Chapter 2

Concluded matters

2.1 This chapter considers the responses of legislation proponents to matters raised previously by the committee. The committee has concluded its examination of these matters on the basis of the responses received.

2.2 Correspondence relating to these matters is available on the committee's website.[1]

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	Privacy; presumption of innocence
Previous report	Report 11 of 2018
Status	Concluded examination

Background

2.3 The committee first reported on the bill in its *Report 11 of 2018*, and requested a response from the minister by 31 October 2018.[2]

2.4 The minister's response to the committee's inquiries was received on 6 November 2018. The response is discussed below and is available in full on the committee's website.[3]

1 See: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports.

2 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018), pp. 2-8.

3 The minister's response is available in full on the committee's scrutiny reports page: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports.

Information disclosure powers

2.5 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.

2.6 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;[4]
- 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;[5]
- 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);[6]
- 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;[7]
- 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;[8]

4 Section 61(1)(a).

5 Section 61(1)(b).

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

7 Section 61(1)(e).

8 Section 61(1)(f).

- 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;[9]
- 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;[10]
- where the disclosure is made to the Aged Care Pricing Commissioner to assist in the performance of their functions under the Aged Care Act;[11] and
- where the disclosure is made to a person of a kind specified in the rules, for a purpose specified by the rules.[12]

2.7 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.

Compatibility of the measure with the right to privacy: initial analysis

2.8 The right to privacy includes 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.[13] The initial human rights analysis stated that, as acknowledged in the statement of compatibility,[14] the power to disclose protected information (including personal information) engages and limits the right to privacy.

2.9 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.

---

9 Section 61(1)(g).

10 Section 61(1)(h).

11 Section 61(1)(i).

12 Section 61(1)(j).

13 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).

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

2.10 The statement of compatibility states that the provisions in proposed section 61 are in place so that immediate action can be taken to protect aged care consumers. It also states that the Commissioner must have the ability to disclose protected information swiftly when an aged care consumer's health, safety or well-being is or may be at risk.[15] In light of this information, the initial analysis stated that it is possible that the measures in proposed section 61 pursue a legitimate objective and are rationally connected to that objective.

2.11 The initial analysis noted that 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 objectives of the measure. In this respect, the initial analysis noted that 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 the persons or organisations to whom information may be disclosed are subject to the *Privacy Act 1988* (Privacy Act).

2.12 The initial analysis further noted that the statement of compatibility does not provide any information as to the proposed power to disclose information pursuant to rules,[16] which raised further additional questions as to whether the disclosure power is sufficiently circumscribed. In this respect, the analysis noted that it is not clear whether the rules will contain safeguards on the disclosure of personal information, such as requiring the consent of a person affected or providing for the review of the disclosure by an independent body.

2.13 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) at pp. 2-6.[17]

2.14 The committee therefore requested the advice of the minister as to whether the limitation on the right to privacy in proposed section 61 is proportionate, in particular:

- 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 Proposed paragraph 61(1)(j).

17 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 2-6 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

- 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 also requested 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).

Minister's response and analysis

2.15 The minister's response acknowledges that proposed section 61(1), which would permit disclosures of protected information in a variety of circumstances, engages and limits the right to privacy.

2.16 The response includes detailed advice as to whether the measures in proposed sections 61(1)(a) and 61(1)(j) are a proportionate limitation on the right to privacy. These aspects of the disclosure powers raised specific concerns as to their proportionality and in particular whether they were sufficiently circumscribed. This is considered below.

Disclosures in the public interest: proposed section 61(1)(a)

2.17 The minister's response states that the power to disclose 'to such persons and for such purposes as the commissioner determines' where it is in the public interest to do so must be broad to ensure that the bill is sufficiently flexible to respond to circumstances where there is an 'unforeseen public interest need' to disclose information. As such, the minister's response appears to indicate that the scope of the power in proposed section 61(1) is the least rights restrictive approach reasonably available The minister's response also states that proposed section 61(1)(a) intends to cover:

> ...a narrow category of disclosures which fall outside the routine administration of the bill or rules as provided by proposed section 60(3), and where disclosure is not available for any of the other specific purposes listed in proposed sections 56 to 59 and 61(1).

2.18 The response further argues that it is not possible to codify the purposes or persons to whom information may be disclosed—particularly given the interrelated purposes for which information is used in aged care regulation. However, the response provides examples of the purposes for which information may be disclosed in the public interest, stating that these may range from:

> …matters affecting the rights of aged care consumers, to broader purposes relating to other areas outside the health portfolio, such as corporate governance or workplace relations or consumer protection more broadly. Disclosures for these purposes are likely to arise from opportunities for policy development, education or quality improvement.

2.19 While it is acknowledged that some flexibility may be required in order to address unforeseen public interest needs, the power itself is nonetheless extremely broad: it would allow the Commissioner to disclose protected information to any

person, for any purpose, if the Commissioner determines that to do so is in the public interest.

2.20 Noting the broad scope of the power, the safeguards that apply when the commissioner may determine whether disclosure is in the 'public interest' are particularly important in determining whether the limitation on the right to privacy is important. In this respect, the minister's response outlines factors to which the Commissioner may have regard when determining whether a disclosure under section 61(1)(a) is in the 'public interest'. The response states that the Commissioner 'would be expected to balance the public interest served by disclosing protected information against a range of considerations in favour of non-disclosure'. It also states that, where protected information contains personal information, the public interest benefit would be weighed against an individual's right to information privacy and the impact that disclosure may have in the circumstances. The response elaborates on this matter, stating that:

> …consideration would be given to factors such as the nature, sensitivity and impacts of any disclosure of information particularly where it includes sensitive health information, the vulnerability of aged care consumers, and whether there are alternatives which might avoid the disclosure of personal information or minimise the scope of information disclosed.

2.21 The minister's response explains that, in determining what is in the public interest, regard would be had to the objectives of the bill and whether they would be served or frustrated by disclosing protected information. The response states that these objectives include protecting the health, safety and wellbeing of aged care consumers, promoting confidence in aged care services, and promoting best practice models of engagement between aged care consumers and providers.

2.22 Finally, the minister's response reiterates that while the 'public interest' exception is broad, it would only apply on a case-by-case basis, and only where the public benefit outweighs privacy considerations in the relevant circumstances.

2.23 Despite the minister's detailed explanation as to the factors that would be taken into account when determining whether disclosure is the 'public interest', it does not appear to *require* the power to be exercised in that manner. For example, the bill does not prescribe any matters to which the Commissioner must have regard before disclosing information under proposed section 61(1)(a), or require the Commissioner to notify a person about whom information is to be disclosed and give that person an opportunity to make representations about the disclosure. Further, there is no explicit requirement that in determining what is in the 'public interest' that an individual's right to privacy be considered at all. This kind of requirement or safeguard would appear to be a less rights restrictive approach which is reasonably available. Given the breadth of the power and the absence of further statutory restrictions with respect to its exercise, the power of disclosure in proposed 61(1)(a) does not appear to be a proportionate limitation on the right to privacy.

Disclosures pursuant to the rules: proposed section 61(1)(j)

2.24 The response states that power to disclose to a person of a kind specified in the rules, for a purpose specified by the rules, is necessarily broad, and that it is not possible to prescribe the specific circumstances for which rules might allow information to be disclosed. The response further states that an equivalent power in the Aged Care Act has been necessary to ensure the seamless operation of aged care quality regulation with related legislation relating to matters such as safety, and the payment of aged care subsidies, pensions and other government payments. As such, the minister's response appears to indicate that the power to disclose information pursuant to rules made under proposed section 61(1)(j) is the least rights-restrictive means available to achieve the objectives of the measure.

2.25 The minister's response further states that any rules made under proposed section 61(1)(j) will be subject to disallowance, and argues that this additional level of parliamentary oversight provides an important safeguard against arbitrary limitations on the right to privacy. It further notes that a statement of compatibility would be incorporated into the explanatory statement for any rules made under proposed section 61(1)(j).

2.26 The fact that any rules would be subject to disallowance may assist the proportionality of the measure. However, it is noted that the bill does not appear to set any further limits on the exercise of the rule-making power in proposed section 61(1)(j). For example, it does not require that the Commissioner have regard to any particular matters when exercising the power, or impose restrictions on the persons or classes of persons to whom the rules may permit disclosure. Accordingly, without sufficient safeguards, it is possible that rules could be made that do not impose a proportionate limitation on the right to privacy.

2.27 As noted in the initial analysis, it is also unclear whether the rules themselves will contain adequate safeguards for the disclosure of personal information, such as requiring the consent of affected persons or providing for the review of disclosures by an independent body. Much will depend on the content of the rules made under section 61(1)(j) and how the power is applied in practice. Any rules made under proposed section 61(1)(j) will need to ensure that authorised disclosures are made in a manner compatible with the right to privacy. Should the bill be passed, the committee will assess the rules for compatibility with human rights. In this respect, it would have been useful had the minister's response included a copy of the rules, or a detailed outline of any proposed rules relating to the right to privacy, as requested by the committee.

Compatibility of the disclosure powers – sections 61(1)(b) to (i)

2.28 In relation to the proposed disclosure powers in sections 61(1)(b) to (i), it is noted that disclosures made under those sections are limited to prescribed circumstances. The minister's response also confirms that, in some circumstances, disclosures of protected information (which may include personal information) may

be made to persons who are not subject to the Privacy Act or to equivalent state or territory privacy regimes. However, the minister's response explains that any disclosures of protected information made under proposed section 61(1) will be subject to the requirement that onward disclosures be limited to the purpose for which the original disclosure was made. It is also noted that the bill contains a prohibition on the use, disclosure and recording of protected information (with exceptions provided for authorised conduct). These safeguards assist the proportionality of the measures, and may be sufficient to ensure that these more limited powers are exercised in a manner that is compatible with human rights.[18]

Committee response

2.29 The committee thanks the minister for his response and has concluded its examination of this issue.

2.30 Based on the information provided, the powers of disclosure in proposed sections 61(1)(b) to (i) may be compatible with the right to privacy.

2.31 However, the preceding analysis indicates that, noting the absence of relevant safeguards and the breadth of the power of disclosure in proposed section 61(1)(a), the power may be incompatible with the right to privacy.

2.32 Subject to the content of any rules made under proposed section 61(1)(j), the committee considers that the power of disclosure in that provision may be capable of operating in a way that is compatible with the right to privacy. However, noting the broad scope of the proposed rule-making power, there may be concerns in relation to its operation. This is because its scope is such that it could be used in ways that may risk being incompatible with the right to privacy. If the bill is passed, the committee will consider the human rights implications of the rules once they are received. The committee also notes that it is preferable for the details of proposed rules to be available for consideration in conjunction with the related bill prior to its passage.

Information sharing arrangements

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

2.34 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

---

18 For example, proposed section 61(1)(e) permits the Commissioner to disclose protected information 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. Noting that onward disclosures are restricted, and that unauthorised disclosures are prohibited, it is likely that the power in proposed section 61(1)(e) would be compatible with the right to privacy.

secretary requires the information to perform their functions or exercise their powers. Proposed 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.

2.35 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: initial analysis

2.36 The relevant principles relating to the right to privacy are outlined above at [2.8]. The initial analysis stated that it was unclear on the face of the bill whether 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'.

2.37 The initial analysis stated that, to the extent that personal information may be disclosed under Division 2, questions arise as to whether the measure is a proportionate limitation on the right to privacy. The initial analysis noted that the statement of compatibility provides no information in this respect. The full initial human rights analysis is set out in *Report 11 of 2018* (16 October 2018) at pp. 6-7.[19]

2.38 The committee therefore requested the minister's advice 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.

Minister's response and analysis

2.39 The minister's response states that information shared in accordance with Division 2, Part 7 of the bill may include personal information. This raises questions as to whether the measures are a proportionate limitation on the right to privacy.

2.40 In relation to the proportionality of the measures, the minister's response states that the provisions do not impose any additional limitations on the right to

19 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 6-7 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

privacy, since they only deal with disclosures that are already permitted under the bill. The response further states that:

> …clauses 56(2)(a), 57(a) and 58(1)(a) and 2(a) limit the information that may be shared under Division 2 of Part 7 to only information that is required for the Commissioner's or Secretary's functions or powers. Sub-clauses 60(3)(a)(i) and (ii) provide that disclosures made in the course of performing functions or exercising powers under the Bill or the *Aged Care Act 1997* will be exceptions to the offence of disclosing protected information under clause 60(1) of the bill.
>
> Given the Commissioner and Secretary share interdependent functions, information that is disclosed for the Secretary's functions and powers, is also treated in the same way as information that is disclosed for the purposes of the Commissioner's functions and powers. Information acquired by the Secretary and Commissioner about the compliance of approved providers must be exchanged, to ensure effective and coordinated regulatory actions are taken in administering the powers under the Bill, under the framework established by the *Aged Care Act 1997*, to promote the provision of quality care by approved providers.

2.41 The minister's response also argues that it is appropriate for disclosures made for the purpose of carrying out the functions and powers of the Commissioner and the secretary to be excluded from the general prohibition on using, recording or disclosing protected information,[20] as well as from the requirement that onward disclosures of information be made for the same purposes as the original disclosure.[21] The response states that imposing such restrictions on disclosures made for the purposes of the Commissioner's functions and powers could frustrate the performance of those powers and indicates this could undermine the legitimate objectives of the bill.

2.42 On balance, in light of the information provided by the minister, the powers of disclosure in proposed sections 56 and 57 may constitute a proportionate limitation on the right to privacy. However, it is noted that much will depend on the manner in which those powers are exercised in practice.

2.43 In relation to the powers in proposed section 58, without further information, it is unclear that these powers constitute a proportionate limitation on the right to privacy. In particular, it is noted that proposed section 58(4) includes a power for the minister to publish a report or document relating to the Commissioner's functions. The publication of a report or document containing personal or sensitive information limits the privacy of those to whom that information relates. In this respect, it is noted that there do not appear to be any restrictions on the exercise of the minister's powers. This raises questions as to

20 Proposed section 60(1).

21 Proposed section 62.

whether there are sufficient safeguards to ensure that the limitation is the least rights restrictive approach.

Committee response

2.44 The committee thanks the minister for his response.

2.45 Based on the information provided by the minister, the committee considers that the information-sharing powers in proposed sections 56 and 57 may be compatible with the right to privacy.

2.46 The committee is unable to conclude whether proposed section 58 is compatible with the right to privacy.

Reverse evidential burden of proof

2.47 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 Act or the rules.

2.48 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.

2.49 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.

2.50 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: initial analysis

2.51 Article 14(2) of the ICCPR 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. The initial analysis noted that the defendant bears an evidential burden in relation to the matters in proposed subsections 60(3) and (4). Those provisions therefore engage and limit the right to be presumed innocent.

2.52 The initial analysis noted that the statement of compatibility does not identify that the reverse burden offences in the bill engage and limit the right to be presumed innocent, and so does not provide an assessment of whether any limitation is justified under international human rights law. The initial analysis stated that relevant information regarding whether the measures constitute a permissible limitation on the right to be presumed innocent included whether the matters for which the defendant would be required to raise evidence includes information that would be peculiarly within the knowledge of the defendant. The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) at pp. 7-8.[22]

2.53 The committee therefore sought 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.

Minister's response and analysis

2.54 The minister's response recognises that the measures engage and limit the right to be presumed innocent. In relation to the objectives of the measure, the minister's response states that the purpose of the measures is:

> …to give a level of confidence to those who are considering making a complaint or providing information to the Commissioner under clause 18, that information which identifies a particular individual (among others) will not be made public, used or disclosed for an unrelated purpose. Given the Commissioner's functions are ultimately reliant on these exchanges for its [*sic*] effective function, it is critical that there is a high level of confidence in the standards of protection afforded.

2.55 Maintaining public confidence in the processes for making complaints and giving information to the Commissioner is likely to be a legitimate objective for the purposes of international human rights law, noting in particular the advice that the Commissioner's functions are ultimately reliant on these processes.

2.56 The minister's response further states that reversing the onus of proof in relation to the relevant defences is necessary to promote information protection in

22 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 7-8 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

the exercise of powers under the bill and the Aged Care Act. In this respect, the response argues that:

> [b]y placing the onus of proof on the defendant to either establish the existence of an authorisation specified under subclause (3) or that the disclosure was made to a person specified under subclause (4), a defendant will be held to a high standard of accountability that requires the defendant to ensure that his or her use, recording or disclosure of protected information is at all times properly authorised or disclosed to authorised persons.

2.57 This information indicates that the measures are likely to be effective to achieve (that is, rationally connected to) their stated objectives.

2.58 In relation to the proportionality of the measures, the minister's response states that:

> Imposing…[the evidential burden of proof] on the defendant is also appropriate given the defendant is best placed to demonstrate the applicability of an exception covered under subclauses 60(3) and (4). Disclosures which qualify for exception, including disclosures to specified persons, or disclosure made on the authority provided by the person or body to whom it relates, or under the authority of a specified law, concern matters directly connected to the defendant's conduct.
>
> In particular, in circumstances where the excluded conduct is carried out in the course of performing functions or exercising powers under the new Act or Rules as per subclause 60(1), the defendant would, as a matter of course, be expected to maintain the appropriate records relating to the purpose of the record, use or disclosure of protected information, or authority which may have been obtained to record, use or disclose this information…
>
> Reversing the onus only requires the defendant to adduce evidence that a defendant is expected to be able to produce, which demonstrates a possibility that an exception exists. It would then be incumbent on the prosecution to refute beyond a reasonable doubt that the disclosure occurred without authorisation, or was disclosed to an unspecified person, together with the other elements of the offence.

2.59 It is acknowledged that the defences in proposed sections 60(3) and (4) impose an evidential rather than a legal burden on the defendant, and that the prosecution will still be required to prove the other elements of the offence beyond reasonable doubt. This assists the proportionality of the measures. Further, it is noted that the class of information the offence captures is restricted to 'protected information' and to persons who have obtained such information in the course of performing functions or exercising powers under the Act or the rules. That is, persons, in respect of whom the offence applies, are in a position of authority and trust. In this context, the sensitive nature of 'protected information' and the class of

persons to which the offence applies assists with the proportionality of the limitation.

2.60 Where relevant matters are peculiarly within the knowledge of the defendant, this may also be relevant to whether reversing the evidential burden of proof constitutes a proportionate limitation on the right to be presumed innocent. As the minister's response states, the defendant may be 'best placed' to provide evidence that disclosure occurred in the performance of their functions or with authority from the person to whom the information relates. However, it is not clear whether it would be peculiarly within the knowledge of the defendant whether the recording, use or disclosure of information was authorised by legislation.[23] However, noting the purpose of the measures to provide confidence to persons who may wish to make complaints that their personal information will not be inappropriately disclosed, on balance the measures may be a proportionate limitation on the right to be presumed innocent in their particular legislative context.

Committee response

2.61 The committee thanks the minister for his response and has concluded its examination of this issue.

2.62 Based on the information provided by the minister and the above analysis, the committee considers that the measures may be compatible with the right to be presumed innocent.

23 Proposed paragraph 60(3)(c).

Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018 [F2018L00464]

Purpose	Makes guidelines for the Secretary of the Department of Education and Training or their delegate in exercising their power under paragraph 168(1)(a) of the *A New Tax System (Family Assistance) (Administration) Act 1999* to disclose certain information if it is necessary in the public interest to do so.
Portfolio	Education
Authorising legislation	*A New Tax System (Family Assistance) (Administration) Act 1999*
Last day to disallow	15 sitting days after tabling (tabled House of Representatives 8 May 2018; tabled Senate 8 May 2018)
Rights	Privacy; rights of the child
Previous report	Report 7 of 2018
Status	Concluded examination

Background

2.63 The committee first reported on the instrument in its Report 7 of 2018 (14 August 2018) and requested a response from the minister by 28 August 2018.[1]

2.64 The minister's response to the committee's inquiries was received on 11 October 2018. The response is discussed below and is available in full on the committee's website.[2]

Disclosure of personal information

2.65 The instrument sets out the circumstances in which the secretary may give a public interest certificate, which allows for the disclosure of information obtained by an officer in the course of their duties or in exercising their powers.[3] The secretary may give a public interest certificate if the following conditions are satisfied:

---

1 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 2-10. The committee previously considered the Family Assistance (Public Interest Certificate Guidelines) Determination 2015, which this determination replaces, in its *Twenty-eight Report of the 44th Parliament* and *Thirtieth Report of the 44th Parliament*.

2 The minister's response is available in full on the committee's scrutiny reports page: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports.

3 Pursuant to section 168(1)(a) of the *A New Tax System (Family Assistance) (Administration) Act 1999* (Administration Act).

- the information cannot reasonably be obtained from a source other than the department;
- the person to whom the information will be disclosed has sufficient interest in the information; and
- the secretary is satisfied that the disclosure is for at least one of a number of specified purposes, including:
    - to prevent, or lessen, a threat to the life, health or welfare of a person;
    - to make or support a proceeds of crime order;
    - to correct a mistake of fact in relation to the administration of a program of the department;
    - to brief a minister;
    - to assist with locating a missing person or in relation to a deceased person;
    - for research, statistical analysis and policy development;
    - to facilitate the progress or resolution of matters of relevance within the portfolio responsibilities of a department that is administering any part of the family assistance law or the social security law;
    - to contact a person in respect of their possible entitlement to recompense in a reparations process;
    - to enable a child protection agency of a state or territory to contact the parent or relative in relation to a child;
    - to facilitate the administration of public housing;
    - to ensure a child is enrolled in or attending school; or
    - to plan for, meet or monitor the infrastructure and resource needs in one or more schools.[4]

2.66 Section 6 of the instrument further provides that in giving a public interest certificate, other than to facilitate 'enforcement related activities', the secretary must have regard to:

- whether the person to whom the information relates is, or may be, subject to physical, psychological or emotional abuse; and
- whether the person in question may be unable to give notice of his or her circumstances because of age; disability; or social, cultural, family or other reasons.[5]

---

4 Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018, section 7.

