the *Surveillance Devices Act 2004* engage and may limit the right to privacy and the right to life. They may also engage the prohibition on torture, cruel, inhuman and degrading treatment or punishment.

1.157 In relation to the right to privacy and right to life, the committee seeks the advice of the minister as to the compatibility of the use of force provisions with these rights, including:

- **whether the measure is aimed at achieving a legitimate objective for the purposes of human rights law;**
- **how the measure is effective to achieve (that is, rationally connected to) that objective; and**
- **whether the limitation is a proportionate measure to achieve the stated objective.**

1.158 In relation to the prohibition on torture, cruel, inhuman and degrading treatment or punishment, the committee seeks the advice of the minister as to the compatibility of the measures with this right, including any safeguards in place governing the use of force, and any monitoring or oversight in relation to the use of force.

Compatibility of the computer access warrants relating to control orders with multiple rights

1.159 The committee has previously considered that the control orders regime engages a number of human rights, including the right to equality and non-discrimination, the right to liberty, the right to freedom of movement, the right to a fair trial and fair hearing, the right to privacy, the right to freedom of expression, the right to freedom of association, the right to protection of the family, the right to work, the right to social security and an adequate standard of living, and the rights of children.[105] To the extent that computer access warrants can be used against persons subject to a control order (including for determining whether a control order

105 See, most recently, Parliamentary Joint Committee on Human Rights, *Report 10 of 2018* (18 September 2018) pp. 21-36.

has been complied with), several of these rights may also be engaged, in particular the right to privacy.

1.160 Human rights, in particular the right to an effective remedy, may also be engaged in relation to the provisions of the bill that preclude criminal liability for persons who exercised powers relating to the control order computer access warrant if the control order is declared void, as well as the provision which allows for the use of information obtained under the warrant even if the order is declared void.[106] Further, in relation to the ability to use such information even if the control order is declared void, insofar as the information obtained can be used in relation to a matter arising under a preventative detention order,[107] the committee's analysis of the human rights compatibility of the preventative detention order regime is also relevant.[108]

1.161 The statement of compatibility does not acknowledge the human rights implications of these measures. Further information in relation to these matters would assist in assessing whether the measures are compatible with human rights.

Committee comment

1.162 **The preceding analysis indicates that computer access warrants relating to control orders engage multiple human rights. The statement of compatibility does not provide an assessment of whether these measures are compatible with human rights.**

1.163 **The committee therefore seeks the advice of the minister as to the compatibility of this measure with human rights, including whether the measures pursue a legitimate objective, and are rationally connected and proportionate to that objective.**

Concealment of access powers

1.164 Schedule 2 of the bill also seeks to amend the ASIO Act and the SD Act to introduce new concealment of access powers. These powers would authorise doing any thing reasonably necessary to conceal the fact that any thing has been done to a computer. This can include authorisation to do any of the following:

- enter premises where the computer is reasonably believed to be, or enter any other premises for the purposes of gaining entry to or exiting the premises where the computer is reasonably believed to be;
- remove the computer or any other thing from any place where it is situated and return the computer or thing to that place;

106 See proposed section 65A(2A) of the SD Act in Schedule 2 of the bill.

107 See section 65B of the SD Act.

108 See, most recently, Parliamentary Joint Committee on Human Rights, *Report 10 of 2018*(18 September 2018) pp. 36-45.

- where it is reasonable in all the circumstances to do so: use any other computer or a communication in transit to conceal access; and if necessary to achieve that purpose – add, copy, delete or alter data in the computer or the communication in transit; and
- intercept a communication.[109]

1.165 The bill also provides authorisation to exercise these concealment powers with or without a warrant. In particular, the powers can be exercised at any time a computer access warrant is in force, or within 28 days after it ceases to be in force.[110] However, if it is not possible to exercise the concealment powers within the 28-day period after the warrant ceases to be in force, the bill authorises the exercise of the powers 'at the earliest time after the 28-day period at which it is reasonably practicable'.[111]

Compatibility of the measures with the right to privacy

1.166 The relevant principles relating to the right to privacy are summarised above. As acknowledged in the statement of compatibility, the concealment of access powers engage and limit the right to privacy by enabling officers to access devices, which hold personal information, for the purposes of concealment.[112]

1.167 The statement of compatibility states that the measures pursue the objective of protecting the rights and freedoms of individuals by providing ASIO with the tools it requires to keep Australians safe.[113] It also provides the following information as to the rationale for introducing the measures:

> The amendments are necessary to address situations where ASIO no longer has access to the computer at the time the warrant expires but needs to undertake concealment activities. Concealment activities are crucial to ensure that a person does not become aware they are the subject of an investigation, the investigation does not become compromised and sensitive agency capabilities are not revealed.
>
> ASIO cannot always reliably predict whether, or when, it will be able to safely retrieve its devices without compromising a covert security intelligence operation. For example, a person may unexpectedly relocate their computer or device prior to the expiry of the warrant, precluding

109 Proposed sections 25A(8), 27A(3C),and 27E(6) of the ASIO Act, and proposed section 27E(7) of the SD Act in Schedule 2 of the bill.

110 Proposed sections 25A(8)(j), 27A(3C)(j), 27E(6)(j) of the ASIO Act, and , and proposed section 27E(7)(j) of the SD Act in Schedule 2 of the bill.

111 Proposed sections 25A(8)(k), 27A(3C)(k), 27E(6)(k) of the ASIO Act, and proposed section 27E(7)(k) of the SD Act in Schedule 2 of the bill.