2.67 Section 7(3) of the instrument provides that public interest certificates to facilitate 'enforcement related activities'[6] can be given 'in any case where the Secretary considers doing so is in the public interest', without any other limitation.[7] In other words, when issuing a public interest certificate for the disclosure of information to facilitate enforcement related activities, the secretary is not required to have regard to the factors prescribed in section 6 set out in paragraph [2.66] above. This is a new ground of disclosure that was not included in the 2015 Determination.[8]

Compatibility of the measure with the right to privacy: initial analysis

2.68 The right to privacy encompasses respect for informational privacy, including the right to respect for private and confidential information, particularly the use and sharing of such information and the right to control the dissemination of information.[9]

2.69 The initial analysis noted that the disclosure of protected information (including personal information) pursuant to a public interest certificate engages and limits the right to privacy. The statement of compatibility acknowledges that this right is engaged and limited by the 2018 Determination.

2.70 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, they must seek to achieve a legitimate objective and be rationally connected (that is, effective to achieve) and proportionate to that objective.

2.71 The statement of compatibility only provided an assessment of the compatibility with the right to privacy in relation to the issuing of public interest certificates to disclose information to facilitate 'enforcement related activities'. It did

---

5 Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018, section 6.

6 'Enforcement related activities' is defined in the *Privacy Act 1988* (Privacy Act) to mean: the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; the conduct of surveillance activities, intelligence gathering activities or monitoring activities; the conduct of protective or custodial activities; the enforcement of laws relating to the confiscation of the proceeds of crime; the protection of the public revenue; the prevention, detention, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations; or the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders.

7 Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018, subsection 7(3).

8 Explanatory Statement (ES), p. 1.

9 International Covenant on Civil and Political Rights, article 17.

not assess whether disclosure of personal information for the other purposes set out at [2.65] above constituted a permissible limitation on the right to privacy.

2.72 In relation to the legitimate objective of allowing information to be disclosed to facilitate 'enforcement related activities', the committee sought further information as to whether and how the measure addressed a pressing and substantial concern. The initial analysis also raised questions as to whether each of the circumstances in which information could be disclosed pursued a legitimate objective, was rationally connected and proportionate.

2.73 The full initial human rights analysis is set out at *Report 7 of 2018* (14 August 2018) at pp. 2-10.[10]

2.74 The committee therefore sought the advice of the minister as to:

- whether each of the proposed purposes for which information can be shared is aimed at achieving a legitimate objective for the purposes of international human rights law;
- how the measure is effective to achieve (that is, rationally connected to) that objective; and
- whether the limitation on the right to privacy is proportionate to the achievement of each objective (including whether the purposes for which information can be disclosed are sufficiently circumscribed, and what safeguards apply to the collection, storage and disclosure of personal and confidential information).

Minister's response and analysis

2.75 In relation to whether the conduct of 'enforcement related activities' is capable of constituting a legitimate objective for the purposes of international human rights law, justifying the disclosure powers for this purpose, the minister's response explains:

> The former provision necessitated a number of practical and technical hurdles to be dealt with and considered before a public interest certificate could be made. In particular, the earlier provision:
>
> - required a delegate to consider or be advised of whether the enforcement purpose related to the enforcement of a criminal offence or civil penalty defined according to thresholds of either:
>   - indicatable offences punishable by 2 or more years imprisonment

10 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 2-10 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_7_of_2018.

- at least 40 penalty units

- alternatively required consideration of whether the disclosure would have a significant adverse effect on "public revenue"

- was tied to restrictions in section 7 which meant that disclosure could not occur where the information may have been able to be obtained from another source (s7(1)(a)) and after consideration of the "sufficient interest" of the potential recipient of the information.

In practice, these restrictions affected the Department of Education and Training's capacity to respond to urgent and legitimate requests from an enforcement body, including police, even where a delegate was assured that disclosure was in the public interest for an investigatory or emergency purpose related to their enforcement power under law. In particular, disclosure had to be delayed until:

- the delegate was assured that the disclosure was for "enforcement" of the law, rather than for investigatory purposes or other legitimate purposes within the scope of the definition of "enforcement related activity" as set out in the *Privacy Act 1988* and in respect of which the same personal information would lawfully be able to be disclosed under APP 6.2(e);

- the delegate was able to confirm or be advised of the penalty that would be imposed upon enforcement (whether summary or indictable and the penalty that might be imposed upon sentencing), even where the disclosure was being made to ensure that police or other enforcement bodies were able to assess which penalty may be able to be enforced;

- the delegate considered the range of other possible sources of the information;

- for disclosures in respect of "public revenue" issues, the delegate needed to consider whether the act to be prevented was related to receipt of money by the Commonwealth (revenue) as opposed to the prevention of adverse (including unlawful) expenditure.

These restrictions also delayed any disclosure designated to permit those important disclosures otherwise prohibited by section 167 of the *A New Tax System (Family Assistance) (Administration) Act 1999,* including where the disclosure was made to comply with a subpoena in respect of court proceedings.

2.76 In light of this information, it appears that the broad powers to disclose personal information for 'enforcement related activities' have been designed to manage the issues and risks with the previous regulatory approach identified in the minister's response. Consequently, it appears that the measures are designed to address a pressing or substantial concern, and are therefore likely to be rationally

connected to a legitimate objective for the purposes of international human rights law.

2.77 The minister's response also provides additional information relevant to the proportionality of the measures in achieving the legitimate objective outlined above. For example, in response to the committee's inquiries about how the measures interact with the *Privacy Act 1988* (Privacy Act), the minister's response explains:

> Any disclosure under new section 9 will authorise a disclosure by law for the purposes of APP 6.2(b). The Privacy Act 1988 also provides Commonwealth agencies with the ability to use or disclose 'personal information' where the agency reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (see APP 6.2(e) in Schedule 1 to the Privacy Act 1988). New section 9 specifically defines the terms "enforcement related activity" and "enforcement body" consistently with this provision.
>
> The reference in the statement of compatibility referred to by the Committee with respect to how "key requirements of the Privacy Act 1988 will still apply", reflects that in any case where the protected information is also "personal information" for the purposes of the Privacy Act 1988 where the recipient of the information where they are an APP entity:
>
> - will need to ensure that their collection of the information is consistent with the collection obligations stated in APP 3 and 5, including the obligation to ensure that any collection is reasonably necessary for, or directly related to, one or more of the entity's functions or activities;
> - for the purposes of the Privacy Act 1988, will still be subject to obligations in respect of the security of the information as set out in APP 11;
> - will also be subject to other obligations in the APPs including in respect of quality, access and correction of the received information.

2.78 Further, regarding the disclosure of personal information to 'contracted service providers', the minister's advice also explains that:

> … [D]ue to section 958 of the Privacy Act 1988, in any case where the recipient of disclosed information is a "contracted service provider" (as noted by the Committee in para 1.20 of the Report), the recipient is required to be under contractual obligations to adhere to the APP as if they were an APP entity under the terms of that provision.

2.79 The minister's response therefore addresses the committee's concern that 'contracted service providers' might not be subject to any relevant safeguards. The minister's response also clarifies the application of the Australian Privacy Principles (APPs) in the Privacy Act. However it is noted that the APPs and the Privacy Act are

not a complete answer to concerns about interference with the right to privacy for the purposes of international human rights law, due to exceptions to the prohibitions on the disclosure of personal information.[11]

2.80 Regarding the concerns in the initial analysis about the adequacy of safeguards where personal information is disclosed to recipients who are not subject to the Privacy Act, the minister's response states:

> Even where recipients of information may not be subject to the Commonwealth Privacy Act 1988, the definition of "enforcement body" for practical purposes extends only to Commonwealth and State/Territory agencies or authorities where the recipient will almost certainly be subject to obligations (including as relevant to collection and security) in either Commonwealth privacy legislation or in similar State or Territory privacy legislation.

2.81 In this regard, noting the potential for variation across jurisdictions, it would have been useful if the minister's response had clarified which specific safeguards are in place to protect personal information disclosed to these recipients.

2.82 The minister's response also notes that, in addition to the safeguards provided by the Privacy Act:

> … [W]here the recipient is an agency whose powers derive from legislation that contains its own secrecy provisions (such as the Australian Taxation Office), the receipt of the information will also trigger those provisions (such as those set out in the Taxation Administration Act 1953) and the received information will therefore become subject to information protections that apply the legislation administered by the receiving agency.

2.83 This example helpfully indicates that safeguards in addition to the Privacy Act may also apply to certain prospective recipients of personal information disclosed under the instrument.

2.84 While the minister's response focuses on the human rights compatibility of section 9 of the instrument, it also provides the following information in relation to the compatibility of other provisions in the instrument:

> …[T]he other measures, which remain unchanged as stated in previous guidelines, also promote, or are reasonably proportionate to achieving, human rights objectives. In particular:
>
> - Section 8, which permits disclosures that are necessary to prevent, or lessen a threat to life, health or welfare is consistent with and promotes a number of human rights, including a range of liberties

11 See, for example, Parliamentary Joint Committee on Human Rights, *Report 1 of 2018* (6 February 2018), p. 87; Parliamentary Joint Committee on Human Rights, *Report 3 of 2018* (27 March 2018), p. 202.

and rights outlined in the International Covenant on Civil and Political Rights

- Section 10, which helps facilitate existing proceeds of crime legislation, is proportionate to the objectives of that legislation which is consistent with the legitimate human rights purposes of the criminal law
- Section 11 (mistake of fact) which is consistent with ensuring that human rights are not compromised due to error
- Sections 12 and 17, which facilitates the Minister's role and the Department's role as the Minister and Department responsible for administering the legitimate purposes of family assistance legislation, consistently with the right to social security and the right to education
- Section 13, which supports the legitimate human rights purposes of courts, inquiries or Commissions in respect of assisting with the identity of missing persons where the revelation of identity is necessary in the public interest
- Section 14, which relates wholly to information about deceased persons
- Sections 15, 16, 18, 23 and 24, which are consistent with ensuring public policy development and administration for the purposes of furthering education and early childhood outcomes for Australians
- Section 19, which is consistent with the public policy purposes of the Family Responsibilities Commission
- Section 20, which is consistent with the human rights objectives of reparations or compensation
- Section 21, which is consistent with the rights of the child that are protected by child protection agencies
- Section 22, which helps facilitate the just and equitable administration of public housing, consistent with the right to an adequate standard of living, set out in the International Covenant on Economic, Social and Cultural Rights.

2.85 The minister's response reiterates that similar provisions to those listed above have been included in public interest disclosures guidelines since 'the enactment of the *A New Tax System (Family Assistance) (Administration) Act 1999* and commencement in 2000'.

2.86 In this regard, it is noted that the replication of provisions in a previous instrument, or similar instruments, will not, of itself, address concerns regarding the human rights compatibility of an instrument.

2.87 The minister's response indicates that some of the other measures in part 2 of the instrument are designed to promote human rights. While protecting the

human rights of others may be a legitimate objective under international human rights law, it would have been useful if the response had provided evidence as to how the relevant measure addresses a substantial and pressing concern. 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.

2.88 Noting the application of the Privacy Act or similar legislation to the majority of prospective recipients of personal information under the instrument, including contracted service providers, and the additional, potential application of secrecy provisions on certain prospective recipients, on balance, and in the context of these particular measures, the measure may be a proportionate limitation on the right to privacy. However, given the broad scope of some of the purposes for which public interest certificates may be issued under the guidelines, much may depend on how the guidelines are applied in practice.

Committee response

2.89 The committee thanks the minister for his response and has concluded its examination of this issue.

2.90 Based on the information provided, the measure may be compatible with the right to privacy. However, the committee notes that much will depend on how the guidelines are applied in practice, and the safeguards applicable to the relevant recipient.

Disclosure of personal information relating to homeless young people

2.91 Part 3 of the instrument applies to the disclosure of information relating to homeless young people.[12] It provides that the secretary may issue a public interest certificate for the disclosure of such information if satisfied:

- the information cannot reasonably be obtained from a source other than the department;
- the disclosure will not result in harm to the homeless young person; and
- the disclosure is for one of the following purposes:
    - the information is about a homeless young person's family member and the secretary is satisfied the homeless young person or a family member has been subjected to abuse or violence (abuse or violence);[13]

12 Subsection 25(2) of the 2018 Determination defines 'homeless young person' as a person under 18 years of age who has sought assistance on the ground of being homeless.

13 Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018, section 27.

- the disclosure is necessary to verify qualifications for a payment under family assistance law or a social security payment on the grounds of being a homeless person (verification for payment);[14]
- the disclosure will facilitate reconciliation between a homeless young person and his or her parent or parents (reconciliation);[15] and
- the disclosure is necessary to inform the parent or parents whether the homeless young person has been in contact with the Department of Education and Training or Human Services Department (assurance).[16]

2.92 Section 6 of the instrument, discussed at paragraph [2.66], also applies to the disclosure of information relating to homeless young people.

Compatibility of the measure with the right to privacy and the rights of the child: initial analysis

2.93 Children have special rights under human rights law taking into account their particular vulnerabilities. Children's rights are protected under a number of treaties, particularly the Convention on the Rights of the Child (CRC). All children under the age of 18 years are guaranteed these rights.

2.94 Article 16 of the CRC provides that children have the right not to be subjected to arbitrary or unlawful interference with their privacy.[17]

2.95 Article 3 of the CRC requires State parties to ensure that, in all actions concerning children, the best interests of the child are a primary consideration.[18]

2.96 The initial analysis noted that the disclosure of personal information relating to homeless young people under the age of 18 years engages and limits these rights. The statement of compatibility acknowledges that the 2018 Determination engages article 3 of the CRC generally. However, it does not specifically address how disclosure of personal information relating to homeless young people is compatible with article 3. It also does not address the limitation the measure imposes on the child's right to privacy.

2.97 The full initial human rights analysis is set out at *Report 7 of 2018* (14 August 2018) pp. 2-10.[19]

---

14 Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018, section 28.

15 Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018, section 29.

16 Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018, section 30.

17 Convention on the Rights of the Child, article 16.

18 Convention on the Rights of the Child, article 3(1).

2.98 The committee therefore sought the advice of the minister as to:

- whether the disclosure of personal information relating to homeless young people is aimed at achieving a legitimate objective for the purposes of international human rights law;
- how the measure is effective to achieve (that is, rationally connected to) that objective; and
- whether the limitation is a reasonable and proportionate measure for the achievement of that objective.

Minister's response and analysis

2.99 The minister's response provides the following information in relation to whether the measure is aimed at achieving a legitimate objective for the purposes of international law:

> Like all Australians, young homeless people are individuals entitled to protection and promotion of their human rights. In 1989, the Human Rights Commission conducted a National Inquiry into Homeless Children. It revealed that approximately 25,000 children and young people in Australia were homeless at that time, with many more at risk of homelessness or surviving in grossly inadequate housing. The inquiry demonstrated the link between homelessness and other problems such as unemployment, sexual abuse and exposure to violence. It also highlighted the lack of properly resourced and co-ordinated support services for homeless young people.
>
> To mitigate the disadvantage identified by the Human Rights Commission, the guidelines provide a framework to minimise the inequities suffered by Australia's most disadvantaged, including those in respect of whom information may be disclosed as necessary in the public interest under Part 3 of the 2018 Guidelines.

2.100 The response further explains that:

> From a human rights perspective, any disclosures made under Part 3 of the Guidelines are only permitted where the purpose of the disclosure is to assist the welfare and interests of young persons, consistently with the rights of the child and other rights of young persons to an adequate standard of living, including housing as set out in the ICESCR.

2.101 This response indicates that the measures are designed to redress the inequities experienced by disadvantaged homeless young people, by promoting their welfare and interests. This is likely to be a legitimate objective for the purposes of international human rights law. Measures which provide for personal information to

---

19 Parliamentary Joint Committee on Human Rights, Report 7 of 2018 (14 August 2018) pp. 2-10 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_7_of_2018.

be disclosed to facilitate the reconciliation of homeless young people with their families or provide assurances to their families, or which respond to abuse or violence experienced by the young person, or facilitate social security payments to them, appear to be rationally connected to the legitimate objective of promoting the welfare and best interests of children.

2.102 In the initial analysis, it was noted that under the determination the secretary can only issue a public interest certificate to disclose information relating to homeless young people if they are satisfied that the disclosure 'will not result in harm to the homeless young person'.[20] It was noted, however, that at international law, the right of a child to have his or her best interests taken as a primary consideration is broader than the right of a child not to be harmed. The child's best interests includes the enjoyment of the rights set out in the CRC, and, in the case of individual decisions, must be assessed and determined in light of the specific circumstances of the particular child'.[21] This raised concerns that there may be a less rights restrictive approach to the sharing of a homeless young person's personal information, such as requiring the decision-maker to be satisfied that the disclosure would be in the best interests of the child, rather than that the disclosure will not result in harm to the child.

2.103 In relation to the proportionality of the measure, and the availability of less rights restrictive approaches, the minister's response states:

> The Committee will note, in the context of its comments paragraph 1.30 of the Report, that the avoidance of "harm" is only one of the required elements before a disclosure is permitted under section 26 of the 2018 Guidelines. As set out in that provision, the information must be unable to be obtained from a source other than department and the disclosure must be for the purposes of the administration of the *Education and Care Services National Law,* the Family Responsibilities Commission, reparations or child protection agencies.

2.104 However, it remains unclear whether other aspects of the child's best interests, including their enjoyment of the rights set out in the CRC, and the requirement that individual decisions 'must be assessed and determined in light of the specific circumstances of the particular child', will also be taken into account by a decision-maker in determining whether to disclose information relating to a homeless young person. While the requirement to consider 'harm' to the child may, as a matter of practice and in most circumstances, involve consideration of the best interests of the child, this may not necessarily be the case. This is because, as noted

---

20 Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018, section 26(1)(a).

21 UN Committee on the Rights of the Child, General comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration, UN Doc CRC/C/GC/14 (29 May 2013), p. 3.

earlier, under international law the right of a child to have his or her best interests taken as a primary consideration is broader than the right of a child not to be harmed.

2.105 Finally, the minister's response also explains that the equivalent measures relating to homeless young people have 'been part of various iterations of public interest guidelines made under section 169 of the *A New Tax System (Family Assistance) (Administration) Act 1999* since 2002'. As noted at [2.86], the replication of provisions in a previous instrument, or similar instruments, will not, of itself, address concerns regarding the human rights compatibility of an instrument.

Committee response

2.106 The committee thanks the minister for his response and has concluded its examination of this issue.

2.107 The preceding analysis indicates that, in most circumstances, the requirement that the disclosure will not result in harm to the homeless young person will ensure that any disclosure of information relating to homeless young people will be compatible with the rights of the child. However, as currently framed, there is a risk in some individual cases that the measure may operate in a way that may be incompatible with the obligation to consider the best interests of the child.

National Disability Insurance Scheme (Restrictive Practice and Behaviour Support) Rules 2018 [F2018L00632]

Purpose	Provides oversight relating to behaviour support, monitoring the use of restrictive practices within the National Disability Insurance Scheme (NDIS)
Portfolio	Social Services
Authorising legislation	*National Disability Insurance Scheme Act 2013*
Last day to disallow	15 sitting days after tabling (tabled Senate 18 June 2018)
Rights	Torture, cruel, inhuman and degrading treatment or punishment; liberty; rights of persons with disabilities
Previous reports	Reports 7 and 9 of 2018
Status	Concluded examination

Background

2.108 The committee first reported on the instrument in its *Report 7 of 2018*, and requested a response from the minister for social services by 28 August 2018.[1] The minister's initial response to the committee's inquiries was received on 28 August 2018, and was considered by the committee in its *Report 9 of 2018*.[2]

2.109 In *Report 9 of 2018,* the committee concluded that the record keeping requirements are likely to be compatible with the right to privacy. However, the committee sought further additional information from the minister in relation to the prohibition on torture, cruel, inhuman or degrading treatment or punishment and the rights of persons with disabilities in respect of conditions relating to the use of restrictive practices by NDIS providers. The committee requested a response by 26 September 2018.

1 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 39-47 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_7_of_2018.

2 Parliamentary Joint Committee on Human Rights, *Report 9 of 2018* (11 September 2018) pp. 7-19 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_9_of_2018.

2.110 The minister's response to the committee's inquiries was received on 23 October 2018. The response is discussed below and is available in full on the committee's website.[3]

Conditions relating to the use of regulated restrictive practices by NDIS providers

2.111 The National Disability Insurance Scheme (Restrictive Practice and Behaviour Support) Rules 2018 (Rules) set out the conditions of registration that apply to all registered National Disability Insurance Scheme (NDIS) providers who use 'regulated restrictive practices' in the course of delivering NDIS support. A 'regulated restrictive practice' involves any of the following:

(a) seclusion, which is the sole confinement of a person with disability in a room or a physical space at any hour of the day or night where voluntary exit is prevented, or not facilitated, or it is implied that voluntary exit is not permitted;

(b) chemical restraint, which is the use of medication or chemical substance for the primary purpose of influencing a person's behaviour. It does not include the use of medication prescribed by a medical practitioner for the treatment of, or to enable treatment of, a diagnosed mental disorder, a physical illness or a physical condition;

(c) mechanical restraint, which is the use of a device to prevent, restrict, or subdue a person's movement for the primary purpose of influencing a person's behaviour but does not include the use of devices for therapeutic or non-behavioural purposes;

(d) physical restraint, which is the use or action of physical force to prevent, restrict or subdue movement of a person's body, or part of their body, for the primary purpose of influencing their behaviour. Physical restraint does not include the use of a hands-on technique in a reflexive way to guide or redirect a person away from potential harm/injury, consistent with what could reasonably be considered the exercise of care towards a person;

(e) environmental restraint, which restricts a person's free access to all parts of their environment, including items or activities.[4]

2.112 The Rules prescribe different conditions of registration of NDIS providers depending on the regulation of restrictive practices in a state or territory. Broadly,

---

3 The minister's response is available in full on the committee's scrutiny reports page: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports.

4 National Disability Insurance Scheme (Restrictive Practice and Behaviour Support) Rules 2018 (Rules), section 6.

for those states and territories that prohibit the use of a restrictive practice, it is a condition of registration of the NDIS provider that the provider must not use the restrictive practice in relation to a person with a disability.[5] However, where the practice is not prohibited but rather is regulated by an authorisation process,[6] registration is conditional upon the use of the regulated restrictive practice being authorised (other than a 'single emergency use'[7]), and the provider must lodge with the NDIS Quality and Safeguards Commissioner (Commissioner) evidence of that authorisation as soon as reasonably practicable after the use of the regulated restrictive practice.[8]

2.113 The Rules also prescribe the conditions of registration where a 'behaviour support plan' is used in relation to a regulated restrictive practice. Behaviour support plans may only be developed by a NDIS behaviour support practitioner[9] and are subject to certain conditions, including the requirement that all reasonable steps be taken to reduce and eliminate the need for the use of regulated restrictive practices.[10] In particular, section 21 of the Rules sets out the minimum content of behaviour support plans containing regulated restrictive practices, and provides that the registration of specialist behaviour support providers[11] is subject to the condition a regulated restrictive practice must:

- be clearly identified in the behaviour support plan;
- if the state or territory in which the regulated restrictive practice is to be used has an authorisation process – be authorised in accordance with that process;

---

5 Rules, section 8.

6 The Rules note that an authorisation process may, for example, be a process under relevant State or Territory legislation or policy or involve obtaining informed consent from a person and/or their guardian, approval from a guardianship board or administrative tribunal or approval from an authorised state or territory officer.

7 'Single emergency use' is not defined in the instrument but is described in the explanatory statement (ES) as 'the use of a regulated restrictive practice in relation to a person with disability, in an emergency, where the use of a regulated restrictive practice has not previously been identified as being required in response to behaviour of that person with disability previously'. See, ES, p. 9.

8 Rules, section 9.

9 'Behaviour support practitioner' is defined in section 5 of the Rules to mean a person the Commissioner considers is suitable to undertake behaviour support assessments (including functional behavioural assessments) and to develop behaviour support plans that may contain the use of restrictive practices.

10 See sections 18-20.

11 A specialist behaviour support provider is defined in section 5 of the Rules to mean a registered NDIS provider whose registration incudes the provision of specialist behaviour support services.

- be used only as a last resort in response to risk of harm to the person with disability or others, and after the provider has explored and applied evidence-based, person-centred and proactive strategies; and
- be the least restrictive response possible in the circumstances to ensure the safety of the person and others; and
- reduce the risk of harm to the person with disability or others; and
- be in proportion to the potential negative consequence or risk of harm; and
- be used for the shortest possible time to ensure the safety of the person with disability or others.[12]

2.114 Where an NDIS provider provides support or services in accordance with a behaviour support plan that includes the use of a restrictive practice, registration as a provider is conditional on the regulated restrictive practice being used in accordance with the behaviour support plan.[13]

2.115 The Rules also set out registration requirements where the use of a regulated restrictive practice may be unauthorised by state or territory law but be in accordance with a behaviour support plan, and vice versa. In particular:

- where the NDIS provider uses a regulated restrictive practice pursuant to an authorisation process but not in accordance with a behaviour support plan (described as the 'first use' in the Rules), and the use of such practices will or is likely to continue, the NDIS provider must take all steps to develop an interim behaviour support plan within one month after the use of the regulated restrictive practice and a comprehensive behaviour support plan within six months;[14]
- where the NDIS provider uses a regulated restrictive practice that is not authorised pursuant to an authorisation *and* is not in accordance with a behaviour support plan, and the use of such practices will or is likely to continue, the NDIS provider must (relevantly) obtain authorisation for the ongoing use of the regulated restrictive practice and take all reasonable steps to develop an interim behaviour support plan within one month and a comprehensive behaviour support plan within six months;[15] and
- where the NDIS provider uses a regulated restrictive practice that is not in accordance with a behaviour support plan but authorisation is not required in the state or territory, and the use will or is likely to continue, the NDIS

12 Rules, section 21(3).

13 Rules, section 10.

14 Rules, section 11.

15 Rules, section 12.

provider must take all reasonable steps to develop an interim behaviour support plan within one month and a comprehensive behaviour support plan within six months that covers the use of the regulated restrictive practice.[16]

Compatibility of the measures with multiple rights: initial analysis

Prohibition on torture, cruel, inhuman or degrading treatment or punishment

2.116 The committee's initial analysis raised concerns as to compatibility of the measures with the prohibition on torture, cruel, inhuman or degrading treatment or punishment. This is because the use of restrictive practices may amount to torture, cruel, inhuman or degrading treatment or punishment. The statement of compatibility acknowledged this right was engaged and acknowledged the concerns raised by the UN Committee on the Rights of Persons with Disabilities (UNCRPD) that Australia's use of restrictive practices may raise concerns in relation to this right and that UNCPRD has recommended Australia take immediate steps to end such practices.[17]

2.117 The committee raised concerns in relation to the safeguards in the Rules to ensure that regulated restrictive practices would not amount to torture, cruel, inhuman or degrading treatment or punishment. In particular, noting that Australia's obligations in relation to torture, cruel, inhuman or degrading treatment or punishment are absolute (that is, they can never be subject to limitations), there were questions as to whether safeguards in the Rules to ensure that regulated restrictive practices were 'proportionate' or the 'least rights restrictive response' would be sufficient in circumstances where the practice amounted to torture, cruel, inhuman or degrading treatment or punishment. The committee also noted that there was limited information provided in the statement of compatibility that addressed how the NDIS provider registration scheme would ensure that regulated restrictive practices used without authorisation or a behaviour support plan would be compatible with this right, and that there was limited information provided as to the regulation of a 'first use' and 'single emergency use' of a regulated restricted practice.

2.118 The committee therefore sought the advice of the minister as to the compatibility of the rules with this right, including:

- safeguards to prevent regulated restrictive practices (including 'first use' of a regulated restrictive practice and 'single emergency use' of a regulated

16 Rules, section 13.

17 The committee notes that the issue of using restrictive practices has been the subject of considerable discussion over many years and is a longstanding human rights issue. See: Committee on the Rights of Persons with Disabilities, *Concluding observations on the initial report of Australia, adopted at its tenth session,* CRPD/C/AUS/CO1 (2013) [31]-[36].

restrictive practice) amounting to torture, cruel, inhuman or degrading treatment or punishment; and

- whether the rules could be amended to include safeguards to prevent regulated restrictive practices (in particular 'first use' regulated restrictive practices and 'single emergency use' regulated restrictive practices) amounting to torture, cruel, inhuman or degrading treatment or punishment.

2.119 The full previous human rights analysis is set out at *Report 7 of 2018* (14 August 2018) pp. 42-44 and *Report 9 of 2018* (11 September 2018) pp. 10-13.[18]

Multiple rights relating to the protection of persons with disabilities

2.120 The committee's initial analysis also raised questions as to the compatibility of the use of regulated restrictive practices with a number of rights under the Convention on the Rights of Persons with Disabilities (CRPD), including the right to equal recognition before the law and to exercise legal capacity,[19] the right of persons with disabilities to physical and mental integrity on an equal basis with others,[20] the right to liberty and security of the person,[21] the right to freedom from exploitation, violence and abuse[22] and the right to freedom of expression and access to information.[23] The statement of compatibility acknowledged that the use of restrictive practices may engage these rights.

2.121 While each of these rights may be subject to permissible limitations providing they addresses a legitimate objective, are effective to achieve (that is, rationally connected to) that objective and are a proportionate means to achieve that objective, the committee raised questions as to whether the Rules met these criteria.

2.122 In relation to whether the measures pursued a legitimate objective and were rationally connected to that objective, the initial analysis noted that the objective of the Rules is identified in the statement of compatibility as overseeing behaviour

---

18 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 42-44 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_7_of_2018; Parliamentary Joint Committee on Human Rights, *Report 9 of 2018* (11 September 2018) pp. 10-13 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_9_of_2018.

19 CRPD, article 12.

20 CRPD, article 17.

21 CRPD, article 14; ICCPR, article 9; Convention on the Rights of the Child, article 37.

22 CRPD, article 16.

23 CRPD, article 21.

support and 'the reduction and elimination of restrictive practices in the NDIS'.[24] The initial analysis stated that while this is capable of being a legitimate objective for the purposes of international human rights law, the statement of compatibility provides limited information about this objective in context of the particular measure. This raised a particular concern as the Rules regulate the use of restrictive practices, that is, are directed toward oversight of their use rather than explicitly eliminating their use.

2.123 There were also questions as to proportionality, noting that there were some safeguards identified in the Rules, including a requirement that the use of any regulated restrictive practice pursuant to a behaviour support plan be the least restrictive, as a matter of last resort and proportionate. However, it was not clear who determined whether a practice was the 'least restrictive' and 'proportionate', the criteria relevant to making such a determination, and whether there was any oversight of such a determination. There were also similar concerns as those raised in the context of the prohibition on torture, cruel, inhuman or degrading treatment or punishment, relating to the lack of information as to safeguards where the use of a regulated restrictive practice occurred not in accordance with a behaviour support plan or without authorisation, or where the use was a 'single emergency use' or 'first use'.

2.124 The committee therefore sought the advice of the minister as to the compatibility of the use of regulated restricted practices with rights related to persons with disabilities, including:

- whether the measures were aimed at achieving a legitimate objective for the purposes of human rights law;
- how the measures would be effective to achieve (that is, rationally connected to) that objective;
- whether the measures are proportionate to achieve the stated objective;
- information as to safeguards to ensure that the 'first use' of a regulated restrictive practice and any 'single emergency use' occurs in a manner that is compatible with human rights;
- whether the Rules could be amended to include safeguards to ensure regulated restrictive practices (in particular 'first use' regulated restrictive practices and 'single emergency use' regulated restrictive practices) occur in a manner that is compatible with the human rights discussed in the preceding analysis.

24 ES, p. 1; Statement of compatibility (SOC), p. 32.

Minister's first response and committee's request for further information

2.125 The minister's initial response provided some information as to the regulation of restrictive practices. The minister's first response emphasised that the Rules do not authorise a registered NDIS provider to use a restrictive practice, but rather the Rules 'seek to achieve a reduction and elimination of restrictive practices in the NDIS by promoting behaviour support strategies including positive behaviour support and imposing significant conditions around the use of restrictive practices'.

2.126 The minister's first response also outlined some safeguards in relation to the use of restrictive practices, including the minimum requirements of behaviour support plans, the requirements not to use a restrictive practice where it has been prohibited in the state or territory (section 8), and the requirement that a restrictive practice be authorised in accordance with any relevant state or territory process in relation to the use of that practice (section 9).The committee noted that these were important safeguards in relation to the compatibility of the measures with human rights.

2.127 The response also provided further information that a 'single emergency use' is a reportable incident within the meaning of the National Disability Insurance Scheme (Incident Management and Reportable Incidents) Rules 2018, which indicated that there are some safeguards in place to regulate and monitor single emergency use of restrictive practices.

2.128 However, the minister's first response otherwise did not address the committee's inquiries in relation to the compatibility of the measure with Australia's obligation not to subject persons to torture, cruel, inhuman or degrading treatment or punishment. Further, the minister's response otherwise did not address the committee's inquiries in relation to the compatibility of the measure with the rights relating to the protection of persons with disabilities. In particular, the minister's response did not provide information in relation to the safeguards in place to ensure that the 'single emergency use' referred to in section 9(2)(a) does not occur in circumstances that would be incompatible with the human rights engaged, nor was there sufficient information to address the committee's inquiries in relation to the 'first use' of a restrictive practice in sections 11, 12 and 13 of the Rules.

2.129 The committee therefore sought further information from the minister as to the compatibility of the measures with Australia's obligation not to subject persons to torture, cruel, inhuman or degrading treatment or punishment. In particular, the committee sought the advice of the minister as to the safeguards to prevent the 'first use' of a regulated restrictive practice in sections 11, 12 and 13 of the Rules and the 'single emergency use' in section 9(2) of the Rules amounting to torture, cruel, inhuman or degrading treatment or punishment.

2.130 The committee also sought further advice of the minister as to the compatibility of the measures with the rights of persons with disabilities, including:

- whether the measures are aimed at achieving a legitimate objective for the purposes of human rights law;
- how the measures are effective to achieve (that is, rationally connected to) that objective;
- whether the limitation on human rights is a reasonable and proportionate measure to achieve the stated objective;
- information as to safeguards to ensure that the 'first use' of a regulated restrictive practice in sections 11, 12 and 13 of the Rules and the 'single emergency use' in section 9(2) of the Rules occurs in a manner that is compatible with human rights;
- whether the Rules could be amended to include safeguards to ensure regulated restrictive practices (in particular 'first use' of a regulated restrictive practice in sections 11, 12 and 13 of the Rules and the 'single emergency use' in section 9(2) of the Rules) occur in a manner that is compatible with the human rights discussed in the preceding analysis.

Minister's further response and committee analysis

2.131 In relation to whether the limitation on the rights of persons with disabilities pursues a legitimate objective and is rationally connected to the objective, the minister's second response explains:

> The Rules aim to achieve the reduction and elimination of restrictive practices in the NDIS, consistent with the Convention on the Rights of Persons with Disabilities… The mechanism for achieving this is imposing conditions of registration on NDIS service providers to ensure the Commission has visibility of the use of restrictive practices and progress made in relation to the reduction and elimination of those practices in the NDIS.
>
> The Rules operate together with relevant processes under state and territory legislation and/or policy, to provide safeguards on the use of restrictive practices and ensure any limitation on the human rights of people with disability is reasonable and proportionate, while maintaining an objective of reducing and eliminating the use of restrictive practices.

2.132 Based on this information, it appears the measures pursue a legitimate objective and are rationally connected to this objective.

2.133 As noted earlier, the initial human rights analysis stated that there were some safeguards identified in the Rules, including a requirement in section 21 of the Rules that the use of any regulated restrictive practice pursuant to a behaviour support plan be the least restrictive, as a matter of last resort and proportionate. As noted in the analysis of the minister's first response, the requirements in section 21 of the Rules are important safeguards. However, it was not clear who determined whether a practice was the 'least restrictive' and 'proportionate', the criteria relevant to making such a determination, and whether there was any oversight of such a

determination. The minister's first and second response did not specifically address these matters.

2.134 The minister's second response does, however, provide further information as to the safeguards available at a state and territory level, and through the NDIS commission, relating to the use of restrictive practices. This is relevant to the proportionality of any limitation on the rights of persons with disabilities. While Australia's obligations in relation to the prohibition on torture, cruel, inhuman and degrading treatment or punishment are absolute and therefore cannot be limited (such that questions of proportionality do not arise), effective safeguards may assist in ensuring that the use of restrictive practices does not rise to the level of torture, cruel, inhuman and degrading treatment or punishment.

2.135 In relation to state and territory processes that would apply in relation to the use of restrictive practices:

> …Some states and territories expressly prohibit the use of particular restrictive practices. As also mentioned in Minister Tehan's letter dated 28 August 2018, the Rules state that an NDIS provider must not use a restrictive practice that has been prohibited by a State or Territory (section 8). The Commission has a range of regulatory powers that may be used in response to breaches of the Rules' requirements.
>
> Further, state and territory restrictive practice authorisation processes may impose specific conditions before a restrictive practice can be used. As agreed in the Council of Australian Governments (COAG) NDIS Scheme Quality and Safeguarding Framework (2016), states and territories are responsible for any arrangements for authorisation of use of a restrictive practice. As outlined in section 181H of the National Disability Insurance Scheme Act (2013), the Commission is working with states and territories to develop a regulatory framework that will provide safeguards around the use of restrictive practices, including the development of nationally consistent minimum standards. This may include, for example, states or territories adopting a restrictive practice authorisation process for the full cohort of NDIS participants and for all regulated restrictive practices. As noted above, state or territory conditions of authorisation can help ensure additional safeguards around the use of a restrictive practice, including before any 'first use'.
>
> A regulatory framework with nationally consistent minimum standards may also include the adoption of consistent definitions of restrictive practices across jurisdictions and agreement as to practices that should be expressly prohibited as they constitute torture, cruel, inhuman or degrading treatment or punishment.

2.136 Processes at the state and territory level, in particular the adoption of a consistent set of definitions as to restrictive practices that should be expressly prohibited due to their human rights concerns would be an important safeguard. However, noting the absolute nature of the prohibition on torture, cruel, inhuman or

degrading treatment or punishment, the processes at the state and territory level may not be a sufficient safeguard for the purposes of Australia's obligations if there were different levels of protection afforded across the states and territories. To that extent, a nationally consistent approach which prohibits restrictive practices that could amount to torture, cruel, inhuman and degrading treatment or punishment would be desirable from a human rights perspective.

2.137 More broadly, however, it appears that the safeguards relating to the use of restrictive practices pursuant to behaviour support plans in section 21 of the rules may be capable, in practice, of providing a sufficient safeguard from a human rights perspective where the use of a restrictive practice occurs in accordance with those plans. It would appear, for example, if the safeguards in section 21 were applied, it would be unlikely that the use of a restrictive practice pursuant to a behaviour support plan would rise to the level of constituting torture, cruel, inhuman or degrading treatment or punishment, because it is unlikely such a practice would be the least restrictive nor would it reduce the risk of harm. Similarly, it is also more likely that the use of such a practice in accordance with a behaviour support plan would be proportionate insofar as it was the least restrictive approach. However, noting that it remains unclear who determines whether a practice was the 'least restrictive' and 'proportionate', and the criteria relevant to making such a determination, much may depend on how use of regulated restrictive practices pursuant to behaviour support plans occurs in practice. In this respect, the Australian government may need to monitor these plans to ensure that their use is compatible with Australia's human rights obligations. This is of particular importance in relation to the prohibition on torture, cruel, inhuman and degrading treatment or punishment which, as noted earlier, cannot be limited in any circumstances.

2.138 As noted in the initial analysis, section 11 of the Rules provides that where a restrictive practice is used (the 'first use') in accordance with an authorisation process but not in accordance with a behaviour support plan, and the use of that practice is likely to continue, registration of the NDIS provider is subject to the condition that (relevantly) a behaviour support plan be developed. While this would mean that ongoing use would be subject to the requirements contained in a behaviour support plan (for example, the requirement that the practice must be the least restrictive response possible in the circumstances), it was not clear what restrictions are placed on, and what safeguards apply to, the 'first use'. The statement of compatibility and the minister's first response did not fully address this issue. Similarly, the statement of compatibility and the minister's first response did not provide information in relation to the safeguards in place to ensure that the 'single emergency use' referred to in section 9(2)(a) does not occur in circumstances where that use may amount to torture, cruel, inhuman or degrading treatment or punishment. While the minister's first response referred to reporting requirements in relation to the 'single emergency use' after it occurs, the committee raised questions as to whether this was sufficient, and whether there were other

safeguards reasonably available which could be put in place to protect the rights of persons with disabilities before the 'single emergency use' occurs.

2.139 In this respect, the minister's second response provides information relating to policy guidance that will be prepared as safeguards relating to the 'first use' and 'single emergency use' of a regulated restrictive practice. In addition to reiterating some of the safeguards outlined in the minister's previous response (namely, that restrictive practices were 'reportable incidents'), the minister's response further states:

> As highlighted in the explanatory statement, there are certain circumstances where immediate action needs to be taken to protect a person with disability or others from harm, as a duty of care. The unplanned use of a restrictive practice may be a one-off 'single emergency use', or the 'first use' of a restrictive practice where the person with disability has newly emerging and anticipated ongoing behaviours of concern. The circumstances around this unplanned use are highly variable and complex and cannot easily be codified in the Rules, however the NDIS Quality and Safeguards Commission (the Commission) will develop policy guidance for service providers around the ' first use' and 'emergency use' of a restrictive practice.
>
> This guidance will emphasise that any use of a restrictive practice must be in response to a risk of harm to the person or others; be the least restrictive response possible in the circumstances to ensure the safety of the person or others; reduce the risk of harm to the person or others; be in proportion to the potential negative consequence or risk of harm; and be used for the shortest possible time to ensure the safety of the person or others.
>
> …
>
> The Commission will also develop guidance as to restrictive practices that would constitute torture, cruel, inhuman or degrading treatment or punishment and which should not be used.