112 SOC, p. 17 [63].

113 SOC, p. 17[69].

> ASIO from taking the necessary steps to conceal the fact that it had accessed the device under warrant until the computer or device is available to be access again.
>
> Once the warrant has expired ASIO may not be able to obtain a further computer access warrant to undertake retrieval and concealment activities, as retrieving and concealing would (by definition) not necessarily meet the statutory threshold of 'substantially assisting the collection of intelligence'.[114]

1.168 While this is capable of giving rise to a legitimate objective, further information is required to determine whether this objective is legitimate in the context of these specific measures. It is not clear from the information provided, for example, how concealment of access powers pursue the objective of 'keeping Australians safe'. Further information is also required in order to determine whether this objective applies to the proposed powers under the SD Act and, if not, the legitimate objective of the concealment of access powers under that Act. This information would also assist in determining whether the measures are rationally connected to the objectives sought.

1.169 In relation to proportionality, the statement of compatibility provides the following information:

> The requirement that the concealment activities be performed 'at the earliest time after than 28-day period at which it is reasonably practicable to do so' acknowledges that this authority should not extend indefinitely, circumscribing it to operational need.
>
> The authority conferred by the amendments can only be exercised by the Director-General, or a person or class of persons approved by the Director-General in writing. This item provides a safeguard against the arbitrary exercise of the range of activities permitted by the new subsection.[115]

1.170 While these are relevant safeguards, there remain questions as to the proportionality of the measures. In particular, the powers to conceal access under the bill are extensive, and include entering premises of third parties and using the computers of third parties to conceal the fact that a thing has been done under a warrant. This raises concerns that the measures may be overly broad and more extensive than is strictly necessary to achieve the objectives of the measures.

1.171 The power to conceal access 'at the earliest time after the 28-day period [after the warrant expires] at which it is reasonably practicable' raises additional concerns in relation to proportionality. While the statement of compatibility states that the requirement to exercise the power as early as reasonably practicable means that the authority should not extend indefinitely, 'reasonably practicable' is not

---

114 SOC, p. 17 [64]-[66].

115 SOC, p. 17 [67]-[68].

defined and the provision is not subject to any express time limits. Therefore while as a matter of practice the authority may not extend indefinitely, on the face of the bill the authority could do so if it were not reasonably practicable to exercise the power within a particular timeframe. It appears possible that the authority could be in force for a substantial period of time. This raises concerns as to whether the measures are sufficiently circumscribed. There also appear to be other, less rights restrictive, options available, including requiring further authorisation and supervision from a court following the expiry of the warrant or 28 day period, or defining 'reasonably practicable' by reference to a specific time limit. Further information in relation to these matters would assist in determining the proportionality of the measures.

Committee comment

1.172 The preceding analysis indicates that concealment of access powers in the proposed amendments to the *Surveillance Devices Act 2004* and the *Australian Security Intelligence Organisation Act 1979* engage and limit the right to privacy.

1.173 The committee seeks the advice of the minister as to the compatibility of the measure with this right, including:

- **whether the proposed concealment access powers in each of the *Surveillance Devices Act 2004* and *Australian Security Intelligence Organisation Act 1979* pursue a legitimate objective (including reasoning and evidence to how the measures address a pressing and substantial concern);**
- **whether the proposed concealment access powers are effective to achieve (that is, are rationally connected to) the stated objective; and**
- **whether the proposed concealment access powers are proportionate (including whether the measures are sufficiently circumscribed and whether there are other less rights restrictive measures available).**

Powers to compel persons to assist officers to access data and devices

1.174 Schedule 2 of the bill also seeks to introduce a new provision into the SD Act relating to 'assistance orders', under which a law enforcement officer may apply to a decision maker for an order requiring certain persons (such as the owner of a computer or an employee of the owner of a computer)[116] to provide any information or assistance that is reasonable and necessary to allow the officer to access data that is held in a computer that is the subject of a computer access warrant or emergency authorisation.[117] Assistance orders can also be made to copy data held in the computer to a data storage device, or convert data held in the computer or data storage device into documentary form or another intelligible form.

116 See proposed sections 64A((2),(3),(4),(5),(6) and(7) of Schedule 2 of the bill.

117 Proposed section 64A of Schedule 2 of the bill.

1.175 Schedules 3 and 4 similarly seek to amend the Crimes Act and Customs Act respectively to compel assistance from a person with accessing a device that has been seized under warrant, by making it an offence not to comply with an order to assist where the person is capable of compliance.[118] The offence is punishable by imprisonment for 5 years or 300 penalty units or both, or 10 years or 600 units or both if the offence to which the relevant warrant relates is a serious offence or a serious terrorism offence.[119]

1.176 Schedule 5 seeks to empower the Attorney-General to make an order requiring a specified person to provide assistance that is reasonable and necessary to ASIO in order to gain access to data on a device subject to an ASIO warrant, upon request by the Director-General of ASIO. A person that does not comply with an order is liable to a maximum of five years' imprisonment.

Compatibility of the measures with the right to privacy

1.177 The statement of compatibility acknowledges that these measures engage and limit the right to privacy, insofar as it enables certain law enforcement officers and agencies, the Australian Border Force and ASIO to access private communications and other information on a person's device.[120]

1.178 The stated objective for the measures is the protection of national security and public order.[121] In relation to the proposed introduction of the measure into the Crimes Act in Schedule 3, the statement of compatibility explains why the measure is necessary to achieve its objectives:

> The power to compel assistance is critical to Australia's national security and ensures that law enforcement has the tools necessary to protect Australians. The power for law enforcement to be able to access portable technology devices is necessary and proportionate to achieving the legitimate objectives of protecting national security and public order.[122]

1.179 The statement of compatibility further states that the language of the current provisions is limited because the current provisions 'do not envision people carrying smartphones in their pockets' and the measure seeks to resolve this gap as 'inability to access information held on devices may impede legitimate investigations

---

118 See proposed subsection 3LA(1)(a)(ia) and proposed subsection 3LA(5) of the Crimes Act in Schedule 3 of the bill; see proposed insertion to subparagraph 201(2)(c)(ii) and proposed subsection 201A(3) of the Customs Act in Schedule 4 of the bill.

119 Proposed subsection 3LA(5) of the Crimes Act in Schedule 3 of the bill; proposed 201A(3) of the Customs Act in Schedule 4 of the bill.

120 SOC, p. 21 [101]; p. 25 [124]; SOC, p. 27 [134].

121 SOC, p. 26 [126].

122 SOC, p. 22 [107].

and prosecutions'.[123] The statement of compatibility indicates that the proposed provisions in Schedule 5 empowering the Attorney-General to make an assistance order is 'directed towards the legitimate objective of ensuring that ASIO can give effect to warrants which authorise access to a device' as 'ASIO's inability to access a device can frustrate operations to protect national security'.[124]

1.180 As previously noted, protecting national security and public order is capable of constituting a legitimate objective for the purposes of international human rights law. However, further information is needed to establish why the power to compel assistance in relation to each of the measures is 'critical' to Australia's national security, in particular, why the current capabilities, technology and powers available are insufficient to achieve the objectives to which the measures are addressed. Given the serious consequences for non-compliance with an assistance order, and its potential impact on the privacy of third parties, further information from the minister as to the pressing and substantial concern the measure seeks to address would assist with this analysis.

1.181 Compelling persons to provide assistance to access data and devices pursuant to a warrant appears to be rationally connected to (that is, effective to achieve) the objectives of protecting national security and public order.

1.182 In relation to the proportionality of the measure for the purposes of the Customs Act, the statement of compatibility provides that 'the requirement for a magistrate to authorise warrants provides an important safeguard for person-based search warrants' and notes that to grant an order the magistrate has to be satisfied of several matters set out in the legislation.[125] This is an important safeguard and is relevant to the proportionality of that measure.

1.183 In relation to safeguards available under the ASIO Act for the proposed measures in Schedule 5, the statement of compatibility provides that 'legislative safeguards ensure any limitation on the right to privacy is reasonable and proportionate'.[126] However, the statement of compatibility does not elaborate as to how these purported safeguards will ensure that an assistance order does not limit the right to privacy beyond the extent which is strictly necessary for the purposes of protecting national security and public order. Similarly there is limited information provided as to the safeguards available in relation to the proposed assistance order provisions in the SD Act and the Crimes Act.

1.184 There are also concerns as to whether the measures are sufficiently circumscribed. The provisions may compel assistance from a broad range of persons.

---

123 SOC, p. 22 [102].

124 SOC, p. 27 [137].

125 SOC, p. 26 [127].

126 SOC, p. 27.

For example under the proposed amendments to the SD Act, persons who may be required to provide assistance include employees of the owner of the computer, a person engaged under a contract for services by the owner of the computer, a person who uses or has used the computer, or a person who is or was a system administrator for the computer.[127] While those persons can only be compelled to assist where the person has relevant knowledge of the computer or the measure applied to protect data held in the computer, 'relevant knowledge' is not defined. In any event, the measures nonetheless may involve a significant interference with a person's privacy. This is of particular concern since penalties for non-compliance with the provisions are significant: for example, the offence for non-compliance with an assistance order in Schedule 2 is punishable by imprisonment for 10 years or 600 penalty units or both,[128] and imprisonment of 5 to 10 years or 300 to 600 penalty units or both in relation to the provisions in Schedules 3 and 4.[129]

Committee comment

1.185 The preceding analysis indicates the assistance order provisions in Schedules 2, 3, 4 and 5 engage and limit the right to privacy.

1.186 The committee therefore seeks the further advice of the minister as to the compatibility of the measures with this right, in particular:

- **the pressing and substantial concern that the measures seek to address; and**
- **whether the measures are a proportionate limitation on the right to privacy (including whether the measures are sufficiently circumscribed and accompanied by adequate safeguards).**

127 See proposed sections 64A(2)(d), (3)(d),(4)(b),(5)(b),(6)(b),(7)(b) of the SD Act in Schedule 2 of the bill. The scope is similar in the amendments to Schedules 3 and 4, see section 201A(2) of the Customs Act and section 3LA(2)(b) of the Crimes Act.

128 Proposed section 64A(8) of Schedule 2 of the bill.

129 Proposed subsection 3LA(5) of the Crimes Act in Schedule 3 of the bill and proposed subsection 201A(3) of the Customs Act in Schedule 4 of the bill; see also proposed section 34AAA(4) of the ASIO Act in Schedule 5 of the bill.

Interception of communications under ASIO computer access warrants

1.187 Schedule 2 of the bill also seeks to amend the ASIO Act to introduce new powers associated with the warrant scheme under the ASIO Act to gain access to computers (an 'ASIO computer access warrant'[130]).

1.188 Section 33(1) of the ASIO Act currently provides that ASIO computer access warrants do not authorise the interception of a communication passing over a telecommunications system operated by a carrier or carriage service provider. In order to intercept communications, ASIO is currently required to obtain a telecommunications service warrant under the TIA Act.[131]

1.189 The bill seeks to amend the ASIO Act to repeal section 33 and to expand the operation of ASIO computer access warrants to allow ASIO to intercept a communication passing over a telecommunications system, if the interception is for the purpose of doing anything specified in the ASIO computer access warrant.[132] As a consequence, ASIO will no longer be required to obtain the second warrant under the TIA Act for this purpose.

Compatibility of the measures with the right to privacy

1.190 The relevant principles relating to the right to privacy are summarised above. As acknowledged in the statement of compatibility, the interception of communications under ASIO computer access warrants engages the right to privacy because interception (including interception to enable remote access to a computer) is 'inherently privacy intrusive'.[133] However the statement of compatibility states that the measures are compatible with the right to privacy as the limitation is reasonable, necessary and proportionate.[134]

1.191 The statement of compatibility states that the objective of this measure is for 'ASIO to have effective powers to execute its statutory function to protect national security'.[135] It further states:

---

130 'ASIO computer access warrant' is defined in the proposed amendment to section 5(1) of the TIA Act in Schedule 2 of the bill to mean: (a) a warrant issued under section 25A of the *Australian Security Intelligence Organisation Act 1979*; or (b) a warrant issued under section 27A of the *Australian Security Intelligence Organisation Act 1979* that authorises the Organisation to do any of the acts or things referred to in subsection 25A(4) or (8) of that Act; or (c) an authorisation under section 27E of the *Australian Security Intelligence Organisation Act 1979*.