2.140 These safeguards in the form of policy guidance may be capable, in practice, of ensuring that any use of a regulated restrictive practice occurs in a manner compatible with the rights of persons with disabilities and with the prohibition on torture, cruel, inhuman and degrading treatment or punishment. However, for the purposes of international human rights law, policy guidance is less stringent than the protection of statutory processes (such as legislation) as the safeguards within that policy guidance can be removed, revoked or amended at any time and are not required as a matter of law. Such guidance may also not be subject to the same levels of scrutiny, or accountability as when the policies are enshrined in legislation.

2.141 Further, while it is acknowledged that circumstances around unplanned use of restrictive practices are highly variable and complex, it remains unclear why the safeguards proposed to be included in policy guidance around the use of 'first use'

and 'single emergency use' restrictive practices (for example, that it must be the least restrictive response possible and must be taken to protect the person with a disability or others from harm) cannot be included in legislation in a similar way to the use of restrictive practices in accordance with a behaviour support plan in section 21(3) of the Rules. This is particularly so in circumstances where Australia's obligations relating to torture, cruel, inhuman and degrading treatment or punishment are absolute.

Committee response

2.142 The committee thanks the minister for his response and has concluded its examination of this issue.

2.143 The preceding analysis indicates that the safeguards in section 21 of the National Disability Insurance Scheme (Restrictive Practice and Behaviour Support) Rules 2018 (Rules) relating to the use of restrictive practices pursuant to behaviour support plans may be capable, in practice, of being compatible with Australia's obligations relating to the prohibition on torture, cruel, inhuman and degrading treatment or punishment, and rights of persons with disabilities. However, it is recommended that the use of restrictive practices pursuant to behaviour support plans be monitored, noting that Australia has an obligation under international human rights law to reduce and eliminate such practices, and noting particularly the absolute nature of the prohibition on torture, cruel, inhuman and degrading treatment or punishment.

2.144 The preceding analysis indicates that there is a risk that the conditions relating to the 'first use' and 'single emergency use' of regulated restrictive practices by NDIS providers may be incompatible with the prohibition on torture, cruel, inhuman and degrading treatment or punishment, and rights of persons with disabilities. However, the policy guidance referred to in the minister's response may be capable, in practice, of addressing these concerns. It is noted that much will depend on how the policy guidance operates in practice.

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
Previous report	Report 11 of 2018
Status	Concluded examination

Background

2.145 The committee first reported on the bill in its *Report 11 of 2018*, and requested a response from the minister by 31 October 2018.[1]

2.146 The minister's response to the committee's inquiries was received on 2 November 2018. The response is discussed below and is available in full on the committee's website.[2]

Technical assistance notices, technical capability notices and technical assistance requests

2.147 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'[3] (provider) technical assistance notices,

1 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 24-73.

2 The minister's response is available in full on the committee's scrutiny reports page: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports

3 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.

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

2.148 Section 317L provides that the Director-General of Security (who leads the Australian Security Intelligence Organisation, ASIO) or the chief officer of an 'interception agency'[4] 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'[5] 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.[6] 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.[7]

Technical capability notice

2.149 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

4 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).

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

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

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

act or thing, or one or more acts or things of a kind determined by legislative instrument.[8]

Technical assistance request

2.150 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 voluntary.[9] 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.[10] 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'.[11]

Listed acts or things

2.151 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'.[12] Listed acts or things include, for example:

- removing one or more forms of electronic protection;[13]
- installing, maintaining, testing or using software or equipment;[14]
- ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format;[15]

---

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

9 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.

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

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

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

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

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

- facilitating access to customer equipment, software or a service;[16] and
- assisting with the testing, modification, development or maintenance of a technology or capability.[17]

2.152 It also includes an act or thing done to conceal the fact that any thing has been done covertly.[18]

Limitations on technical assistance notices and technical capability notices

2.153 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.[19] 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.[20]

2.154 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.[21]

Compatibility of the measure with the right to privacy and freedom of expression: initial analysis

2.155 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. The initial analysis noted that the measures engage the right to privacy because, as a consequence of the requests or notices, 'communications providers may facilitate law enforcement, security and intelligence agencies' access to private

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

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

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

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

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

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

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

communications and data where an underlying warrant or authorisation is present'.[22]

2.156 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. The statement of compatibility acknowledges that the measures may engage the right to freedom of expression 'by indirectly making some people more reluctant to use communications services'.[23]

2.157 The right to freedom of expression, as the statement of compatibility identifies,[24] may only be subject to restrictions which are rationally connected and proportionate to specific objectives: the protection of national security, public order, public health or morals. The right to privacy may also 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.

2.158 The statement of compatibility states that 'the bill pursues the legitimate objective of protecting national security and public order by addressing crime and terrorism',[25] specifically referring to 'terrorism, espionage, acts of foreign interference and serious and organised crime'.[26] The initial analysis stated that, in general terms, this would be capable of constituting a legitimate objective for the purposes of international human rights law. However, further information was required in order to determine the pressing and substantial concerns which the measures sought to address, as this was not addressed in the statement of compatibility. In particular, while the measures are directed towards addressing the 'challenges associated with encrypted communications', it was not clear whether the aspects of the measures that do not appear on their face to relate to decryption addressed a pressing or substantial concern. The initial analysis also raised questions as to whether aspects of the technical assistance requests restrict the right to freedom of expression on permissible 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'.[27] These grounds are broader than those on which the right to

22 Statement of compatibility (SOC), p. 9 [8].

23 SOC, p. 14 [40].

24 SOC, p. 14 [39].

25 SOC, p. 11 [16].

26 SOC, p. 11 [21].

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

freedom of expression can be validly restricted, and the statement of compatibility does not address if they are relevant to a valid ground.

2.159 The previous analysis also raised a number of questions in relation to whether the measures are rationally connected and proportionate to the stated objectives of the measures.

2.160 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 27-38.[28]

2.161 The committee therefore sought the advice of the minister as to the compatibility of the measures with the right to privacy and freedom of expression, 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 therefore represent the least rights restrictive approach to addressing the objectives of the bill;
    - safeguards relevant to the decision to issue technical assistance requests;

28 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 27-38 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

- 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 freedom of expression.

Minister's response and analysis

Legitimate objective

2.162 The minister's response explains that means to address encryption are necessary because:

> Measures employed by serious criminals and terrorists include, but are not limited to, communication devices with military grade encryption, remote-

> wipe capabilities, duress passwords, and secure cloud-based services. Beyond traditional communications platforms, online-only services now provide unprecedented secure connection and storage that enable the easy sharing, promotion and discussion of illicit material, such as child pornography. During development of the Bill, the government identified that 95 per cent of ASIO's most dangerous counter-terrorism targets use encrypted communications. Additionally, encryption has directly impacted around 200 operations conducted by the AFP in the last 12 months, all of which related to the investigation of serious criminality and terrorism offences. It is estimated that by 2020, all electronic communications of investigative value will be encrypted.

2.163 In relation to aspects of the measures that do not appear on their face to address a pressing or substantial concern, such as measures other than those directly related to overcoming encryption, the minister's response provides the following context:

> The increasing use of encryption is symptomatic of a more dramatic change in the communications environment. It is enabled by the growing digitisation of communications and presence of new providers who, unlike traditional domestic carriers and carriage service providers, remain largely unregulated in the Australian market. The new spread and scope of providers and the multiple different ways for communications to be constructed and transmitted require agencies to work with multiple other entities in the communications supply chain to achieve investigative results…
>
> Decryption is only part of a solution, and is not possible or desirable in some circumstances. It may provide a better outcome to allow agencies access to communications at a point where data is unencrypted (via schedule 2), have longer to examine a computer (schedule 3 and 4), or to receive technical assistance from a directly relevant designated communications provider (DCP)…
>
> [T]he 'problem' to be overcome is not the use of encryption itself, but the degradation of agencies' access to existing methods of obtaining communications. Viewed through this lens, the measures of all schedules of the Bill can be seen as directed towards the objective of assisting agencies to restore the balance of access to communications that Parliament has seen fit to provide.

2.164 The growing digitisation of communications, presence of new telecommunications providers who are largely unregulated, multiple different ways for communications to be constructed and transmitted, and the resulting degradation of agencies' access to existing methods of obtaining communications, appear to give rise to a pressing and substantial concern to be addressed by the measures. The minister's response explains how existing methods to address encryption are insufficient, as those methods are degraded by the new telecommunications environment. In light of this information, the measures in

Schedule 1 appear to pursue a legitimate objective for the purposes of international human rights law.

Rational connection

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

2.165 The initial analysis noted that the definition of 'interception agency' is very broad and includes state-based anti-corruption agencies. The initial analysis noted that it was 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,[29] was effective to achieve the objectives of the bill (namely, protecting national security and public order). In response to this, the minister identifies that:

> Interception agencies comprise the AFP, ACIC, ACLEI and State Police and anti-corruption agencies. These are the agencies that are charged, at both Commonwealth and Federal levels with the prevention, investigation and detection of serious crime (including national security threat) and the protection of the public…
>
> The Bill is designed to address the impact that a rapidly evolving communications environment characterised by increasing encryption is having on the ability of agencies to exercise their lawful functions. Interception agencies are those very agencies that are experiencing this problem most acutely and it is their existing powers of interception and surveillance are impacted by the move into the digital era. It is appropriate that the same agencies which investigate Australia's most serious criminal matters and have been granted some of the most intrusive investigatory powers have the ability to seek the necessary assistance to ensure that these powers remain effective.

2.166 Empowering agencies that investigate Australia's most serious criminal offences with the ability to procure technical assistance in investigating serious crime and terrorism appears rationally connected with (that is, effective to achieve) the bill's objectives of protecting national security and public order. The proportionality of these measures is considered further below.

29 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'.

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

2.167 In the initial analysis, questions also arose as to whether all of the 'acts or things' that may be specified in a technical assistance notice or request, or technical capability notice, are rationally connected to the stated objectives of the measures. The statement of compatibility did 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, was rationally connected to the objectives of the bill. It was not clear, for example, how modifying a service provided by a provider,[30] or requiring a provider to install software,[31] would be effective to achieve the objectives of protecting national security and public order by addressing crime and terrorism. In this respect, the minister's response explains that:

> The types of assistance listed in section 317E are broadly cast in order to be responsive to operational needs and to reflect the rapidly changing capabilities of the communications industry. Regulation in such a dynamic and industry quickly becomes overly burdensome, obsolete and ineffective if prescriptive requirements are established in the legislation. Items 317E(1)(a) – (j) were developed in close consultation with agencies and, to some extent, reflect the nature of assistance received from domestic carriers and carriage service providers under obligations for reasonably necessary assistance in section 313 of the Telecommunications Act 1997 (the Telecommunications Act).

2.168 The minister's response then sets out examples of assistance that could be requested, from law enforcement and intelligence agencies respectively, in relation to each listed act or thing. In particular, in relation to modifying a service provided by a provider (subsection 317E(1)(h)), the minister's response provides that law enforcement might request a carrier increase the data allowance on a device that is subject to a surveillance device warrant to enable the surveillance device to be remotely monitored without consuming the target's data, or temporarily blocking internet messaging to force a device to send the messages as unencrypted SMS messages. In relation to requiring a provider to install software, the minister's response does not provide an example for the type of request that law enforcement may make, but provides the following example of a request in this category that an intelligence agency may make:

> An anonymous call is placed to the National security Hotline indicating that a Terrorist cell is planning a bombing attack against a fun run. ASIO receives this tip-off just two weeks before the event and only knows one of the group members involved. To avoid detection the group do not communicate via phone calls or face to face meetings but instead plan

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

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

> their attack online using application that encrypts messages as they are sent by users. Sent messages are received by the application's central server where they are decrypted and then re-encrypted with the intended recipient's key before being delivered to the intended recipient's device. ASIO secures an appropriate warrant and asks the communications provider to store copies of the target's communication before they are re-encrypted with recipient keys. To facilitate this, ASIO works with the DCP [designated communications provider] to install ASIO-controlled equipment that stores the communications. Interestingly, ASIO would store the communications in an encrypted format to prevent unauthorised access to the warranted material prior to it being disseminated back to ASIO.

2.169 The detailed information provided in the minister's response appears to demonstrate rational connection between the listed acts or things, and the objectives of the bill. The proportionality of these measures is considered below.

Proportionality

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

2.170 The initial analysis noted that 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 addressed the features of the measures and relevant safeguards, it did 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 did it consider whether the measures represent the least rights restrictive approach, compared with, for example, amending the relevant warrant and authorisation regimes. In this respect the minister's response advises that the measures in Schedule 1 are not 'vehicles for evidence collection in their own right' and safeguards in the bill prevent them from being used instead of a warrant or authorisation.

2.171 Therefore, as the minister's response explains, the sufficiency of the current warrant and authorisation schemes is not directly relevant to the need for the measures in Schedule 1, which are intended to complement, but not replace, these schemes. Rather, the minister states that the issue is the 'technical barriers' that prevent lawful access to communications and therefore the sufficiency of the current obligations for industry to assist with overcoming these technical barriers, which are currently set out in section 313 of the Telecommunications Act. The minister's response states that these obligations are 'clearly insufficient' and that section 313 is 'now inadequate' as it requires only a limited subset of providers to provide 'reasonably necessary' assistance to agencies, and suffers from considerable ambiguity.

2.172 The minister's response goes some way towards explaining why the measures are necessary, by reference to how technical barriers impede lawful access

to information granted pursuant to a warrant or authorisation, and how obligations for industry to assist with overcoming those barriers are 'inadequate'. However, having explained why the measures are necessary, the minister's response does not address whether the measures are *no more extensive* than is necessary to achieve the objectives of the bill, that is, whether the measures adopt the least rights restrictive approach, in order to satisfy the requirements of proportionality for the purposes of justifying a restriction on rights under international human rights law.

2.173 For example, some of the agencies designated as 'interception agencies' may have functions broader than addressing serious crime and terrorism, such as state-based integrity commissions, which have functions that include, for example, promoting the integrity and accountability of public administration.[32] It remains unclear from the minister's response how the limitation on the rights to privacy and freedom of expression associated with strengthening such agencies' capacity to undertake these broader functions, which do not appear to be related to serious crime and terrorism, is proportionate to the bill's objectives of protecting national security and public order.

2.174 Further, as to the power to issue a technical assistance request in relation to 'the interests of Australia's foreign relations or the interests of Australia's national economic well-being', the minister's response explains that the exercise of this power is 'intentionally linked' with the legitimate objective of protecting Australia's national security. However, the scope of proposed section 317G(5) does not link 'economic wellbeing and foreign relations' with national security when setting out the objectives for which a technical assistance request may be issued. Rather the section is framed disjunctively, allowing intelligence agencies to issue technical assistance requests for the objective of protecting 'the interests of Australia's national security, the interests of Australia's foreign relations *or* the interests of Australia's economic wellbeing'. This raises concerns as to whether the measure is sufficiently circumscribed, as well as additional concerns that issuing a technical assistance request for the purpose of economic wellbeing and foreign relations may fall outside the permissible grounds on which the right to freedom of expression can be restricted.

2.175 As noted in the initial analysis, the existence of safeguards is relevant to proportionality. In relation to the safeguards relating to the decision to issue technical assistance requests, questions arose because, in giving a technical

32 See section 2A of the *Independent Commission against Corruption Act 1988* (NSW) (Act), which 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'.

assistance request (in contrast to technical assistance notices and technical capability notices) the Director-General or chief officer of an interception agency would not be required to determine whether the requirements imposed by the notice are proportionate and reasonable, and whether compliance with the notice is practicable and technically feasible. While it was relevant that the power to issue such notices was limited to senior staff, further information was required to determine if this was sufficient.

2.176 The minister's response states that the requests are voluntary in nature, that this must be notified to the provider, and that a provider retains the legal capacity to refuse a request. However, this does not function as a safeguard on the *exercise* of the power to give a technical assistance request by the decision-maker, only on compliance by a third party provider. Therefore, there could still be circumstances in which a technical assistance request is made that is not proportionate but that is nonetheless voluntarily complied with by a provider. The fulfilment of such a request may ultimately have an impact which is more rights-restrictive than a technical assistance notice or technical compatibility notice, given the issue of notices is constrained by the requirements of proportionality, reasonableness, practicality and technical feasibility. It is also noted that the person whose privacy is impacted by the technical assistance request will not be in a position to comment on whether a request be voluntarily complied with, and so to this extent the voluntary nature of the request is not a sufficient safeguard.

2.177 The minister also reiterated that a technical assistance request can only be issued by the Director-General of ASIO, ASIS or ASD (or a delegate, who must be 'appropriately senior'), which 'ensures that issuing a TAR [technical assistance request] is done by the most senior officer of the relevant agencies'. However, it remains unclear why the power to issue a technical assistance notice and technical capability notice is limited by the requirement that such a notice be proportionate, reasonable, practicable and technically feasible, but no similar limitation is provided for technical assistance requests. While senior officers are more likely to have the requisite skills and experience to make a normative judgment as to whether a request made in a notice is proportionate, in circumstances where the issue of technical assistance requests does not require decision-makers to turn their minds to such matters (once the requirements of section 317G are met), restricting this power to senior officers does not appear to be a sufficient safeguard for the purposes of international human rights law. Accordingly, questions remain as to whether the power to give technical assistance requests is appropriately circumscribed so as to limit rights only as far as necessary to achieve the objectives of the bill.

2.178 In relation to safeguards regarding oversight and review of the measures, the initial analysis noted that a relevant factor in assessing whether a measure is proportionate is whether there is the possibility of oversight and the availability of

review.[33] Questions therefore arose in the context of the current bill insofar as 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. In this respect, the minister's response states that 'firstly, it is important to note that the bill does not in any way allow for agencies to access the content or substance of communications'. It is acknowledged that there are provisions of the bill that state that notices have no effect to the extent that they request information for which a warrant or authorisation would be required. However, this of itself is not an answer to whether the oversight and review mechanisms are sufficient.[34]

2.179 International human rights jurisprudence has stated the importance of providing for judicial oversight where surveillance measures or acquisition of communications are undertaken covertly, that is, without the knowledge of the individual affected by the measure. The European Court of Human Rights (ECHR) has explained:

> [S]ince the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights.[35]

2.180 In this respect, the ECHR has emphasised the importance of judicial oversight, noting that 'it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure'.[36] However, as noted earlier and in the initial analysis, the giving of a technical assistance notice or request, or technical capability notice, is not required to be authorised by a judge, nor does a judge supervise its application. While the minister's response states that judicial review of a decision to issue a notice is available pursuant to the *Judiciary Act 1903,* this appears to be relevant only to a provider's ability to apply for review of a decision to issue a notice. That is, it

---

33 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].

34 See the committee's previous analysis relating to warrantless access to metadata: Parliamentary Joint Committee on Human Rights, Telecommunications (Interception and Access) Regulations 2017, *Report 3 of 2018* (27 March 2018) pp. 129-137; Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *Fifteenth Report of the 44th Parliament* (November 2014) pp. 10-22; *Twentieth report of the 44th Parliament* (18 March 2015) pp. 39- 74; and Law Enforcement Legislation Amendment (State Bodies and Other Measures) Bill 2016*, Report 1 of 2017* (16 February 2017) p. 36

35 *Big Brother Watch v United Kingdom*, European Court of Human Rights application nos.58170/13, 62322/14 and 24960/15 (13 September 2018) [309].

36 *Big Brother Watch v United Kingdom*, European Court of Human Rights application nos.58170/13, 62322/14 and 24960/15 (13 September 2018) [309].

does not appear to give an individual whose rights may be impacted by a request or notice the ability to apply for review. In light of the secrecy provisions in the bill, it is unlikely that any person who has their rights affected by a technical assistance notice, technical capability notice or technical assistance request would be aware of the existence of a notice or request in order to seek review of the decision to issue it. Therefore, in terms of ensuring the impact on individual rights is proportionate for the purposes of international human rights law, the availability of judicial review for providers does not appear to be an adequate safeguard.

2.181 Other than judicial oversight, the minister's response notes that the bill does not change the existing regimes for oversight and accountability, including under the TIA Act and the SD Act and that 'accordingly, the powers that new requests and notices will be used in conjunction with are already subject to intense scrutiny'. In particular, the minister's response points to the following aspects of the bill:

- technical assistance notices may only be issued by the director general of ASIO, the chief officer of an interception agency or their senior delegate;
- technical capability notices may only be issued by the Attorney-General, and prior to the issue of a technical capability notice, there is a 28 day period for a telecommunications provider to make a submission to the Attorney-General; and
- the agencies that can issue notices are subject to oversight from integrity bodies, including the Commonwealth Ombudsman, State Ombudsman, Inspector-General of Intelligence and Security.

2.182 However, while the minister's response describes the oversight mechanisms, the minister's response does not provide information as to whether these oversight mechanisms are sufficient for the purposes of international human rights law. For example, the minister's response does not address the questions raised in the initial analysis as to whether the mandatory 28 day consultation period prior to issue of a technical capability notice is an adequate safeguard, given that the Attorney-General is not required to take into account any concerns raised by the provider, and in any case, the concerns raised by a provider may not necessarily be relevant to the impact a technical capability notice may have on human rights. Therefore, concerns remain as to whether the oversight and review mechanisms are adequate to ensure the measures restrict rights only so far as is strictly necessary to achieve the objectives of the bill.

<u>'Acts or things' compelled by a technical assistance notice or technical capability notice, or requested by a technical assistance request</u>

2.183 The initial analysis raised questions as to the adequacy of the safeguards relating to the disclosure of private information. It was noted 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 or their state and territory

equivalents.[37] This is a relevant and important safeguard in relation to the proportionality of the measures. However, it was noted that this safeguard only applied to technical assistance notices and technical capability notices, and not to technical assistance requests.

2.184 In relation to technical assistance requests and the relevant safeguards that would apply, the minister's response states that a technical assistance request cannot be used to request a provider to do a thing for which a warrant or authorisation would be required under an existing warrant regime. It also states that existing prohibitions in legislation like the prohibition against interception absent a warrant in section 7 of the TIA Act or the prohibition against disclosing data in section 276 of the Telecommunications Act are still in effect. The minister's response states that a technical assistance request 'is not an avenue to overcome these provisions and allow agencies to do things that they are currently not authorised to do'. However, it is noted that the minister's response states that the government is currently considering the possibility of amending section 317ZH to also apply to technical assistance requests.

2.185 The initial analysis also raised broader concerns as to the sufficiency of the safeguard in section 317ZH. In particular, 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),[38] it appears that a decision-maker can still issue a notice even if it seeks 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. The initial analysis raised questions as to how a provider, especially smaller or unsophisticated providers, would be expected to know whether or not what has been requested or compelled requires a warrant, and therefore how to respond accordingly.

2.186 In relation to this matter, the minister's response reiterates that section 317ZH prohibits the use of notices to obtain information for which a warrant would be required. The minister's response notes that, for example, under the TIA Act a warrant is required for the content of communications and an authorisation is required for the disclosure of metadata, and therefore it would be prohibited to use a notice to acquire this type of information. Further, it notes that the list of acts or things in section 317E does not include the disclosure of personal information as a form of assistance. However, as noted in the initial analysis, section 317E does not define 'acts or things' exhaustively and so it is not clear that this would be a sufficient

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

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

safeguard in and of itself. Similarly, since the TIA Act was legislated prior to the establishment of the committee and 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,*[39] it is difficult to conclude that the underlying warrant scheme in the TIA Act would operate as a sufficient safeguard.[40]

2.187 In the initial analysis, the committee sought the advice of the minister as to whether it would be feasible to amend the decision-making criteria to make it a requirement that the decision-maker be satisfied the request or notice does not seek information for which a warrant or authorisation would be required. The minister's response states that, because of section 317ZH and 317E, 'the Government does not consider it appropriate' to amend the decision-making power to state that a notice must not be issued unless the decision-maker is satisfied that it does not seek to compel a provider to do an act or thing for which a warrant is required. Therefore, for the reasons stated in the initial analysis, concerns remain that section 317ZH would not function as an effective safeguard.

2.188 The initial analysis also addressed the safeguard in section 317ZG, which would prohibit a provider from being compelled to implement or build a systemic weakness or vulnerability into a form of electronic protection,[41] also known as a 'back door'.[42] It was noted that this safeguard only applied to technical assistance notices and technical capability notices, not technical assistance requests. The committee also raised questions as to whether the safeguard would be sufficient in

---

39 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.

40 The committee has also raised serious concerns in relation to warrantless access to metadata: see Parliamentary Joint Committee on Human Rights, Telecommunications (Interception and Access) Regulations 2017, *Report 3 of 2018* (27 March 2018) pp.129-137; Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *Fifteenth Report of the 44th Parliament* (November 2014) pp. 10-22; *Twentieth report of the 44th Parliament* (18 March 2015) pp. 39- 74; and Law Enforcement Legislation Amendment (State Bodies and Other Measures) Bill 2016*, Report 1 of 2017* (16 February 2017) p. 36.

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

42 SOC, p. 11 [20].

circumstances where 'systemic weakness' and 'systemic vulnerability' were not defined.

2.189 In relation to 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, the minister's response states that:

> The government considers that a definition of 'systemic vulnerability' and 'systemic weakness' would be problematic for a number of reasons. Firstly, there is a significant divergence in the system architecture of the myriad of products, devices or software of the DCPs [designated communications providers] that are captured by the Bill. This makes a global definition difficult to settle.
>
> The activities that DCPs undertake under the Bill will not be uniform. One DCP may be able to meet requirements of a notice without creating a systemic weakness, while others may not. A prescriptive, inflexible application of the safeguard carries the risk of creating loop-holes and eroding the global protection it provides. In order to avoid this, the Bill allows each case to be considered individually. Each DCP, with intimate knowledge of its own systems is able to engage with agencies on whether a request would create a systemic weakness in a particular product or service. As such, the Government asserts that the scheme is sufficiently bounded and described within legislation to ensure that the broader effects are considered as part of the process.

2.190 However, the absence of a definition of 'systemic weakness' or 'systemic vulnerability' gives rise to a risk that those expressions could be interpreted and applied in an overly broad way, which may have broader effects on the users of a provider's service or device. Further, by placing the burden on the provider to determine what does or does not constitute a systemic vulnerability or weakness, it would not operate as a safeguard to avoid the arbitrary exercise of power by the decision-maker.

2.191 In relation to whether a technical assistance request could be used to request or compel a provider to implement or build a systemic weakness or vulnerability, the minister's response states that it could not, because compliance with a request is voluntary. However, as noted above, that a provider may choose to engage in conduct willingly versus being compelled to do so may not be a sufficient safeguard to ensure that the limitation on the rights to privacy and freedom of expression of users of a provider's service or device are proportionate.

2.192 In this respect, it is noted that 'the Government is considering whether amendments are necessary to extend the prohibition in 317ZG to technical assistance requests'. As noted earlier, the response also indicates the government is considering a similar amendment in relation to section 317ZH. However, the response also states the voluntary nature of technical assistance requests 'may make

this amendment unnecessary', as the provider responding to the request 'should be in a position to understand' when actioning a request would result in the creation of a systemic weakness and refuse to act on the request as appropriate. As has been discussed above, for the purposes of international human rights law, the ability of the provider to assess whether or not a notice is seeking the creation of a systemic weakness or vulnerability and to respond accordingly is not likely to be a sufficient safeguard to prevent an arbitrary exercise of power to give a technical assistance request.

2.193 In relation to whether it would be feasible to amend sections 317ZG and 317ZH to expressly refer to *variations* to technical assistance notices and technical capability notices, the minister's response states that 'the limitations set under sections 317ZG and 317ZH already apply to variations to technical assistance notices and technical capability notices'. This clarification as to the interpretation of these sections is helpful.

2.194 While the measures in the bill do not alter the underlying warrant and authorisation regime in the TIA Act, in circumstances where the measures in the bill interact with that regime it is difficult to fully consider the human rights compatibility of the proposed measures without a foundational human rights assessment of the TIA Act. The committee reiterates its previous position that the TIA Act would benefit from a foundational assessment of its compatibility with human rights.

Committee response

2.195 The committee thanks the minister for his response and has concluded its examination of this issue.

2.196 While technical assistance requests, technical assistance notices and technical capability notices pursue a legitimate objective and are likely to be rationally connected to that objective, the preceding analysis indicates that the regime is unlikely to constitute a proportionate limitation on the rights to privacy and freedom of expression, and is therefore likely to be incompatible with those rights.

Compatibility of the measure with the right to an effective remedy: initial analysis

2.197 The initial analysis raised questions as to the compatibility of the measures with the right to an effective remedy. The right 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. Limitations may be placed on the nature of the remedy, but state parties must comply with the fundamental obligation to provide a remedy that is effective.

2.198 The statement of compatibility did not consider the right to an effective remedy in relation to the measures. The initial analysis therefore sought the advice

of the minister as to the compatibility of measures with this right. In particular, it raised questions as to how an individual that was or would be detrimentally impacted by a provider's compliance with a notice or request could seek judicial review, given the secrecy provisions in the bill are likely to mean they would be unaware a notice or request was given. It also raised questions as to how the provision of immunity from civil liability to providers was compatible with the right to an effective remedy for persons detrimentally impacted by the provider's compliance with a request.

2.199 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) at pp. 39-40.[43]

2.200 The committee therefore sought the advice of the minister as to the compatibility of technical assistance notices, technical capability notices and technical assistance requests with the right to an effective remedy.

Minister's response and analysis

2.201 The minister's response states that there is an express exclusion of judicial review under the ADJR Act, and of merits review, consistent with the existing exclusion of other national security and law enforcement legislation from these types of review. The minister's response notes that should a provider seek to challenge a notice, there are a number of grounds available, as well as specific defences, such as that compliance with the notice would contravene the law of a foreign country or would create broad vulnerabilities in a network. In relation to the rights of individuals, the minister's response states:

> [T]he sensitive and timely nature of investigations require tools that can be issued quickly and effectively, without compromising the nature of the investigation. The Bill, in conjunction with warranted powers enables the gathering of evidence. Where that evidence is later tendered in criminal proceedings, a defendant would then have an opportunity to challenge the admissibility of that evidence. If the evidence was unlawfully or improperly obtained, the right to an effective remedy is available.

2.202 While this might be capable of serving as a relevant safeguard for an accused person in relation to the investigation of whom assistance has been sought pursuant to the bill, the minister's response does not address the right to effective remedy of persons whose rights are impacted by a provider's compliance with a technical assistance request, but against whom no criminal proceedings are brought. It is also noted that while the remedy available may prevent use of evidence unlawfully or improperly obtained, it may not provide a remedy for the original violation of the

43 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 39-40 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

right to privacy. Since a provider receives immunity from civil liability for an act or thing done pursuant to a technical assistance request, then a person or persons whose rights are detrimentally impacted by that compliance is unable to pursue a civil remedy against the provider in relation to that act or thing. Similarly, the minister's response does not consider or engage with the question raised in the initial analysis as to 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.

Committee response

2.203 The committee thanks the minister for his response and has concluded its examination of this issue.

2.204 The committee is unable to conclude that the measure is compatible with the right to an effective remedy. The committee notes that the minister's response did not fully address the committee's inquiries in relation to these complex issues.

Computer access warrant scheme in the Surveillance Devices Act

2.205 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[44] remotely or physically and access content on that computer.[45]

Computer access warrants

2.206 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'[46] or where there has been a 'mutual assistance authorisation'[47] where the law enforcement officer suspects on reasonable grounds that access to data[48]

---

44 '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; or (c) one or more computer networks; or (d) any combination of the above'.

45 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.

46 '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.

47 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.

48 '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).

held in a computer[49] (the 'target computer')[50] is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the commission of the relevant offences, or the identity or location of the relevant offenders;

- where a recovery order[51] 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'[52] 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.

2.207 Proposed section 27C provides that a computer access warrant is issued by an eligible Judge or a nominated AAT member (decision-maker).[53] 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

---

49 '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.

50 '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.

51 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*.

52 'integrity authority' is defined in section 6 of the SD Act.

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

to be obtained, and the likely evidentiary or intelligence value of evidence or information obtained.

2.208 A computer access warrant authorises specified things to be done covertly 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;
- 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;[54] and
- any other thing reasonably incidental to any of the above.[55]

2.209 There are also concealment of access powers[56] and provisions which compel persons to provide assistance to law enforcement to allow the officer to access data,[57] discussed in further detail below.

2.210 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.[58] 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.[59]

---

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

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

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

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

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

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

Additional measures in relation to computer access warrants for control orders

2.211 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 control order is void, any information obtained under the control order computer 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.[60]

Emergency authorisation for access to data held in a computer

2.212 Additionally, the bill seeks to amend the SD Act to provide that a law enforcement officer may apply to an 'appropriate authorising officer'[61] for an emergency authorisation for access to data held in a target computer[62] 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.[63] 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.[64]

2.213 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 (the decision-maker) may give the approval if satisfied of certain matters.[65] In making this decision, the decision-maker considering the application must, in

---

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

61 '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).

62 '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.

63 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).

64 See sections 28(4), 29(3) and 30(3) of the SD Act.

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

particular, and 'being mindful of the intrusive nature of accessing data held in a target computer',[66] 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.[67]

Compatibility of the measures with the right to privacy: initial analysis

2.214 The initial analysis stated that the measures engaged and limited the right to privacy. This is because the new computer access warrant scheme in the SD Act would allow for accessing a person's personal information held in a computer, which is inherently privacy intrusive. This limitation was acknowledged in the statement of compatibility.

2.215 The statement of compatibility identified the objective of the measures as protecting national security and public order, and addressing advances in technology which enable criminals to conduct activities and communicate anonymously.[68] While this is capable of being a legitimate objective, the initial analysis stated that further information was required in order to determine whether the measures addressed a substantial or pressing concern.

2.216 The committee also raised questions as to whether the measures were rationally connected (that, is effective to achieve) and proportionate to the stated objectives. In particular, the committee noted that it was difficult to assess the human rights compatibility of amendments to the SD Act in circumstances where the underlying Act has not been subject to a foundational human rights compatibility assessment, because it predated the establishment of the committee. It was also noted that there were concerns as to whether the measures were sufficiently circumscribed, noting the intrusive nature of the power and its application to third party premises and third party computers. There were also questions as to the proportionality of the emergency authorisation procedures, including whether there were sufficient safeguards and whether the measure was the least rights restrictive approach.

2.217 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 43-47.[69]

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

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

68 SOC, p.18 [84].

69 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 43-47 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

2.218 The committee therefore sought the advice of the minister as to the compatibility of the measures with the right to privacy, 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.

Minister's response and analysis

2.219 The minister's response provides the following information as to the pressing and substantial concern the measures seek to address:

> Traditionally, the Surveillance Devices Act 2004 (Cth) (SD Act) has permitted a range of devices such as mobile phones to be accessed via warrant. However, this warranted access has so far only enabled 'view only' access. Essentially, once the surveillance device is installed on the mobile phone, law enforcement currently cannot access files or file structure, only view what the person of interest is currently doing. With the incredible uptake of technology, this is becoming increasingly restrictive to law enforcement efforts. For example, a person who accesses child sexual abuse material may have large collections on their device and is sharing with individuals overseas. This information may not be easily detected purely through read only viewing of the device. The added complexity of encryption means that accessing data on the phone both within the file structure of the device and before encryption takes place can be key to obtaining vital evidence to investigate and prosecute serious crime.

> …
>
> These changes modernise the evidence and intelligence collection capabilities of Australia's key agencies and will facilitate the lawful collection of data in a more accessible state.

2.220 In light of this information, it appears that the measures seek to address a pressing and substantial concern such that the measures pursue the legitimate objective of protecting national security and public order. The measures also appear to be rationally connected to this objective.

2.221 The minister's response also provides further information as to the extent to which computer access warrants interfere with data:

> Interference is not authorised when executing a CAW [computer access warrant]. Specifically, the warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. However, there may be addition, deletion or alteration of data where necessary for the execution of the CAW. The execution of a CAW may necessarily require that software be installed on the device, and naturally this will require interference with the underlying data on the device …
>
> Moreover, the warrant does not authorise the material loss or damage to other persons lawfully using a computer, except where necessary for concealment. Concealment is necessary to ensure that these proposed powers can be utilised effectively. Where there is the potential for terrorists or those committing serious crime to identify that their devices are being monitored through the use of a CAW, it may significantly jeopardise ongoing resource intensive criminal investigations involving the device. The interference with data is a proportionate limitation on the right to privacy, and is necessary to achieve the stated objectives of public order and national security.

2.222 This information clarifies the scope of interference with data, and it is important that the warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. However, it is still apparent that the scope of interference pursuant to the warrants is very privacy intrusive, particularly as it applies to third party premises and the computers of third parties used to access relevant data. Issues relating to concealment are discussed in further detail below.

2.223 Noting the intrusive nature of the computer access warrant scheme, the safeguards that are in place are particularly important to ensure that any limitation on the right to privacy goes only so far as is strictly necessary. In this respect, the minister's response reiterates the safeguards that are in place to protect a person's right to privacy:

> In exercising these powers, activities must be proportionate and reasonable to any specific limitation on the right to privacy. For example, there are existing safeguards and oversight mechanisms under the SD Act which will apply for CAWs. These significant safeguards and oversight mechanisms include:
>
> • minimum offence threshold requirements (3 years' imprisonment or above);
>
> • must be issued by an eligible Judge or AAT member;
>
> • the warrants must specify the things that are authorised under the warrant;
>
> • unauthorised disclosure of information about, or obtained under, a CAW is an offence;
>
> • strong reporting requirements to provide assurance to Parliament and the Australian community that the powers are being used only as required; and
>
> • oversight by the Commonwealth Ombudsman to review the performance of CAWs and determine compliance with law.
>
> Judicial oversight is a key safeguard to the CAW regime under Schedule 2. The things that an eligible Judge or AAT member must have regard to under proposed subsection 27C(2) will ensure that any limitation on the right to privacy by the execution of a CAW is proportionate and necessary to achieve the stated objectives of the measures. For example, an eligible Judge or AAT member must weigh up the nature and gravity of the alleged offending with the likely evidentiary or intelligence value of any evidence that might be obtained, 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.

2.224 The minister's response also reiterates the safeguards in the SD Act which apply to the SD Act as a whole, including offences for misuse and disclosure and oversight arrangements by the Commonwealth Ombudsman or the Inspector-General of Security and Intelligence (in the case of ASIO).

2.225 These safeguards are important in assessing the proportionality of the computer access warrant regime. In particular the provisions of the bill that provide for judicial oversight over the issue of warrants (with the exception of emergency authorisations, discussed further below, and the use of force, control order computer access warrants, concealment of access powers, and assistance orders discussed in the sections below) provide an important safeguard against abuse.[70] However, it is noted that while judicial authorisation is an important safeguard, by

70 *Big Brother Watch v United Kingdom,* European Court of Human Rights application nos. 58170/13, 62322/14 and 24960/15 (13 September 2018) [308]-[310].

itself it is not necessarily sufficient to ensure compliance with the right to privacy, noting the extent of possible interference with the right to privacy.[71] Rather, much will depend on how the scheme operates in practice and how that scheme is monitored while the warrant is in force.

2.226 Additionally, the requirement for the judge or AAT member to consider the extent to which the privacy of any person is likely to be affected and the existence of alternative means of obtaining the evidence or information before determining whether a computer access warrant should be issued goes some way towards ensuring that any decision to issue a computer access warrant will be the least rights restrictive approach available. However, noting the particularly significant interference with the right to privacy for the target of a computer access warrant and potentially for third parties,[72] a stronger safeguard could be to identify not only the existence of alternative means of obtaining evidence[73] but also an explicit requirement that a computer access warrant application must demonstrate that it is not possible to obtain the evidence in any other way and that the proposed computer access is the least restrictive approach in the circumstances, and that a warrant must not be authorised unless it is so demonstrated. The strength of the safeguards is particularly important in circumstances where computer access warrants generally operate covertly, and so there will be no opportunity for either the target of the warrant or an affected third party to know whether access is in accordance with the terms of the warrant or the law more generally.[74] Concerns therefore remain that the proposed computer access warrant scheme may not be a proportionate limitation on the right to privacy.

2.227 As to compatibility of emergency authorisations with the right to privacy, the minister's response provides the following information:

> The use of emergency authorisations for the use of surveillance devices is not new. Since 2004, emergency authorisations have been available for the broader set of surveillance device powers under the SD Act.

---

71 *Big Brother Watch v United Kingdom,* European Court of Human Rights application nos.58170/13, 62322/14 and 24960/15 (13 September 2018) [20], [320].

72 Including other persons on the premises subject to a computer access warrant and third party users of 'any other computer' that may be authorised to be accessed pursuant to the warrant.

73 Or, in the case of authorising the use of 'any other computer', the requirement of having regard to other methods of obtaining access to the relevant data which are likely to be as effective: see proposed section 27E(1)(e) of the SD Act in Schedule 2 of the bill.

74 The committee has previously raised concerns about the human rights compatibility of covert warrants in the context of its consideration of delayed notification search warrants: see, Parliamentary Joint Committee on Human Rights, Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014, *Fourteenth Report of the 44th Parliament* (October 2014), pp. 29-33.

> Emergency authorisations are available only in very limited circumstances, namely where there is imminent risk of serious violence or substantial property damage, where it will assist relating to a recovery order, and where there is a risk of loss of evidence. In each of these circumstances, the use of an emergency authorisation must be immediately necessary to achieve the stated purpose, and must demonstrate that it is not practical to apply for a CAW. In practice, emergency authorisations are only utilised rarely. For example, in the Surveillance Device Act Annual Report 2016-2017, no law enforcement agencies made an emergency authorisation.
>
> Various safeguards exist to ensure that emergency authorisations are necessary and proportionate. Within 48 hours after an emergency authorisation is given by an authorising officer, there must be an application to an eligible Judge or AAT member for approval. In deciding whether to approve this application, an eligible Judge or AAT member must, being mindful of the intrusive nature of the use of a surveillance device, consider various things, such as urgency in relation to the stated purpose (e.g. risk of serious violence to a person), alternative methods, and whether or not it was practicable in the circumstances to apply for a surveillance device warrant.
>
> Information gathered as part of an emergency authorisation is considered 'protected information' and is subject to the strict use and disclosure provisions that ordinarily exist for information obtained from powers exercised under the SD Act. Criminal liability is attached to unauthorised disclosure of information protected under the SD Act.
>
> The availability of the use of computer access powers under an emergency authorisation is proportionate and is necessary to ensure that, in special circumstances, the computer access powers can be used for the purposes of public safety and national security. The Government views these powers as balancing the interests of the public and recognition of the importance of privacy of the Australian community.