131 See sections 9 and 9A of the TIA Act.

132 See proposed sections 25A(4)(ba), 25A(8)(h), 27A(3C)(h) and 27E(2)(ea) of the ASIO Act in Schedule 2 of the bill.

133 SOC, p. 15 [50].

134 SOC, p. 15 [50].

135 SOC, p. 15 [51].

> The current arrangements cause administrative inefficiency by requiring ASIO to prepare two warrant applications, addressing different legal standards, for the purpose of executing a single computer access warrant. The process requires the Attorney-General to consider each application separately and in accordance with each separate criterion.
>
> The amendments will mean ASIO will be able to obtain a single computer access warrant, which authorises an officer to undertake all activities that are required to give effect to that warrant. The amendments enhance the operational efficiency of ASIO to collect intelligence in Australia's interest.[136]

1.192 To be capable of justifying a proposed limitation on human rights, a legitimate objective must address a pressing or substantial concern and not simply seek an outcome regarded as desirable or convenient. The stated justification for limiting the right to privacy in the statement of compatibility – namely, to enhance the operational effectiveness of ASIO and address an 'administrative inefficiency' caused by needing to obtain two warrants – does not appear to constitute a pressing and substantial concern for the purposes of international human rights law. Further information as to the legitimate objective of the measure would be helpful in this regard, and would also assist in determining whether the measure is rationally connected to this objective.

1.193 As to proportionality, the statement of compatibility states that the new interception powers are proportionate on the following basis:

> The power is proportionate because the new provisions tightly constrain the purposes for which ASIO may use information intercepted under this provision. ASIO can only use intercepted information in order to execute the computer access warrant. In order for ASIO to use intercepted information for its own intelligence value, ASIO must obtain an interception warrant under the TIA Act.
>
> Consistent with the existing provisions in the ASIO Act, computer access warrants are subject to strict tests and must be signed by the Attorney-General. The Attorney-General may only issue a warrant if he or she is satisfied that there are reasonable grounds for believing that access to data held in a computer will substantially assist the collection of intelligence in respect of matter that is important in relation to security.

1.194 There are safeguards in the bill that assist with the proportionality of the measure. This includes safeguards to be introduced into the TIA Act, including:

- prohibitions on ASIO, the Inspector-General of Intelligence and Security and the Director-General of Security using the computer access intercept

136 SOC, p. 15 [52].

information in connection with the performance of those organisations' functions;[137]

- prohibitions on disclosing information to staff members of certain agencies except for limited purposes of testing and development;[138] and
- a prohibition on giving ASIO computer access intercept evidence in an exempt proceeding, except in certain circumstances.[139]

1.195 However, there remain concerns in relation to the proportionality of the measure. In particular, by expanding the operation of ASIO computer access warrants to allow ASIO to intercept a communication passing over a telecommunications system, the bill appears to, in effect, lower the threshold for obtaining a warrant to intercept such communications. This is because, under the current regime, the threshold for obtaining the second warrant under the TIA Act is that the Attorney-General has be satisfied that:

> (a) the telecommunications service is being or is likely to be:
>
> > (i) used by a person engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, activities prejudicial to security; or
> >
> > (ia) the means by which a person receives or sends a communication from or to another person who is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, such activities; or
> >
> > (ii) used for purposes prejudicial to security; and
>
> (b) the interception by the Organisation of communications made to or from the telecommunications service will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relating to security.[140]

1.196 In contrast, the threshold for obtaining an ASIO computer access warrant under the ASIO Act is that the Attorney-General is satisfied that there are reasonable grounds for believing that access 'will substantially assist the collection of intelligence' in respect of a matter that is important in relation to national

---

137 See proposed sections 64(1)(a) and 65(1)(a) of the TIA Act in Schedule 2 of the bill.

138 See proposed section 65(4)-(7) of the TIA Act in Schedule 2 of the bill.

139 See proposed section 74(1) of the TIA Act in Schedule 2 of the bill. 'Exempt proceeding' is defined in section 5B of the TIA Act. There are certain bases on which ASIO computer access information can be disclosed set out in proposed sections 63AB and 63AC of the TIA Act in Schedule 2 of the bill.

140 See sections 9 and 9A of the TIA Act.

security.[141] This test appears to be a lower threshold for obtaining the warrant. This appears to be acknowledged in the explanatory memorandum to the bill, which states that currently in some circumstances ASIO can obtain a computer access warrant (as currently defined) but cannot contain a telecommunications interception warrant.[142] Based on the information provided, however, it is not clear why the lower threshold in the ASIO Act, as opposed to the higher threshold in the TIA Act, was adopted for the amended ASIO computer access warrants. In this respect, a possible less rights restrictive approach would be to apply the higher threshold under the TIA Act.

Committee comment

1.197 The preceding analysis indicates the proposed amendments to ASIO computer access warrants to allow ASIO to intercept a communication passing over a telecommunications system engage and limit the right to privacy.

1.198 The committee therefore seeks the advice of the minister as to the compatibility of the measures with this right, including:

- **whether the proposed amendments to ASIO computer access warrants to allow ASIO to intercept a communication passing over a telecommunications system pursue a legitimate objective (including reasoning and evidence to how the measures address a pressing and substantial concern);**
- **whether the measure are effective to achieve (that is, are rationally connected to) the stated objective; and**
- **whether the measures are proportionate (including whether there are other less rights restrictive measures available).**

Assistance to foreign countries in relation to data held in computers

1.199 Schedule 2 of the bill also seeks to amend the *Mutual Assistance in Criminal Matters Act 1987* (MA Act) to provide that the Attorney-General may, in the Attorney-General's discretion, authorise an 'eligible law enforcement officer'[143] to

141 See section 25A of the ASIO Act, and proposed section 25A(4)(ba) of the ASIO Act in Schedule 2 of the bill. See also section 27E(4) of the ASIO Act and proposed section 27E(2)(ea) of the ASIO Act in Schedule 2 of the bill.