2.228 It is acknowledged that there are a number of safeguards in place to ensure that emergency authorisations to obtain computer access only occur in limited circumstances. This includes a requirement that an authorising officer must reasonably suspect that the circumstances are so serious and the matter is of such urgency that access to data held in the target computer is warranted, and that it is not practicable in the circumstances to apply for a computer access warrant.[75] The requirement for a judge to consider the extent to which alternative methods could have been used and the 'intrusive nature of accessing data' before deciding an application for approval is also important.[76] The minister's clarification that

75 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).

76 See proposed section 34(1A) of the SD Act in Schedule 2 of the bill.

information gathered pursuant to an emergency authorisation will be 'protected information' and therefore governed by the use and disclosure provisions of the SD Act also assists in determining the proportionality of the limitation.

2.229 However, the minister's response does not address the specific concerns raised in the initial analysis relating to the treatment of information where a decision-maker does not subsequently approve the authorisation. As noted in the initial analysis, in such circumstances the decision-maker may make certain orders but may not order the destruction of any relevant information obtained.[77] The explanatory memorandum explains that this is because 'such information, while improperly obtained may still be required for a permitted purpose such as an investigation'.[78] However, there are concerns that using information that has been improperly obtained to pursue an investigation against a person would not be a proportionate limitation on the right to privacy. As noted in the initial analysis, there would appear to be other less rights restrictive approaches available, including the destruction of information that has been improperly obtained or obtaining a new warrant to obtain information in accordance with the warrant scheme.

Committee response

2.230 The committee thanks the minister for his response and has concluded its examination of this issue.

2.231 The preceding analysis indicates that there is a risk that the proposed computer access warrant scheme in the *Surveillance Devices Act 2004* may be incompatible with the right to privacy, due to the extent of the impact on privacy. However, noting the requirements for a decision-maker issuing the warrant to consider the extent to which the privacy of persons is likely to be affected and the existence of any alternative means of obtaining evidence, much will depend on how the computer access warrant scheme operates in practice. It is recommended that the scheme be monitored to ensure that any limitation on the right to privacy be only as extensive as is strictly necessary to achieve the legitimate objectives of the bill.

2.232 The committee considers that emergency authorisations to obtain access to data held on a computer are likely to be incompatible with the right to privacy.

Compatibility of the measure with the right to a fair trial and fair hearing: initial analysis

2.233 The right to a fair trial under 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

77 See proposed section 35A(5) and (6) of the SD Act in Schedule 2 of the bill.

78 Explanatory memorandum (EM), p.105 [579]-[580].

to understand the nature 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.

2.234 The initial analysis stated that prohibiting disclosure of information relating to computer access technologies and methods in proceedings may engage the right to a fair trial and fair hearing. This is because the result of the prohibition is that there may be circumstances in which a defendant would not have the opportunity to review material that the judge considers warrants protection. This limitation was acknowledged in the statement of compatibility.[79]

2.235 The statement of compatibility states that it is necessary to prevent the release of sensitive operational information into the public domain to protect the public and national security. The initial analysis stated that this may be capable of being a legitimate objective for the purposes of international human rights law. However, it was stated that while such an objective may be legitimate in relation to *public* disclosure of sensitive information, it was not clear whether that explanation was sufficient to preclude a defendant from accessing such information which may be relevant to their case. The initial analysis also raised questions as to whether the measure was rationally connected and proportionate to the objective.

2.236 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 47-49.[80]

2.237 The committee therefore sought the advice of the minister as to the compatibility of the measure with the right to a fair trial and fair hearing, 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).

Minister's response and analysis

2.238 The minister's response provides the following information in relation to the compatibility of the measure with the right to a fair trial and fair hearing:

79 SOC, p.20 [92].

80 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 47-49 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

> The provisions engage the right to a fair hearing under Article 14(1) of the ICCPR, specifically that evidence should be available to be contested where it forms part of one sides arguments (such as where it forms part of the prosecution case).
>
> The Government recognises the importance of the protection to sensitive information relating to computer access methodologies to prevent the release of such information to the public domain in a way that might harm future law enforcement operations. This is the stated objective of these proposed provisions.
>
> The proposed protections permit a person to object to the disclosure of information on the ground that, if disclosed, it could reasonably be expected to reveal details of computer access technologies and methods. The objection is not absolute, the public interest in protecting sensitive law enforcement information must be weighed against other public interest concerns by the person presiding over the proceedings, be he or she a Judge, Magistrate, Tribunal member or Royal Commissioner or any other type of presiding officer. This will permit arguments by those that may oppose the objection to raising less restrictive measures which may be available.
>
> The proposed protections also do not prohibit the disclosure of information in so far as it relates directly to the alleged conduct of an accused person and any alleged criminal offending (including disclosure of offences alleged against the accused). Accordingly, the Government views that this measure is strictly necessary and proportionate to ensure protection of future law enforcement operations, whilst providing sufficient judicial oversight in the exercise of that protection. It also reflects existing accepted practices of protection of sensitive information relating to law enforcement surveillance technologies and methodology.

2.239 The European Court of Human Rights has held that it is permissible to place restrictions on the right to a fully adversarial procedure if there are strong national security grounds that require certain information to be kept secret.[81] However, while information can be withheld from a person, sufficient information about the allegations against the person must be provided to enable them to give effective instructions in relation to those allegations.[82]

2.240 The requirement that the person conducting the proceeding must take into account whether disclosure of information is necessary for a fair trial of the defendant or is in the public interest is an important safeguard. As noted in the

---

81 See *A and Others v the United Kingdom*, European Court of Human Rights, Application no. 3455/05 (19 February 2009).

82 See *A and Others v the United Kingdom*, European Court of Human Rights, Application no. 3455/05 (19 February 2009); *Sher and Others v the United Kingdom*, European Court of Human Rights, Application no. 520/11 (20 October 2015).

minister's response, this would permit arguments to be made by a defendant and the prosecution about non-disclosure, including whether other less restrictive means may be available. However, depending on how much information is proposed not to be disclosed to a defendant, it still may be the case that a defendant is at a disadvantage to the prosecution in making submissions as to the effect of the non-disclosure of information on the substantive hearing in the proceedings. The minister's clarification that the provision would not prohibit disclosure of information in so far as it relates directly to the alleged conduct of an accused person and any alleged criminal offending assists with proportionality of the measure in this respect. Therefore, while it appears the safeguard in section 47A would be sufficient, it is suggested that the operation of the provision be monitored to ensure that a defendant affected by the measure has sufficient information available to able to prepare a defence.

Committee response

2.241 The committee thanks the minister for his response and has concluded its examination of this issue.

2.242 The committee considers that proposed section 47A may be compatible with the right to a fair trial and fair hearing. However, the committee recommends that the operation of this provision be monitored to ensure that a defendant affected by the measure has sufficient information available to able to prepare a defence.

Compatibility of the use of force power with multiple rights

2.243 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.

2.244 The initial analysis noted that the use of force provisions engage multiple human rights. The provisions engage the right to privacy insofar as using force to enter 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) such as amounts to a violation of these rights.

2.245 The statement of compatibility did not acknowledge that the use of force provisions engaged any of these rights.

2.246 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 49-50.[83]

2.247 The committee therefore sought the advice of the minister as to compatibility of the use of force provisions with the right to privacy and right to life, 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.

2.248 In relation to the prohibition on torture, cruel, inhuman and degrading treatment or punishment, noting the absolute nature of this prohibition, the committee sought 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.

Minister's response and analysis

2.249 In relation to the compatibility of the use of force provisions with the prohibition on torture, cruel, inhuman and degrading treatment or punishment, the minister's response states:

> The government considers that the measures contained under proposed subsection 27E(6) of the Bill are compatible with the prohibition against torture, cruel, inhuman or degrading treatment or punishment, contained under article 7 of the ICCPR.
>
> Under proposed subsection 27E(D) [sic], an eligible Judge or AAT member in authorising a CAW must only authorise the use of force against a person or things that is necessary and reasonable to do the things specified in the warrant. This does not permit law enforcement to subject a person to torture or cruel, inhuman or degrading practices, particularly where it involves detention of a person.
>
> The use of force by law enforcement is inherently, and more broadly, restricted under Commonwealth domestic legislation to ensure the appropriate balance is struck between actions required in enforcing a warrant and the expected treatment of individuals.

83 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 49-50 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

> Acquiring a warrant of the kind referred to under subsection 27E(6) requires independent third party authorisation and, when issuing such a warrant, an eligible Judge or AAT member, which ensures there is oversight to ensure the individuals referred to within warrants are not subject to torture or inhumane treatment.
>
> Other oversight mechanisms such as the Commonwealth Ombudsman in respect of law enforcement agencies, and the Inspector-General of Intelligence and Security in respect of national security agencies, are responsible for receiving complaints where it is alleged that an officer may have exceeded lawful use of force.

2.250 The minister's response appears to indicate the assessment as to what would constitute 'necessary and reasonable' is an assessment made by the decision-maker authorising the warrant. To that extent, the requirement that a judge issuing a computer access warrant may only authorise force that is 'necessary and reasonable' is a relevant safeguard that may be capable of ensuring that the use of 'any force' would not occur in a way that causes pain (physical or mental) in such a way that it amounts to a violation of the prohibition on torture, cruel, inhuman and degrading treatment. However, while the minister's response states that law enforcement is not permitted to submit a person to torture, cruel, inhuman or degrading practices, the response does not provide any information (for example, relevant training of law enforcement officers who use force) that would guarantee that force would not be used in a way that is contrary to these rights. Therefore, much may depend on how the use of force power is implemented in practice.

2.251 The minister's response does not respond to the committee's inquiries in relation to the compatibility of the use of force provision with the right to life and the right to privacy. However, the requirement that force may only be 'necessary and reasonable' may also be capable of ensuring that the use of any force would not occur in a way that is incompatible with the right to life and the right to privacy. As discussed earlier, whether any limitation on these rights that arises from the use of force power will be proportionate will depend on how the use of force power is implemented in practice.

Committee response

2.252 The committee thanks the minister for his response and has concluded its examination of this issue.

2.253 The committee considers that the requirement that a decision-maker (judge or AAT member) may only authorise force that is 'necessary and reasonable' pursuant to a computer access warrant may be capable of operating as a sufficient safeguard so as to be compatible with the prohibition on torture, cruel, inhuman and degrading treatment or punishment, the right to life and the right to privacy. However, much will depend on how the use of force power operates in practice. The committee recommends that the operation of the use of force power be monitored to ensure that it occurs in a manner compatible with human rights.

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

2.254 As noted earlier, Schedule 2 of the bill provides that computer access warrants could be used against persons subject to a control order (control order computer access warrant), including for determining whether a control order has been complied with. There is also a provision which precludes criminal liability for persons who exercise powers relating to control order computer access warrants if the control order is declared void, as well as a provision which allows for the use of information obtained under the warrant even if the order is declared void,[84] including use of the information in relation to matters arising under a preventative detention order.[85]

2.255 The initial analysis noted that the committee previously considered that the control orders regime engages a number of human rights.[86] To the extent computer access warrants could be used against persons subject to a control order, several of these rights may be engaged and limited, in particular the right to privacy. The right to an effective remedy is also engaged by the provisions of the bill that preclude liability for persons who exercised powers relating to control order computer access warrant if the control order is declared void.

2.256 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 50-51.[87]

2.257 The committee therefore sought 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.

Minister's response and analysis

2.258 The minister's response provides the following information as to the compatibility of control order computer access warrants with human rights:

> The Government acknowledges that CAWs issued for monitoring compliance with control orders issued under Schedule 2 of the Bill engages with multiple human rights. Australia continues to face a serious terrorist

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

85 See section 65B of the SD Act.

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

87 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 50-51 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

> threat which has seen an increased operational need to protect the public from terrorist acts.
>
> As noted above, Schedule 2 of the Bill engages the protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR. The Government considers the implementation of the power to issue a CAW for the purposes of monitoring a control order to be in pursuit of a legitimate objective (the objectives in which a control order can be obtained, i.e. protection of the public from a terrorist act), which remains rationally connected and proportionate to the pursuit of that objective.
>
> A control order CAW is a computer access warrant that may be applied for by a law enforcement officer if a control order is in force and he or she suspects that access to data held in a computer would be likely to substantially assist in either protecting the public from a terrorist act, preventing the provision of support for a terrorist act or a hostile activity, or determining whether the control order is being complied with. In order for a control order computer access warrant to be granted, the law enforcement officer applying for the warrant, and the issuing eligible Judge or AAT member, must be satisfied that there is a rational connection between the stated legitimate objective of the measure (e.g. protection of the public from a terrorist act), and the use of a CAW being likely to substantially assist in achieving that objective.
>
> The Government affirms that the new power is proportionate, as the new provisions tightly constrain the purposes for which law enforcement agencies may use the information intercepted under this provision, include necessary safeguards such as judicial oversight, and appropriate use and disclosure provisions.
>
> As part of the introduction of the monitoring warrant powers under the SD Act for the purposes of monitoring compliance with control orders, the human rights compatibility of the control order regime and monitoring powers were detailed significantly as part of the *Counter-Terrorism Legislation Amendment Act (No.1) 2016*.

2.259 As noted earlier, the safeguards that apply when determining whether to issue a computer access warrant (including control order computer access warrants), in particular the requirement for a judge to consider the impact on the privacy of the individual and the requirement to take into account alternative means of obtaining the information, are important safeguards. However, noting the broader concerns with the control orders regime,[88] there are additional concerns relating to computer access warrants as they apply to control orders.

2.260 In particular, the minister's response does not specifically engage with whether precluding criminal liability for persons who exercised powers relating to a

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

control order computer access warrant, if the control order is subsequently declared void, is compatible with the right to an effective remedy. The minister's response also does not specifically address whether being able to use information obtained pursuant to a control order computer access warrant where the control order is declared void,[89] including in relation to a matter arising from a preventive detention order,[90] is a proportionate limitation on human rights. In the absence of such information, notwithstanding the safeguards identified by the minister, it is not possible to conclude that the control order computer access warrants are compatible with human rights.

Committee response

2.261 The committee thanks the minister for his response and has concluded its examination of this issue.

2.262 The committee is unable to conclude that control order computer access warrants are compatible with human rights. The committee notes that the minister's response did not fully address the committee's inquiries in relation to these complex issues.

Concealment of access powers

2.263 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;
- 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.[91]

2.264 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

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

90 See section 65B of the SD Act.

91 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.

computer access warrant is in force, or within 28 days after it ceases to be in force.[92] 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'.[93]

Compatibility of the measure with the right to privacy: initial analysis

2.265 The initial analysis raised questions as to the compatibility of the concealment of access powers with the right to privacy. The statement of compatibility acknowledged that this right was engaged and limited by the powers, as officers would be enabled to access devices, which hold personal information, for the purposes of concealment.[94]

2.266 The stated objective of the concealment of access powers was to protect the rights and freedoms of individuals by providing ASIO with the tools it requires to keep Australians safe.[95] The initial analysis noted that while this may be capable of giving rise to a legitimate objective, further information was required to determine whether this objective was legitimate in the context of the specific measures. The initial analysis also raised questions as to whether the measures were rationally connected and proportionate to the stated objective.

2.267 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 52-54.[96]

2.268 The committee therefore sought the advice of the minister as to the compatibility of the measure with the right to privacy, 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 as 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

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

93 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.

94 SOC, p.17 [63].

95 SOC, p.17 [69].

96 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 52-54 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

- 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).

Minister's response and analysis

2.269 In relation to the objective of the measures, the minister's response identifies the objective of protecting public safety, public order and national security and provides the following additional information:

> Undertaking surveillance activities on an electronic device may alter data, or leave traces of activity, on that device. This may allow for alleged terrorists and criminals to recognise the lawful intrusion by law enforcement agencies and effectively change the way they communicate for the purposes of avoiding law enforcement (e.g. recognition may lead to reverse engineering the police capabilities and methodology leading to individuals avoiding certain technologies or undertaking counter-surveillance activities). Accordingly, the concealment of the execution of a CAW is vital to the exercise of the powers under Schedule 2, and indeed, the existing powers under the Australian Security Intelligence Organisation Act 1979 (ASIO Act).
>
> In the event that law enforcement agencies and ASIO are unable to conceal, there is significant risk to the exposure of police technologies and methodologies. This could reduce opportunities for agencies to prevent serious crime and acts of terrorism.

2.270 The minister's response identifies the pressing and substantial concern which the concealment of access powers seek to address. In light of the information provided by the minister it appears the measures pursue a legitimate objective for the purposes of international human rights law, and are rationally connected to this objective.

2.271 In relation to the proportionality of the measures, the minister's response states:

> The measures are subject to limitations, safeguards and oversight mechanisms designed to ensure that the proposed and existing measures are used proportionately, reasonably and only as necessary. For example, the proposed CAWs under the Bill are subject to the requirement for judicial authority and oversight by the Commonwealth Ombudsman, and the existing ASIO CAWs are subject to ministerial oversight (approval required by the Attorney-General) and oversight by the IGIS.

2.272 As noted earlier, the judicial oversight over the issue of a computer access warrant (which may include an order for concealment) is an important safeguard. However, as concealment of access powers allow warrants to operate covertly, there will be no opportunity for either the target of the warrant or the third party to know whether access is in accordance with the terms of the warrant or the law more generally. Further, in relation to the power to conceal access pursuant to a computer

access warrant, there are additional concerns that the judicial oversight of the computer access warrant does not address. As noted in the initial analysis, 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 defined and the provision is not subject to any express time limits. As noted in the initial analysis, 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. There would appear to be less rights restrictive measures available to address this, including requiring further authorisation or 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.

Committee response

2.273 The committee thanks the minister for his response and has concluded its examination of this issue.

2.274 The preceding analysis indicates that the concealment of access powers are likely to be incompatible with the right to privacy.

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

2.275 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)[97] 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.[98] 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.

2.276 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.[99] The offence is punishable by

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

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

99 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.

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.[100]

2.277 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 who does not comply with an order is liable to a maximum of five years' imprisonment.[101]

Compatibility of the measure with the right to privacy: initial analysis

2.278 The initial analysis raised questions as to the compatibility of the assistance order provisions with the right to privacy. The statement of compatibility acknowledges the measures engage and limit the right to privacy, insofar as it enables certain law enforcement officers and agencies, and the Australian Border Force and ASIO to access private communications and other information on a person's device.[102]

2.279 The stated objective for the measures is the protection of national security. The initial analysis noted that while protection of national security was capable of being a legitimate objective for the purposes of international human rights law, further information was needed to establish the pressing and substantial concern the measures seek to address. Further, while compelling persons to provide assistance to access data and devices pursuant to a warrant appeared to be rationally connected to this objective, the initial analysis raised questions as to the proportionality of the measures.

2.280 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 55-57.[103]

2.281 The committee therefore sought the advice of the minister as to the compatibility of the assistance order provisions in Schedules 2, 3, 4 and 5 with the right to privacy, in particular:

- the pressing and substantial concern that the measures seek to address; and

100 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.

101 Proposed section 34AAA of the ASIO Act in Schedule 5 of the bill.

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

103 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 55-57 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

- whether the measures are a proportionate limitation on the right to privacy (including whether the measures are sufficiently circumscribed and accompanied by adequate safeguards).

Minister's response and analysis

2.282 The minister's response states that recent law enforcement experiences have highlighted that current assistance order powers are significantly outdated as they can only be issued pursuant to a premises search warrant, and that law enforcement can't compel that assistance in relation to a device, such as a mobile device, found on a person. The response also explains the broader importance of assistance orders in undertaking investigations of serious criminal activity to ensure that either law enforcement have access to devices subject to protections such as passwords, or there is criminal accountability in the event that a person refuses and a prosecution is in the public interest. In light of this information and the information in the statement of compatibility that the inability to access devices found on persons significantly impedes investigations and, in the context of ASIO, can frustrate operations to protect national security, on balance the measures appear to pursue a legitimate objective for the purposes of international human rights law. As noted in the initial analysis, 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.

2.283 In relation to the proportionality of the measures, the minister's response firstly emphasises that assistance orders must be judicially authorised. As noted earlier, this is an important safeguard. The response also emphasises that the process of obtaining an assistance order will require a lawful warrant as the basis for the order, and as a result will be subject to the review and supervision by an independent and impartial body. The response explains that this 'will assure the Australian community that this power (both existing and proposed orders) will be based on the public interest'. As noted in the initial analysis, ensuring that such orders can only be granted through a warrant process is also an important safeguard.

2.284 As to the extent to which the warrant process is a sufficient safeguard, the minister's response provides the following example relating to the proposed amendments to the Crimes Act in Schedule 3 of the bill:

> The proposed and existing provisions will be subject to safeguards and oversight mechanisms. Currently, the Crimes Act requires law enforcement officers to apply to a magistrate for assistance to access a device. Before a Judge or AAT member issues a person-based warrant, subsection 3E(2) states that they must be satisfied that there are reasonable grounds for suspecting that the person has in his or her possession, or will within the next 72 hours have in his or her possession, any evidential material. Evidential material is anything relevant to an indictable offence or summary offence that has been or will be committed.

> A number of additional conditions in subsection 3LA(2) must be met before a magistrate grants an order to allow enforcement to compel a person to give assistance accessing data. The person must be connected to the device (for example, as the device owner or user) and have the relevant knowledge to enable them to access the device.