142 EM, p. 80 [354].

143 'eligible law enforcement officer' means, in the context of the Australian Federal Police, the Commissioner of Police, a Deputy Commissioner of Police, an AFP employee (within the meaning of the *Australian Federal Police Act 1979*), a special member or a person seconded to the Australian Federal Police. In the context of state and territory police forces it includes an officer of the police force or a person seconded to the police force: see column 3 of item 5 of the table in subsection 6A(6), and in column 3 of item 5 of the table in subsection 6A(7), of the SD Act.

apply for a computer access warrant under the SD Act if the Attorney-General is satisfied that:

> (a) an investigation, or investigative proceeding, relating to a criminal matter involving an offence against the law of a foreign country (the *requesting country*) that is punishable by a maximum penalty of imprisonment for 3 years or more, imprisonment for life or the death penalty has commenced in the requesting country; and
>
> (b) the requesting country requests the Attorney-General to arrange for access to data held in a computer[144] (the *target computer*); and
>
> (c) the requesting country has given appropriate undertakings in relation to:
>
> > (i) ensuring that data obtained as a result of access under the warrant will only be used for the purpose for which it is communicated to the requesting country; and
> >
> > (ii) the destruction of a document or other thing containing data obtained as a result of access under the warrant; and
> >
> > (iii) any other matter the Attorney-General considers appropriate.[145]

1.200 The 'target computer' may be a particular computer, a computer on particular premises, or a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).[146]

1.201 The bill also amends the definition of 'protected information' in the MA Act to incorporate the proposed new definition of 'protected information' in the SD Act, which states that any information (other than general computer access intercept information) obtained from access to data under either the new computer access warrant or emergency authorisation for access to data held in a computer is 'protected information'.[147] The effect of this, according to the explanatory memorandum, is that where information is obtained in response to a computer access warrant for a domestic investigation, the Attorney-General may authorise the provision of that information to a foreign country in response to a mutual assistance request, subject to existing restrictions under section 13A of the MA Act.[148]

---

144 The phrases 'data', 'data held in a computer' and 'computer' have the same meaning as in the SD Act discussed above.

145 Proposed section 15CC(1) of the MA Act in Schedule 2 of the bill.

146 Proposed section 15CC(2) of the MA Act in Schedule 2 of the bill.

147 See proposed amendments to section 44 of the SD Act in Schedule 2 of the bill, and proposed amendment to section 3(1) of the MA Act in Schedule 2 of the bill.

148 See EM, p. 84 [395].

Compatibility of the measure with multiple rights

1.202 The committee has previously raised concerns regarding the human rights implications of Australia's mutual legal assistance scheme in relation to the right to liberty, right to life, prohibition against torture and cruel, inhuman and degrading treatment, the right to a fair hearing, right to equality and non-discrimination and the right to an effective remedy.[149]

1.203 For example, concerns regarding the right to life arise because the MA Act allows the Australian government to give assistance to a foreign country to help it investigate an offence or gather evidence in order to prosecute. The MA Act provides that a request by a foreign country for assistance under the Act must be refused if the offence is one in respect of which the death penalty may be imposed. However, the MA Act qualifies this by saying that this prohibition will not apply if 'the Attorney-General is of the opinion, having regard to the 'special circumstances' of the case, that the assistance requested should be granted'.[150] In relation to the present bill, then, providing assistance in the form of a computer access warrant may engage and limit the right to life to the extent it may lead to an individual in another country being tried and convicted of a criminal offence that carries the death penalty.[151]

1.204 The statement of compatibility does not acknowledge that the amendments to the MA Act introduced in Schedule 2 of the bill may engage multiple human rights and therefore does not provide an analysis of whether any limitation on these rights is permissible.[152] In accordance with the committee's *Guidance Note 1,* the committee's usual expectation where a measure may limit a human right is that the accompanying statement of compatibility explain how the measure supports a legitimate objective and how it is rationally connected to, and proportionate to achieve, its legitimate objective.

---

149 See, in relation to amendments to the MA Act, Parliamentary Joint Committee on Human Rights, *Report 2 of 2017*, (21 March 2017) pp. 3-9; *Report 4 of 2017* (9 May 2017) pp. 70-73 and pp. 90-98; *Twenty-second report of the 44th Parliament* (13 May 2015) pp. 108-110; *Sixth report of 2013* (15 May 2013) pp. 167-172; *Tenth Report of 2013* (26 June 2013) pp. 56-75.

150 See subsection 8(1A) of the MA Act.

151 While the ICCPR itself does not completely prohibit the imposition of the death penalty, international law prohibits states which have abolished the death penalty, such as Australia, from exposing a person to the death penalty in another nation state. The United Nations Human Rights Committee has outlined that this not only prohibits deporting or extraditing a person to a country where they may face the death penalty but also prohibits the provision of information to other countries that may be used to investigate and convict someone of an offence to which the death penalty applies: see See Human Rights Committee, *Concluding observations on the fifth periodic report of Australia*, CCPR/C/AUS/CO/5, 7 May 2009, [20].

152 It is noted that some of the human rights that may be engaged by the MA Act are absolute rights that are not capable of limitation, namely the prohibition against torture and cruel, inhuman and degrading treatment.

Committee comment

1.205 The committee has previously stated that the *Mutual Assistance in Criminal Matters Act 1987* would benefit from a full review of the human rights compatibility of the legislation, as it raises human rights concerns in relation to the right to liberty, right to life, prohibition against torture and cruel, inhuman and degrading treatment, the right to a fair hearing, right to equality and non-discrimination and the right to an effective remedy.

1.206 The statement of compatibility does not acknowledge that any human rights are engaged by the amendments to the *Mutual Assistance in Criminal Matters Act 1987* introduced in Schedule 2 of the bill. The committee therefore seeks the advice of the Minister on the compatibility of the amendments to that Act with these human rights.

Power for law enforcement and Australian Border Force to access computers remotely

1.207 Schedules 3 and 4 of the bill seek to empower law enforcement agencies and the Australian Border Force to remotely access a computer on premises the subject of a warrant obtained pursuant to the Crimes Act and *Customs Act 1901* (Customs Act), respectively.[153]

1.208 The proposed amendments provide that, for the purposes of obtaining access to data (relevant data) held in a computer or device on premises subject to a warrant, an officer executing the warrant (executing officer) may use any other computer to determine if the relevant data is evidential material of the kind specified in the warrant. In doing so, an executing officer may also copy the relevant data, or add, copy, delete or alter other data where necessary to use the computer or device for the purposes of the warrant.

1.209 The proposed amendments to the Crimes Act additionally seek to empower law enforcement agencies to use a computer found during a search authorised under the warrant (warrant computer), or telecommunications facility, or any other electronic equipment, for the purpose of obtaining access to 'account-based data'[154] of a living or deceased person who is/was the owner or lessee of the warrant

153 See proposed section 3F(2A) of the Crimes Act in Schedule 3 of the bill and proposed section 199(4A) of the Customs Act in Schedule 4 of the bill.

154 Data is 'account-based data' if an electronic service has accounts for end-users, and the person (living or deceased) holds (or held) an account with the electronic service, or the person is or is likely to be (or was) a user of an account with an electronic service, and the person can (or could) access particular data provided by the service: see proposed section 3CAA of the Crimes Act in Schedule 3 of the bill.

computer, or who uses or has used the warrant computer,[155] to determine if it is evidential material of a kind specified in the warrant.

Compatibility of the measures with the right to privacy

1.210 The statement of compatibility notes that the measure engages the right to privacy by enabling law enforcement agencies and Australian Border Force 'to access private communications and other information on a device using a range of methods'.[156] However, it states that the restriction is necessary and proportionate to achieve the legitimate objective of 'protecting national security and public order' by providing law enforcement and Australian Border Force with 'the tools they require to investigate criminal activity and protect Australian's [sic] national security in a modern context'.[157] The statement of compatibility states further that 'currently... to use [the power to access data electronically] an officer must be physically located at the warrant premises' and that 'these amendments will allow [officers] to access data without having to be physically present'.[158] While protecting national security and public order is capable of constituting a legitimate objective, as noted earlier in order to justify a restriction on human rights, the measure must address a pressing and substantial concern, not just an outcome regarded as desirable and convenient. In this respect it is not clear whether introducing the measures so executing officers do not have to attend warrant premises in person addresses a pressing and substantial concern.

1.211 The power to access data held in a computer or device on premises the subject of a warrant under the Crimes Act or Customs Act appears to be rationally connected with the objective of protecting national security and public order.

1.212 As to proportionality, the statement of compatibility provides that 'the bill includes limitations to ensure the power is proportionate and does not impact other users of communications services, including joint account holders',[159] namely:

> The addition, deletion or alteration of data is not authorised when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless specified in the warrant. The addition, deletion or alteration of data is also not authorised when those actions are likely to cause other material loss or damage to other persons lawfully using a computer.[160]

155 See proposed section 3F(2B) of the Crimes Act in Schedule 3 of the bill.

156 SOC, p. 21 [96]; p. 234 [116].

157 SOC, p. 25 [120]; see also p. 21 [100].

158 SOC, p. 21 [97]-[98]; p. 24 [117]-[118].

159 SOC, p. 1 [99]; p. 24 [119].

160 SOC, p. 24 [119]; p. 21 [99].

1.213 This is capable of constituting a relevant safeguard, but questions remain as to the extent to which the safeguard will be effective. While the addition, deletion or alteration of data is not authorised if it will materially interfere with, interrupt or obstruct the lawful use by other persons of a computer, it will be authorised if it is necessary to do one or more of the things specified in the warrant.[161] Given that a computer or device on warrant premises is accessed for the broad purposes of obtaining evidential material of the kind described in the warrant, it appears that there could be a large number of circumstances in which adding, deleting or altering data such as to interfere with the lawful use of that computer by a third person could be justified as necessary to do one or more things for the purposes of the warrant.

1.214 This raises concerns in the context of the proposed warrants under the Crimes Act, which allow access to account-based information. This measure could affect not just joint account holders, as the statement of compatibility notes, but could also potentially affect any person who has used that computer, for example to access their bank account through online banking. Further information from the minister as to how the safeguard will operate to limit the impact on third parties would be useful for the purposes of this analysis.

1.215 The statement of compatibility provides that the interference with privacy is 'not arbitrary' as it is 'authorised under domestic law'.[162] However, the exercise of a power prescribed by law can still be arbitrary if it is not necessary or if it is not sufficiently circumscribed in light of its objectives. Here, it is relevant that the power to access relevant data remotely can only be exercised if it is 'reasonable in all the circumstances to do so' having regard to 'other methods (if any) of obtaining access to the relevant data which are likely to be as effective'.[163]

1.216 This goes some way towards ensuring that the limitation on rights occasioned by remote access to data occurs only when it is strictly necessary. However, it is not required that other less rights restrictive means must be pursued first if available, just that they be considered before exercising the power. In addition, other than the availability of alternative means, no definition or guidance is provided as to when it will be 'reasonable in all the circumstances' to access data remotely, thereby appearing to leave interpretation of this standard to the executing officer. Therefore, it is unclear whether this will function as an effective safeguard to ensure that the power is only exercised when necessary such that the limitation on rights occasioned by the measure is proportionate to its objectives.