2.285 The response also emphasises that similar safeguards apply to the proposed new assistance orders in Schedules 2 and 5 of the bill. As noted in the initial analysis, similar safeguards exist in relation to the proposed amendments to the Customs Act in Schedule 4.[104]

2.286 However, the minister's response does not address the concerns raised in the initial analysis as to the whether the measures are sufficiently circumscribed. The provisions may compel assistance from a broad range of persons. 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, or a person who has used the computer, or a person who is or was a system administrator for the computer.[105] As noted in the initial analysis, while those persons can only be compelled to assist where the person has relevant knowledge of the computer or the measure is applied to protect data held in the computer, 'relevant knowledge' is not defined. The minister's response does not provide any information as to the definition of 'relevant knowledge'.

2.287 Thus, while there are likely to be a number of circumstances in which compelling a device or computer owner or user to assist law enforcement to enable them to access to the device would be a proportionate limitation on the right to privacy, it remains unclear whether it is proportionate for the broader categories of persons, such as employees of owners of a device. This is of particular concern in light of the significant penalties for non-compliance with an assistance order. For example, non-compliance with an assistance order under the SD Act in Schedule 2 of the bill is punishable by imprisonment for 10 years or 600 penalty units or both,[106] and imprisonment of 5 to 10 years or 300 to 600 penalty units or both in relation to the provisions under the Crimes Act and Customs Act in Schedules 3 and 4 of the bill.[107] The minister's response states that the increased penalties 'reflect the

---

104 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) p.56.

105 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 in relation to mandatory assistance with computers or devices, see sections 201A(2) of the Customs Act and section 3LA(2)(b) of the Crimes Act.

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

107 See proposed section 3LA(5) of the Crimes Act in Schedule 3 of the bill and proposed section 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.

importance of assistance orders to investigations and the deficiencies in the current regime', but does not otherwise provide any information as to the proportionality of these penalties for non-compliance with an assistance order, particularly as they would apply to persons who do not own the device or computer.

Committee response

2.288 The committee thanks the minister for his response and has concluded its examination of this issue.

2.289 The committee is unable to conclude that the assistance order provisions in Schedules 2, 3, 4 and 5 are compatible with the right to privacy.

Interception of communications under ASIO computer access warrants

2.290 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'[108]).

2.291 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.[109]

2.292 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.[110] As a consequence, ASIO will no longer be required to obtain the second warrant under the TIA Act for this purpose.

Compatibility of the measure with the right to privacy: initial analysis

2.293 The initial analysis raised questions as to the compatibility of the measure with the right to privacy. As acknowledged in the statement of compatibility, the interception of communications under ASIO computer access warrants engages and

---

108 '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*.

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

110 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.

limits the right to privacy because interception (including interception to enable remote access to a computer) is 'inherently privacy intrusive'.[111]

2.294 The stated objective of the measure was for 'ASIO to have effective powers to execute its statutory function to protection national security'.[112] The statement of compatibility explained that the current arrangements caused administrative inefficiency by requiring ASIO to prepare two warrant applications addressing different legal standards for the purpose of executing a single computer access warrant.[113] The initial analysis stated that the objectives of enhancing operational effectiveness of ASIO and addressing an 'administrative inefficiency' did not appear to constitute a pressing and substantial concern for the purposes of international human rights law, and that further information as to the legitimate objective of the measure was required. The initial analysis also raised questions as to whether the measures were rationally connected and proportionate to these objectives.

2.295 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 58-61.[114]

2.296 The committee therefore sought the advice of the minister as to the compatibility of the measures with the right to privacy, 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 as to how the measures address a pressing and substantial concern);
- whether the measures 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).

Minister's response and analysis

2.297 In relation to 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, the minister's response states:

---

111 SOC, p.15 [50].

112 SOC, p.15 [50].

113 SOC, p.15 [52].

114 Parliamentary Joint Committee on Human Rights, Report 11 of 2018 (16 October 2018) pp. 58-61 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

> Access to mobile devices is increasing, and so is the use of various types of mobile devices, in committing crimes or acts of terrorism. As a consequence, accessing such devices is incredibly important to ensuring our law enforcement and national security agencies have effective powers to combat those threats. However, new mobile devices are constantly being created, and respective software subject to near daily updates. Computer access capabilities do not work in a vacuum and require some degree of knowledge of the device and systems before execution. As a consequence, it may be necessary to use interception capabilities in order to technically enable computer access. For example, it may be vital that communications from the handset be intercepted in order to determine the make and model of the device. The TIA Act has been amended in order to provide for this incidental interception.
>
> The legitimate objective of this measure is the protection of national security, public order and the Australian community. Having law enforcement agencies and ASIO meet the thresholds for the existing interception regime may also mean that a CAW [ASIO computer access warrant] cannot be executed, or significant delay imported into the process. Where operational effectiveness requires the use of interception capabilities in order to determine device details, were this proposed amendment not to be introduced, there may be significant delay, or an inability to execute a judicially approved CAW. Delay, or inability, may result in either significant loss of evidence or the continuation of serious crime.

2.298 The information provided by the minister identifies the pressing and substantial concern that the measures seek to address, and clarifies that the objective of the measures is the protection of national security, public order and the Australian community. In light of this information it appears the measures pursue a legitimate objective for the purposes of international human rights law. Enabling interception to give effect to an ASIO computer access warrant also appears to be rationally connected to this objective.

2.299 In the initial analysis, a number of safeguards proposed to be introduced into the TIA Act relating to ASIO computer access warrants were identified as being relevant to determining the proportionality of the measure, including:

- prohibitions on ASIO, the Inspector-General of Intelligence and Security and the Director-General of Security using the computer access intercept information in connection with the performance of those organisations' functions;[115]

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

- prohibitions on disclosing information to staff members of certain agencies except for limited purposes of testing and development;[116] and
- a prohibition on giving ASIO computer access intercept evidence in an exempt proceeding, except in certain circumstances.[117]

2.300 As to proportionality, the minister's response provides the following additional information as to the safeguards in place to protect the right to privacy:

> Incidental interception to give effect to a CAW [ASIO computer access warrant] is strictly limited to only what is required to give effect to that warrant. Law enforcement agencies and ASIO are not permitted to use that evidence for intelligence or evidentiary purposes. Should an agency wish to pursue interception for those purposes, they must seek an interception warrant.
>
> The Government views that incidental interception is rationally connected to computer access and is a necessary, proportionate and reasonable measure to ensure available judicially approved powers can actually be executed.
>
> CAWs are subject to strict tests and either must have judicial authorisation in the case of law enforcement agencies, or ministerial authorisation for ASIO. Further, strict restrictions are proposed which ensure that intercepted information[118] obtained for the purpose of executing a CAW is only used for the purposes of that execution. In order for intercepted information to be used for evidentiary or intelligence purposes, an interception warrant must be obtained.

2.301 The clarification from the minister that interception by ASIO pursuant to the ASIO computer access warrant would be strictly limited to the purpose of executing the warrant and that ASIO are not permitted to use evidence from the interception for intelligence or evidentiary purposes without an interception warrant is useful in assessing the proportionality of the measure. However, notwithstanding the narrow function of the interception power in the ASIO computer access warrant, it is noted that the impact on the right to privacy as a result of an ASIO computer access warrant more broadly remains potentially significant.

---

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

117 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.

118 Intercepted information obtained due to assisting in the execution of an ASIO computer access warrant is strictly separated from what would ordinarily be obtained under an interception warrant; see, for example, 'general computer access intercept information' included within the definitions under the TIA Act.

2.302 The initial analysis stated that by expanding the operation of the ASIO computer access warrants allowing 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 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.[119]

2.303 In contrast, the threshold for obtaining an ASIO computer access warrant under the ASIO Act (which is the standard that would apply if the bill is passed) 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 security.[120] This test is very broad, and 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 obtain a telecommunications interception warrant.[121] By outlining the difficulties associated with meeting the current threshold for the interception regime (including that existing ASIO computer access warrants cannot be executed or are delayed), the minister's response appears to suggest that the higher threshold under the TIA Act is not reasonably practicable for the ASIO computer access warrants, and that the lower threshold under the ASIO Act is necessary. However, noting the potentially significant impact on the right to privacy that may occur as a result of ASIO computer access warrants, and the fact that the

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

120 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.

121 EM, p. 80 [354].

regime is overseen by the Attorney-General and not by judicial authorisation, in the absence of further information from the minister as to why adopting a lower threshold for such warrants is strictly necessary, it remains unclear whether this is the least rights restrictive approach.

Committee response

2.304 The committee thanks the minister for his response and has concluded its examination of this issue.

2.305 The preceding analysis indicates that there is a significant risk that the proposed amendments to ASIO computer access warrants to allow ASIO to intercept a communication passing over a telecommunications system may be incompatible with the right to privacy. It is recommended that the scheme be monitored to ensure that any limitation on the right to privacy be only as extensive as is strictly necessary to achieve the legitimate objectives of the measure.

Assistance to foreign countries in relation to data held in computers

2.306 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'[122] to 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[123] (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

122 '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.

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

(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.[124]

2.307 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).[125]

2.308 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'.[126] 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.[127]

Compatibility of the measure with multiple rights: initial analysis

2.309 The initial analysis noted that 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.[128] For example, it was noted that 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

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

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

126 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.

127 See EM, p. 84 [395].

128 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.

being tried and convicted of a criminal offence that carries the death penalty.[129] The statement of compatibility did not acknowledge that the amendments to the MA Act introduced in Schedule 2 of the bill may engage multiple human rights.

2.310 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 63-64.[130]

2.311 The committee reiterated its previous statement 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.

2.312 Because 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 sought the advice of the Minister on the compatibility of the amendments to that Act with these human rights.

Minister's response and analysis

2.313 In relation to undertaking a review of the human rights compatibility of the MA Act as a whole, the minister's response states:

> Australia's mutual assistance regime and procedures are frequently considered and assessed. The Government is satisfied with the current operation of MACMA [*Mutual Assistance in Criminal Matters Act 1987*]. The operation of Australia's mutual assistance laws are subject to Parliamentary scrutiny through the Joint Standing Committee on Treaties hearings for new treaties and reports by the Parliamentary Joint Committee on Human Rights. Australia conducted a comprehensive review of its mutual assistance arrangements which resulted in amendments that were passed in 2012.

---

129 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 Human Rights Committee, *Concluding observations on the fifth periodic report of Australia*, CCPR/C/AUS/CO/5 (7 May 2009) [20].

130 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 63-64 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

2.314 It is acknowledged that there are a number of mechanisms through which the MA Act has been, and is able to be, reviewed. However, those mechanisms do not necessarily involve consideration of the compatibility of the MA Act with Australia's international human rights law obligations. As the MA Act was legislated prior to the establishment of the committee, the Act itself was not required at that time to be subject to a foundational review for its human rights compatibility in accordance with the terms of the *Human Rights (Parliamentary Scrutiny) Act 2011*. It is also noted that the amendments passed in 2012 pre-dated the establishment of the committee and so were not the subject of a full analysis for compatibility with human rights. However, it is noted that the committee has raised concerns about the human rights compatibility of provisions in the MA Act on a number of occasions.[131] It would therefore be of considerable assistance if the MA Act was subject to a foundational human rights assessment.

2.315 For the rights that are engaged by the measures that may be subject to permissible limitations,[132] the minister's response states that the objective of the measures is to 'ensure that no matter the origin of serious crime and terrorism, Australian law enforcement can assist foreign law enforcement agencies through mutual assistance processes to use investigatory powers within Australia'. The minister's response identifies the following pressing and substantial concern which the measures seek to address:

> The reforms in the Bill will strengthen the available tools for the purposes of mutual assistance assisting in the enforcement of foreign serious crime and terrorism. These crimes frequently involve aspects which transcend borders and involve large criminal networks that may span the globe. International crime cooperation must evolve to ensure that tools that would otherwise be available to domestic law enforcement can be used to assist foreign countries where it is appropriate and reasonable to do so.

2.316 Based on this information it appears the proposed amendments to the MA Act in Schedule 2 pursue a legitimate objective for the purposes of international human rights law. Providing assistance to a foreign country in relation to data held in computers also appears to be rationally connected to this objective.

2.317 As to proportionality and the safeguards in the bill where a foreign country requests access to data held on a computer, the minister's response provides the following information:

---

131 See, Parliamentary Joint Committee on Human Rights, *Tenth Report of 2013* (26 June 2013) pp. 56-61; Parliamentary Joint Committee on Human Rights, *Report 2 of 2017* (21 March 2017) pp. 3-7.

132 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.

> Use of the new power requires both the Attorney-General's approval and the approval of a judicial officer (or AAT member). For example, if a foreign country requests access to data held on a computer, the Attorney-General must be satisfied of certain things before authorising an eligible law enforcement officer to apply for a computer access warrant. Part IIIB includes specific safeguards such as ensuring a minimum threshold (3 or more years' imprisonment) and a tangible link between the request and a device in Australia. Further, in addition to the general power to impose conditions on the provision of assistance in section 9 of MACMA ([MA Act]), the proposed amendments enable the Attorney-General to request appropriate undertakings in relation to:
>
> - the information being used only for the purposes in which it was sought;
> - destruction requirements subsequent to its use; and
> - any other matter the Attorney-General may consider appropriate.
>
> These amendments are made for the purpose of international law enforcement in relation to serious crimes and are limited to interferences that are necessary to achieve this. Computer access powers are a vital tool not only domestically but also where those powers may be exercised by a foreign jurisdictions law enforcement to assist Australian investigations into serious crime and terrorism.

2.318 These are important safeguards and may be capable in practice of ensuring that any limitation on human rights that may arise from the measures is permissible. However, in order to determine the proportionality of the measures it is necessary to consider the broader operation of the MA Act and how it would interact with the measures in the bill.

2.319 In this respect, the minister's response states:

> Schedule 2 amendments which relate to MACMA do engage multiple human rights (such as the right to life) (Article 6 and Article 17 of the ICCPR, respectively). However, the Government views that these measures pursue the legitimate objective of assisting in public safety, public order and national security in assisting foreign countries where appropriate to do so. This appropriateness is shaped by the current mandatory and discretionary grounds of refusal within MACMA. Australia's mutual assistance domestic framework ensures that there are human rights protections in place for the purposes of any incoming request from a foreign country and stand as an appropriate yardstick in determining whether undertaking powers, such as that under Part IIIBB would meet reasonable community expectations as to balancing human rights and law enforcement/national security interests.

2.320 The minister's response then identifies the safeguards in the MA Act that protect the right to life. In particular, 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'.[133] The minister's response notes that 'special circumstances' is not defined in the MA Act but points to the explanatory memorandum to that Act which 'envisages that it may include where a requesting country has provided an undertaking that the death penalty will not be imposed, or if it is imposed, will not be carried out'. The response also explains that where a person has not yet been charged, arrested, detained or convicted, there is a general discretion to refuse assistance.

2.321 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 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.[134]

2.322 The prohibition on providing assistance to a foreign country where that assistance relates to a person arrested, detained, charged or convicted of an offence where the death penalty may be imposed is an important safeguard. However, while the minister identifies some examples of what may constitute 'special circumstances' in which an assistance request should be granted notwithstanding the potential application of the death penalty, it is noted that 'special circumstances' is not defined. Therefore, while the receipt of an undertaking that the death penalty will not be imposed would likely be consistent with Australia's obligations under Article 6 of the ICCPR,[135] the absence of a definition of 'special circumstances' raises concerns that the MA Act as drafted creates a risk that the Attorney-General may exercise their discretion in a manner that is incompatible with Australia's international human rights obligations with respect to the death penalty. The committee has previously

133 Section 8(1A) of the MA Act.

134 See UN Human Rights Committee, *Concluding observations on the fifth periodic report of Australia*, CCPR/C/AUS/CO/5 (7 May 2009) [20].

135 The committee has recently considered when examining the *Extradition Act 1988* that the provision of prior undertakings that the death penalty would not be imposed or implemented, and monitoring compliance with such undertakings, was likely to be compatible with Australia's obligations under Article 6 of the ICCPR. However, the committee noted that the requirements under that Act could be strengthened by legislating a requirement that a person not be extradited if, notwithstanding the receipt of an undertaking, there remains a real risk that the death penalty will be carried out upon the person: Parliamentary Joint Committee on Human Rights, *Report 5 of 2018* (19 June 2018) p. 88.

expressed concern that the MA Act allows assistance to be given to a foreign country if there are 'special circumstances', even if the death penalty may apply.[136]

2.323 As to the general discretion to refuse assistance where a person has not yet been charged, arrested, detained or convicted, but where the Attorney-General believes the provision of assistance may result in the death penalty being imposed on a person,[137] it is not clear whether this would be a sufficient safeguard for the purposes of international human rights law due to its discretionary nature. This is because unconstrained discretion is generally insufficient for human rights purposes to ensure that powers are exercised in a manner compatible with human rights. That is, it is possible that the Attorney-General may decline to exercise their discretion not to provide assistance to a foreign country even though there is a real risk that such assistance may result in the death penalty being imposed on a person. The UN Human Rights Committee has emphasised the importance of laws using precise criteria and not conferring unfettered discretion on those charged with their execution,[138] and that a legislative provision in very general terms does not, of itself, provide a satisfactory legal safeguard.[139]

2.324 The minister's response also identifies a number of other safeguards, including the requirement to refuse requests where there are substantial grounds for believing that if the request was granted the person would be in danger of being subject to torture.[140] This is an important safeguard. However, the committee has previously expressed concern that there is no explicit obligation to consider refusing assistance where a person may be subject to cruel, inhuman or degrading treatment or punishment.[141] In this respect the minister's response further states that the general discretion to refuse assistance if 'it is appropriate, in all the circumstances of the case, that the assistance requested should not be granted'[142] can 'cover any concerns about cruel, inhuman or degrading treatment of punishment'. However,

---

136 Parliamentary Joint Committee on Human Rights, *Tenth Report of 2013* (26 June 2013) p.60.

137 Section 8(1B) of the MA Act provides that the Attorney‑General may refuse a request for assistance in circumstances where he or she believes that the provision of assistance may result in the death penalty being imposed on a person, and, after taking into consideration the interests of international criminal co-operation, he or she is of the opinion that in the circumstances of the case, the request should not be granted.

138 UN Human Rights Committee, *General Comment 27: Freedom of Movement (Article 12)* (1999) [13].

139 *Pinkey v Canada,* UN Human Rights Communication No.27/1977 (1981) [34]. See also *Hasan and Chaush v Bulgaria,* European Court of Human Rights Application No.30985/96 (26 October 2000) [84]-[86]; *Maestri v Italy,* European Court of Human Rights Application No.39748/98 (17 February 2004) [30]-[31].

140 Section 8(1)(ca) of the MA Act.

141 Parliamentary Joint Committee on Human Rights, *Tenth Report of 2013* (26 June 2013) p.60.

142 Section 8(2)(g) of the MA Act.

for the reasons stated earlier, the general discretion to refuse assistance may not be a sufficient safeguard for the purposes of international human rights law.[143] This is particularly the case given that the prohibition on torture, cruel, inhuman or degrading treatment or punishment is absolute and may never be subject to permissible limitations.

2.325 As to the proposed amended definition of 'protected information' which would enable the Attorney-General to provide information obtained in response to a computer access warrant to a foreign country in response to a mutual assistance request, the minister's response provides the following information:

> The specific inclusion of computer access information as part of the definition of 'Protected information' under section 13A of MACMA accords with the existing practice of lawfully obtained surveillance device information and intercepted information. Notably the Attorney-General can only provide such an authorisation in relation to an offence which is a serious offence punishable by a maximum penalty of imprisonment for 3 years or more. In giving such an authorisation the Attorney-General may specify the uses to which the material may be put.
>
> The provision of that information for the purposes of mutual assistance will continue to be governed by the existing safeguards under sections 8 and 9 of MACMA.

2.326 As noted above, however, the safeguards in section 8 of the MA Act may not be sufficient for the purposes of international human rights law, due to the considerable discretion that is left to the Attorney-General when determining whether to provide assistance. The safeguard in section 9, which allows for the Attorney-General to provide assistance subject to such conditions as the Attorney-General determines, is also an important safeguard but does not necessarily provide a complete answer to whether the limitations on human rights that may arise from providing assistance to foreign countries are permissible.

Committee response

2.327 The committee thanks the minister for his response and has concluded its examination of this issue.

2.328 The committee reiterates its previous concern as to the human rights compatibility of allowing assistance to be given to a foreign country, even if the death penalty may apply, if there are 'special circumstances', and that there is no

143 The committee recently concluded in the context of the Extradition Act 1988 that the general discretion in section 22(3)(f) of that Act for the minister to determine whether to surrender a person is not likely to be sufficient to ensure compatibility with Australia's absolute obligations under article 7 of the ICCPR not to extradite persons who may be subject to cruel, inhuman or degrading treatment or punishment if extradited: Parliamentary Joint Committee on Human Rights, *Report 5 of 2018* (19 June 2018).

explicit obligation to consider whether a person may be subject to cruel, inhuman or degrading treatment or punishment.

2.329 The committee otherwise considers that there is a risk that the proposed amendments to the *Mutual Assistance in Criminal Matters Act 1987* in Schedule 2 of the bill may be incompatible with human rights, noting however that much will depend on how the applicable safeguards operate in practice.

2.330 The committee reiterates its previous view 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.

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

2.331 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 search warrant obtained pursuant to the Crimes Act and *Customs Act 1901* (Customs Act), respectively.[144]

2.332 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. 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 the relevant data which are likely to be as effective'.[145]

2.333 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

144 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.