---

161 See proposed section 3F(2C) of the Crimes Act in Schedule 3 of the bill and proposed section 199(4B) of the Customs Act in Schedule 4 of the bill.

162 SOC, p. 21 [100].

163 See proposed section 3F(2A)(c) of the Crimes Act in Schedule 3 of the bill and proposed section 199(4A) of the Customs Act in Schedule 4 of the bill.

1.217 As currently framed, the power is such that it could be exercised in a broad range of circumstances, including potentially where it was simply more convenient to access information remotely than to attend warrant premises. Further information from the minister as to how safeguards will ensure that the measure is only used where necessary, such as any relevant guidelines that may assist executing officers in determining whether it is 'reasonable in all the circumstances' to access data remotely, would assist with this analysis.

Committee comment

1.218 The preceding analysis raises questions as to the compatibility of the proposed power of law enforcement and Australian Border Force to access computers remotely with the right to privacy.

1.219 The committee therefore seeks the advice of the minister as to the compatibility of the measures with this right, including:

- **the pressing and substantial concern which the measures seek to address**;
- **how the proposed safeguards will be effective to limit the impact on the right to privacy of third parties who are lawful users of the computer or device subject to the warrant; and**
- **any relevant guidelines that may apply to the exercise of the power to access data remotely.**

Power for Australian Border Force to search persons who may have computers or devices under the Customs Act

1.220 Proposed section 199A of the Customs Act in Schedule 4 of the bill empowers a judicial officer to issue a warrant authorising an ordinary search or a frisk search of a person where there are reasonable grounds to suspect the person has in their possession, or will in the next 72 hours have in their possession, any computer, or data storage device, that is evidential material.[164]

Compatibility of the measure with the right to privacy

1.221 The statement of compatibility acknowledges that the measure engages the right to privacy but concludes that 'the interference is proportionate and necessary to meet legitimate objectives'.[165] The statement of compatibility states that:

> While the nature of searching a person in order to gain access to a device is inherently intrusive, it is not arbitrary as it is a targeted law enforcement tool designed to assist the [Australian Border Force] to effectively investigate crimes in the current technological environment. The power

164 See proposed section 199A(1) of the Customs Act in Schedule 4 of the bill.

165 SOC, p. 24 [115].

has the legitimate objective of protecting national security and public order.[166]

1.222 Protecting national security and public order are capable of constituting a legitimate objective for the purposes of international human rights law, where there is a pressing or substantial concern to which the measure responds. While this is not explicitly identified, the statement of compatibility provides that 'under existing laws, the [Australian Border Force] could obtain a judicial warrant to search premises' but 'the amendments recognise that information is often stored on devices, held physically by persons, and that an inability to access the information may impede legitimate investigation and prosecutions'.[167] Given that the device would be subject to the warrant but for it being on a person, and given the prevalence of portable devices, such as smartphones, it would appear this is a pressing and substantial concern which the measure seeks to address. The measure also appears to be rationally connected to the objective.

1.223 In relation to proportionality, as noted by the statement of compatibility, the requirement for a judicial officer to authorise warrants, and the time limit of seven days for executing the warrant, are capable of functioning as relevant safeguards.[168] In relation to whether the warrant power is sufficiently circumscribed, the matters that are authorised by a search warrant relating to a person are largely identical to those authorised in relation to the proposed powers to access computers remotely under the Crimes Act and the Customs Act.[169] Therefore, the analysis and concerns raised above at [1.212]-[1.213] and [1.215]-[1.217] also apply in relation to the measure. That is, whether the safeguards will ensure that the power is only exercised when necessary, and in a manner that will limit its impact on third parties, such that the limitation on rights occasioned by the measure is proportionate to its objectives.

Committee comment

1.224 The preceding analysis raises questions as to the compatibility of the power for Australian Border Force to search persons who may have computers or devices under the *Customs Act 1901* with the right to privacy.

1.225 The committee therefore seeks the advice of the minister as to the proportionality of the limitation on this right, including whether the proposed safeguards will be effective to limit the impact on the right to privacy of third parties who are lawful users of the computer or device subject to the warrant.

166 SOC, p. 24 [114].

167 SOC, p. 24 [113].

168 SOC, p. 24 [115].

169 Compare proposed subsections 199B(2)-(3) of the Customs Act in Schedule 4, with proposed subsection 3F(2A) of the Crimes Act in Schedule 3 and proposed section 4A of the Customs Act in Schedule 4.

Amendments to the Crimes Act and Customs Act which allow electronic devices moved under warrant to be kept for analysis for 30 days

1.226 Schedules 3 and 4 of the bill seek to amend the Crimes Act and Customs Act respectively to extend the time period for which devices moved under warrant can be kept for analysis to 30 days, from the current period of 14 days permitted under the Crimes Act,[170] and 72 hours under the Customs Act.[171]

Compatibility of the measure with the right to privacy

1.227 The statement of compatibility states that 'moving a person's computer or data storage device engages the right to privacy, as it may restrict a person's access to person information'[172] but that it is 'a proportionate and necessary measure to achieve the legitimate objective of protecting national security and public order'.[173]

1.228 The statement of compatibility does not identify the pressing and substantial concern which the measure seeks to address, but states that extending the timeframe to 30 days will ensure Australian Border Force can 'fulfil its statutory functions with forensic best practice'.[174] The statement of compatibility also indicates that extended timeframes will allow law enforcement agencies 'adequate time to conduct the lengthy and intricate forensic processes necessary to determine whether there is evidential material in the electronic advice'.[175] Further information from the minister as to how these matters constitute a pressing and substantial concern, including what constitutes 'forensic best practice' and information as to how current timeframes are inadequate or insufficient, would assist with assessing whether the measure pursues a legitimate objective and is rationally connected to that objective.

1.229 As to proportionality, limited information is provided in the statement of compatibility. It is not clear, for example, whether extending the time period to 30 days represents the least rights restrictive approach, or whether the same objectives could be achieved by, for example, extending the time period for less than 30 days, or extending the number of times an extension can be sought and the time period of those extensions. The statement of compatibility does not identify any safeguards to ensure the measure does not limit the right to privacy any more than necessary, nor does it consider the impact that, for example, holding a person's computer or mobile phone for a month, as opposed to three days or two weeks, may have on other

---

170 See proposed subsection 3K(3B) of the Crimes Act in Schedule 3 of the bill.

171 See proposed subsection 200(3A) of the Customs Act in Schedule 4 of the bill.

172 SOC, p. 23 [108]; p. 26 [129].

173 SOC, p. 23 [112]; see also p. 26 [131].

174 SOC, p. 26 [131].

175 SOC, p. 23 [108].

rights.[176] It is also not clear from the bill or acts it seeks to amend whether there are processes in place to ensure that devices are returned expeditiously if it is determined that they do not contain evidential material relevant to the warrant before the end of the period for which the device may be lawfully held. Therefore, further information from the minister as to the relevant safeguards that apply to ensure that warrant property is only held as long as necessary to achieve the objectives of the bill would assist in determining the proportionality of the measure.

Committee comment

1.230 The preceding analysis raises questions as to the compatibility of the amendments to the *Crimes Act 1914* and *Customs Act 1901* which allow electronic devices moved under warrant to be kept for analysis for 30 days with the right to privacy.

1.231 The committee therefore seeks the advice of the minister as to the compatibility of the measure with this right, including:

- **the pressing and substantial concern which the measure seeks to address (including how existing timeframes are inadequate for determining whether the device moved from warrant premises and kept for analysis contains evidential material of the type listed in the warrant)**;
- **how extending the timeframes for which a device moved under a warrant can be held for analysis is rationally connected with (that is, effective to achieve) the objectives of the measure; and**
- **whether the measure represents a proportionate limitation on the right to privacy (including whether the measure represents the least rights restrictive approach to ensuring law enforcement and Australian Border Force have adequate time to determine if the device contains evidential material of the kind specified in the warrant, and any processes in place to ensure the devices are returned expeditiously)**.

Release from civil liability for providing voluntary assistance to ASIO

1.232 Schedule 5 of the bill amends the ASIO Act to release from civil liability, any person who voluntarily engages in conduct in accordance with a request from the Director-General of ASIO, for or in relation to that conduct.[177]

Compatibility of the measure with the right to an effective remedy

1.233 The bill does not define 'conduct' (except insofar as it specifies some conduct which will not attract immunity from civil liability),[178] so it is difficult to assess what

176 For example, the right to work (article 6 of the ICCPR).

177 Proposed section 21A of Schedule 5 of the bill.

178 Proposed subsections 21A(1)(b),(d),(e) of Schedule 5 of the bill.

rights this measure may engage and limit, and whether those limitations are legitimate for the purposes of international human rights law. However, in general releasing a person from civil liability in relation to conduct engages the right to an effective remedy, insofar as an individual whose rights are violated by that conduct cannot pursue a civil remedy against the person. This raises concerns given that 'conduct' is not defined in the bill and therefore could potentially encompass a wide range of acts that could impact individual rights, relevantly limited only by the requirement that it not be an offence.[179] However, the statement of compatibility does not address the right to an effective remedy in relation to the measure, and accordingly no assessment was provided as to the compatibility of this measure with this right.

Committee comment

1.234 The preceding analysis raises questions as to the compatibility of providing voluntary assistance to ASIO with the right to an effective remedy.

1.235 The committee therefore seeks the advice of the minister as to the compatibility of the measure with this right.

179 Proposed section 21A(1)(e) of Schedule 5 of the bill.

Bills not raising human rights concerns

1.236 Of the bills introduced into the Parliament between 17 and 20 September, the following did not raise human rights concerns (this may be because the bill does not engage or promotes human rights, and/or permissibly limits human rights):

- Aviation Transport Security Amendment Bill 2018
- Corporations Amendment (Strengthening Protections for Employee Entitlements) Bill 2018
- Criminal Code Amendment (Food Contamination) Bill 2018
- Customs Amendment (Collecting Tobacco Duties at the Border) Bill 2018
- Customs Amendment (Peru-Australia Free Trade Agreement Implementation) Bill 2018
- Customs Amendment (Product Specific Rule Modernisation) Bill 2018
- Customs Tariff Amendment (Peru-Australia Free Trade Agreement Implementation) Bill 2018
- Excise Tariff Amendment (Collecting Tobacco Duties at Manufacture) Bill 2018
- Higher Education Support (Charges) Bill 2018
- Higher Education Support Amendment (Cost Recovery) Bill 2018
- Higher Education Support Amendment (VET FEE-HELP Student Protection) Bill 2018
- Income Tax (Managed Investment Trust Withholding Tax) Amendment Bill 2018
- Income Tax Rates Amendment (Sovereign Entities) Bill 2018
- Maritime Legislation Amendment Bill 2018
- Treasury Laws Amendment (2018 Measures No. 5) Bill 2018
- Treasury Laws Amendment (Black Economy Taskforce Measures No. 2) Bill 2018
- Treasury Laws Amendment (Design and Distribution Obligations and Product Intervention Powers) Bill 2018
- Treasury Laws Amendment (Gift Cards) Bill 2018
- Treasury Laws Amendment (Making Sure Foreign Investors Pay Their Fair Share of Tax in Australia and Other Measures) Bill 2018
- Treasury Laws Amendment (Making Sure Multinationals Pay Their Fair Share of Tax in Australia and Other Measures) Bill 2018
- Veterans' Affairs Legislation Amendment (Omnibus) Bill 2018