145 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.

electronic equipment, for the purpose of obtaining access to 'account-based data'[146] of a living or deceased person who is/was the owner or lessee of the warrant computer, or who uses or has used the warrant computer,[147] to determine if it is evidential material of a kind specified in the warrant.

Compatibility of the measure with the right to privacy: initial analysis

2.334 The statement of compatibility acknowledges that the measure engages the right to privacy by enabling law enforcement agencies and the Australian Border Force 'to access private communications and other information on a device using a range of methods'.[148]

2.335 The initial analysis noted that the stated objective of the measure, the protection of national security and public order, was capable of constituting a legitimate objective, however further information was required to determine whether the measures addressed a pressing and substantial concern. The initial analysis also raised questions as to the proportionality of the measures, in particular the impact of the measures on third parties who are lawful users of the computer or device subject to the warrant.

2.336 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 65-67.[149]

2.337 The committee therefore sought the advice of the minister as to compatibility of the measures with the right to privacy, 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.

---

146 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.

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

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

149 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 65-67 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

Minister's response and analysis

2.338 In relation to the pressing and substantial concern which the measures seek to address, the minister's response provides the following information:

> The introduction of provisions which allows for the remote access of computers under warrant addresses current operational issues experienced by law enforcement and the Australian Border Force (ABF) when executing warrants, and maintains the integrity of evidential material. These provisions do not provide law enforcement and the ABF with any unfettered, additional powers but ensures that agencies can access lawfully obtained data and information, which are integral to investigating and prosecuting serious criminals and terrorists. As a result, these new powers are a necessary and proportionate limitation on the right to privacy.
>
> Currently, the Crimes Act 1914 and Customs Act 1901 requires law enforcement and the ABF to be physically located at the warranted premises when executing an overt search warrant to seize and search computers. Remote access to computers ensures that agencies can rely upon specialist equipment and expertise located offsite which is critical to obtaining data and information related to protecting national security and the public order. Executing search warrants at premises also presents additional risks to the safety of law enforcement and ABF officers. The ability to remotely execute these warrants reduces direct contact between law enforcement and potentially dangerous criminals and terrorists. This also minimises the risks of harm to officers or damage to expensive equipment.
>
> Remote access conforms with forensic best practices and maintains the integrity of evidential material. Specifically, these measures reduce the risk of altering, damaging or destroying evidence by using a suspect's computer, consistent with the requirements under the current search warrant provisions. Maintaining the integrity of evidential material is critical for prosecuting and investigating those illegal activities that impact national security and public order.

2.339 In light of this information, on balance it appears that the measures pursue a legitimate objective for the purposes of international human rights law.

2.340 The minister's response also identifies a number of safeguards in the bill to limit the impact on the right to privacy of third parties who are lawful users of a computer or device subject to warrant to access the computer remotely:

> … the Bill includes provisions to minimise the impact on the right to privacy of innocent third-parties during the execution of a warrant. As commented in the report, the Bill expressly prohibits the addition, deletion or alteration of data if it is likely to interfere with communications in transit or the lawful use by other persons of a computer. This prevents a warrant from being used to disrupt or deny a service to other innocent parties that may use the computer. The Bill also protects the data of innocent third

> parties by prohibiting law enforcement and the ABF from engaging in activities that may cause the material loss or damage to other persons lawfully using a computer.
>
> The exception to these limitations is in cases where the addition, deletion or alteration of data, or obstruction of lawful use by other persons of a computer is necessary to give effect to the warrant. While this may be privacy intrusive on third-parties, the Bill includes tight constraints to ensure any interference is reasonable, proportionate and necessary. Importantly, a warrant can only be issued by a judge or a nominated member of the AAT. These are independent authorities that routinely assess the lawfulness and proportionality of law enforcement requests and, prior to issuing a warrant, must consider the impact to privacy and the existence of alternative means of obtaining information. The Bill includes clear thresholds to ensure that warrants are only issued when necessary and proportionate. Specifically, warrants can only be issued if the issuing officer is satisfied that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, evidential material on the premises or person.

2.341 These are important safeguards which may be capable, in practice, of ensuring that any limitation on the right to privacy due to remote access to data is proportionate. The threshold for obtaining the warrant is also an important safeguard. The minister's response also identifies a number of additional safeguards to ensure that the measures 'do not adversely affect privacy and the integrity of the data or device'. This includes a requirement that the issuing officer consider alternative means to obtaining evidence. As noted in the initial analysis, the requirement that the power to access data remotely can only be exercised if it is reasonable in all the circumstances to do so, having regard to other methods of obtaining access which are likely to be as effective, is an important safeguard.

2.342 In terms of whether there may be other less rights restrictive measures available, such as providing an exhaustive list in legislation for when it will be 'reasonable in all the circumstances' to access data remotely, the minister's response states:

> Providing an exhaustive list in legislation … may prevent the Bill from being able to adapt to changes in technology and create further operational issues in the future. However, broadly speaking, the issuing of warrants is restricted to meeting the ABF's functions and must relate to an offence listed in the Customs Act, the Commerce (Trade Descriptions) Act 1905 or the Criminal Code. Offences for which a warrant can be issued includes the importation of narcotics or firearms. Similarly, proposed CAWs under the Crimes Act can only be issued for indictable or summary offences.

2.343 However, under an ordinary search warrant of a premises a person targeted by the warrant would be present, aware the search is being carried out and of the material taken and therefore would be in a better position to ascertain whether the search warrant is undertaken in accordance with the warrant or with the law. Where

a computer is accessed remotely, there would appear to be limited opportunity for the target of the warrant to know whether access is in accordance with the terms of the warrant or the law more generally. To that extent, the safeguards relating to authorising and issuing warrants are particularly important, and so the absence of any guidance as to what constitutes 'reasonable in all the circumstances' raises concerns as to whether the limitation on the right to privacy is proportionate.

Committee response

2.344 The committee thanks the minister for his response and has concluded its examination of this issue.

2.345 The preceding analysis indicates that there is a risk that remote access of computers pursuant to a warrant under the Crimes Act and Customs Act may be incompatible with the right to privacy. However, noting the safeguards that apply before law enforcement and the Australian Border Force may access computers remotely, much will depend on how the scheme operates in practice. It is recommended that the scheme be monitored to ensure that any limitation on the right to privacy be only as extensive as is strictly necessary to achieve the legitimate objectives of the bill.

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

2.346 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.[150]

Compatibility of the measure with the right to privacy: initial analysis

2.347 The statement of compatibility acknowledges that being able to search a person in order to gain access to a device is inherently intrusive and therefore engages and limits the right to privacy.[151] The initial analysis stated that the measure would appear to pursue a legitimate objective (protecting national security and public order) and appeared to be rationally connected to the objective. However, the initial analysis raised questions as to the proportionality of the measure, including whether the measures were sufficiently circumscribed and accompanied by adequate safeguards.

150 See proposed section 199A(1) of the Customs Act in Schedule 4 of the bill. Evidential material is anything relevant to an indictable or summary offence: see SOC, p.24 [113].

151 SOC, p.24 [115].

2.348 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 67-68.[152]

2.349 The committee therefore sought the advice of the minister as to the proportionality of the limitation on the right to privacy, 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.

Minister's response and analysis

2.350 The minister's response provides the following information as to the proportionality of the limitation on the right to privacy:

> While the nature of searching a person in order to gain access to a device is inherently intrusive, it is a necessary and proportionate limitation on the right to privacy as it provides a targeted law enforcement tool designed to assist the ABF to effectively investigate crimes in the current technological environment. These amendments recognise that information is often stored on devices, held physically by persons, and that an inability to access this information may impede legitimate investigations and prosecutions. The Bill reflects criminals' increased reliance on portable devices such as smart phones to communicate and conduct illegal activities.
>
> The Bill also addresses existing operational issues which have adversely impacted ABF investigations. Existing search warrants available to the ABF are limited to an ordinary search or frisk search for a computer or data storage device in a premises and are not a general search warrant power relating to persons. These existing warrants inhibit the ABF's ability to target specific persons of interest at a premises and fails to account for criminals operating from different locations. The Bill addresses these operational issues by allowing the ABF to apply for a warrant that effectively and efficiently targets individuals.
>
> The amendments to the Customs Act are supported by robust safeguards to ensure a warrant is only issued to meet ABF objectives and, that in executing a warrant, the ABF do not adversely impact privacy and the integrity of the data or device. These safeguards include:
>
> - Warrants are authorised by a judicial officer to ensure a warrant is issued only when necessary to meet the ABF's objectives and is proportionate to the potential offence.
> - The amendments provide a strict time limit of seven days to undertake a search authorised by the warrant.

152 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 67-68 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

- The executing officer must believe on reasonable grounds that the computer or data storage device is evidential material and that the seizure is necessary to prevent the concealment, loss or destruction of that item.
- 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

Specific judicial officer considerations are circumscribed by the legislation. Where this relates to search warrants relating to a person, the judicial officer may issue that warrant where there are reasonable grounds to suspect the person has in his or her possession, or will have in the next 72 hours, any computer, or data storage device, that is evidential material.

2.351 The minister's response also reiterates the safeguards that apply more broadly in relation to the warrants to minimise the impact on the right to privacy of innocent third-parties during the execution of a warrant, including the prohibition on the addition, deletion or alteration of data if it is likely to interfere with communications in transit or the lawful use by other persons of a computer, and the prohibition on the ABF engaging in activities that may cause the material loss or damage to other persons lawfully using a computer. However, for the reasons stated above in relation to remote access of computers under the Crimes Act and Customs Act, it is not clear whether these safeguards would be sufficient.

2.352 However, in the particular context of the ordinary or frisk search warrants, the requirement for a judicial officer to authorise the warrants, and the time limit of seven days for executing the warrant, are capable of functioning as relevant safeguards insofar as it may assist in ensuring that warrants are appropriately circumscribed, minimally invasive and time-limited.[153] Further, it appears that the safeguards identified by the minister that apply to the search warrant may be capable, in practice, of ensuring that any limitation on the right to privacy that arises from the Australian Border Force being able to frisk search persons in order to obtain a device would be proportionate. However, much will depend on how the powers are exercised in practice.

Committee response

2.353 The committee thanks the minister for his response and has concluded its examination of this issue.

2.354 The preceding analysis indicates that the safeguards associated with the issue of a warrant authorising an ordinary search or a frisk search of a person by the Australian Border Force may be capable, in practice, of ensuring that the limitation on the right to privacy of persons subject to an ordinary or frisk search is

153 SOC, p.24 [115].

proportionate. However, much will depend on how the scheme operates in practice. It is recommended that the scheme be monitored to ensure that any limitation on the right to privacy be only as extensive as is strictly necessary to achieve the legitimate objectives of the bill.

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

2.355 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,[154] and 72 hours under the Customs Act.[155]

Compatibility of the measure with the right to privacy: initial analysis

2.356 The statement of compatibility acknowledges that moving a person's computer or data storage device engages the right to privacy as it may restrict a person's access to personal information.[156] The initial analysis raised questions as to whether extending the timeframe to 30 days addressed a pressing and substantial concern, including information as to how current timeframes are inadequate or insufficient. The initial analysis also raised questions as to proportionality, including 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 could be sought and the time period for those extensions.

2.357 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 69-70.[157]

2.358 The committee therefore sought the advice of the minister as to the compatibility of the measure with the right to privacy, 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);

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

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

156 SOC, p.23 [112]; p. 26 [131].

157 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 69-70 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

- 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).

Minister's response and analysis

2.359 The minister's response provides the following information as to the pressing and substantial concern which the measures seek to address:

> The provisions in the Bill that amends the Crimes Act and Customs Act to increase existing timeframes for the temporary removal of devices is a proportionate limitation on the right to privacy as it ensures that the integrity of evidential material is maintained and addresses operational issues which have adversely impacted legitimate law enforcement and ABF investigations. The extended timeframes are not intended to allow for the arbitrary access of data (that access has already been authorised), but to ensure law enforcement and the ABF are able to examine complex and sophisticated modern devices for evidential material, and to ensure that evidential material is handled appropriately.
>
> The existing timeframes for devices to be moved for examination fails to take into regard the complex nature of modern technology. Specifically, the timeframes are inadequate for law enforcement and the ABF to properly analyse modern devices, such as smart phones, laptops and portable hard drives, which rely on sophisticated and complex technology including encryption to protect data and communications. These new technologies means [sic] that agencies are unable to immediately access content on modern devices for the purpose of determining whether it is evidential material. To access and examine this content, agencies are increasingly relying upon the use of specialised equipment and the expertise of industry which can be time consuming and has not been factored into the existing timeframes. The vast volumes of data produced by modern devices adds a layer of complexity and increases the timeframes required for law enforcement and the ABF to determine if evidential material is located on the device. As a result of modern technology, law enforcement and the ABF are required to examine exponentially larger volumes of content today in comparison to when the provisions for the existing timeframes were introduced. There is also the challenge that encryption presents with more devices utilising encryption as a standard. These issues have limited the ability of law enforcement and the ABF to determine if evidential material is in a lawfully seized device

> and, as a result, have impacted legitimate investigations into matters related to protecting national security and the public order.
>
> The current timeframes, particularly for the ABF, also do not account for many of the internal authorisations and relocation processes which must occur to ensure transparency and accountability, as well as secure relocation of devices once moved. If accessing the device is not possible, there may a requirement for significant amounts of time to utilise computer expertise to penetrate the device (if possible). This intrudes on investigation timeframes and particularly impacts the ability for law enforcement and the ABF to examine devices for evidential material.

2.360 This information provided by the minister indicates that the measures address a pressing and substantial concern, in particular 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. Accordingly, it appears the measures pursue a legitimate objective for the purposes of international human rights law. The measures would also appear to be rationally connected to this objective.

2.361 As to proportionality, the minister's response provides the following information as to the safeguards that apply when determining whether a device can be temporarily removed for examination:

> The Bill is supported by safeguards and limitations which ensures that the extended timeframes prevents law enforcement and the ABF from arbitrarily accessing data and intruding on privacy. The temporary removal of a device for examination is only permitted under warrant which is issued by a judge or AAT member after considering whether the warrant is reasonable, proportionate and necessary. These are independent authorities that routinely assess the lawfulness and proportionality of law enforcement requests. The issuing of a warrant can only occur if the issuing officer is satisfied that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, evidential material on the premises or person. This ensures that warrants are not issued for arbitrary reasons.
>
> Devices must be returned to the premises or person after 30 days which, as detailed above, this provides adequate opportunity for law enforcement and the ABF to examine devices for evidential material. 30 days will be the maximum period allowed for law enforcement and the ABF to undertake device interrogation. In many instances, it is expected the 30 days will be sufficient for these activities to take place.

2.362 The safeguards identified by the minister, including the requirement for judicial authority in order to obtain the warrant, are important safeguards. Based on this information, it appears that the measure may be capable of being a proportionate limitation on the right to privacy.

2.363 However, it is noted that beyond stating that 30 days is the maximum period allowed and that 30 days will be sufficient for the activities to take place, the minister's response does not address the concerns raised in the initial analysis as to whether extending the time period to 30 days represents the least rights restrictive approach. It is not clear, for example, whether the same objectives could be achieved by, for example, extending the time period to less than 30 days. The statement of compatibility and the minister's response also do not identify any safeguards to ensure the measure does not limit the right to privacy any more than necessary, nor do they consider the impact of, for example, holding a person's computer for a month.[158]

Committee response

2.364 The committee thanks the minister for his response and has concluded its examination of this issue.

2.365 The preceding analysis indicates that the proposed amendments to the Crimes Act and Customs Act which extend the time allowed for electronic devices moved under warrant to be kept for analysis for up to 30 days may be compatible with the right to privacy. However, it is noted that the minister's response did not explain why extending the time period to 30 days represented the least rights restrictive approach, and so there is a risk that the measures may not constitute a proportionate limitation on the right to privacy in an individual case. It is suggested the scheme be monitored to ensure that any limitation on the right to privacy go only as far as is strictly necessary to achieve the legitimate objectives of the measure.

Release from civil liability for providing voluntary assistance to ASIO

2.366 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.[159]

Compatibility of the measure with the right to an effective remedy: initial analysis

2.367 The initial analysis noted that 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 remedy against that person. The initial analysis noted that because 'conduct' was not defined in the bill,[160] it could potentially encompass a wide range of acts that could impact individual rights.

---

158 Keeping a person's computer for 30 days may also impact other rights, such as the right to work.

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

160 Except insofar as it specifies some conduct which will not attract immunity from civil liability, including a requirement that the conduct not be an offence: see section 21A(1)(b) of the ASIO Act in Schedule 5 of the bill.

2.368 The full initial human rights analysis is set out at *Report 11 of 2018* (16 October 2018) pp. 70-71.[161]

2.369 The committee therefore sought the advice of the minister as to the compatibility of the measure with the right to an effective remedy.

Minister's response and analysis

2.370 The minister's response acknowledges that the proposed measure may engage and limit the right to an effective remedy. The response states the objective of the proposed measure is to provide a legal basis for ensuring that those persons or bodies that have access to valuable information which may assist ASIO can assist voluntarily, and is aimed at ensuring that persons or bodies feel confident that they can voluntarily assist where it would contribute to the objective of protecting Australia's national security. The minister's response also explains that the measure is compatible with the right to an effective remedy in light of the list of activities that are excluded from the application of the civil immunity. This includes the requirement that the director-general must have requested the person to engage in conduct, the director-general is satisfied on reasonable grounds that the conduct is likely to assist ASIO in the performance of its functions, the person engages in conduct in accordance with the request, the conduct does not involve the person committing an offence, and the conduct does not result in significant loss of or damage to property.[162] The minister's response also explains that the proposed measure does not provide immunity from criminal liability.

2.371 Based on this information, and noting in particular the types of activities that are excluded from the application of civil immunity, on balance it appears the measure may be compatible with the right to an effective remedy.

Committee response

2.372 The committee thanks the minister for his response and has concluded its examination of this issue.

2.373 The preceding analysis indicates that the measure may be compatible with the right to an effective remedy.

161 Parliamentary Joint Committee on Human Rights, *Report 11 of 2018* (16 October 2018) pp. 70-71 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_11_of_2018.

162 See proposed section 21A(1) of the ASIO Act in Schedule 5 of the bill.

Unexplained Wealth Legislation Amendment Bill 2018

Purpose	Seeks to extend the scope of commonwealth unexplained wealth restraining orders and unexplained wealth orders under the *Proceeds of Crime Act 2002* (POC Act) to state and territory offences; allow participating state and territory agencies to access commonwealth information gathering powers under the POC Act for the investigation or litigation of unexplained wealth matters under state or territory unexplained wealth legislation; amend the way in which recovered proceeds are shared between the Commonwealth, states and territories and foreign law enforcement entities; also seeks to amend the *Telecommunications (Interception and Access) Act 1979* to facilitate information-sharing on unexplained wealth between commonwealth, participating state and territory agencies
Portfolio	Home Affairs
Introduced	House of Representatives, 20 June 2018
Rights	Fair trial; fair hearing; privacy
Previous reports	Report 7 of 2018
Status	Concluded examination

Background

2.374 The committee first reported on the bill in its *Report 7 of 2018*, and requested a response from the Minister for Home Affairs by 29 August 2018.[1]

2.375 The bill passed both Houses of Parliament on 19 September 2018 and received Royal Assent on 3 October 2018.

2.376 The minister's response to the committee's inquiries was received on 14 September 2018. The response is discussed below and is available in full on the committee's website.[2]

Background to the unexplained wealth order regime

2.377 Part 2-6 of the *Proceeds of Crime Act 2002* (POC Act) enables certain orders to be made relating to 'unexplained wealth':[3]

1 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 65-81.

2 The minister's response is available in full on the committee's scrutiny reports page: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports

- unexplained wealth restraining orders, which are interim orders that restrict a person's ability to dispose of, or otherwise deal with, property;[4]
- preliminary unexplained wealth orders, which require a person to appear before a court to enable the court to determine whether or not to make an unexplained wealth order against the person;[5] and
- unexplained wealth orders, which require a person to pay an amount to the commonwealth where the court is not satisfied that the whole or any part of the person's wealth was not derived or realised, directly or indirectly, from an offence against the law of the commonwealth, a foreign indictable offence or a state offence that has a federal aspect. The amount to be paid (the unexplained wealth) is the difference between a person's total wealth and the wealth shown to have been derived lawfully.[6]

Previous committee reports on the compatibility of unexplained wealth orders with human rights

2.378 The committee has previously commented on the human rights compatibility of the unexplained wealth regime. In those reports, the committee raised concerns that the unexplained wealth provisions may involve the determination of a criminal charge for the purposes of international human rights law.[7] Similar concerns have been discussed in the context of the broader underlying regime established by the POC Act for the freezing, restraint or forfeiture of property.[8]

2.379 The committee has previously noted that the POC Act was introduced prior to the establishment of the committee and therefore before the requirement for bills to contain a statement of compatibility with human rights. The committee has therefore previously recommended that the minister undertake a detailed

---

3 'Unexplained wealth' refers to an amount that is the difference between a person's total wealth and the wealth shown to have been derived lawfully: see POC Act, section 179E(2).

4 POC Act, section 20A.

5 POC Act, section 179B.

6 POC Act, section 179E.

7 See, Parliamentary Joint Committee on Human Rights, *Report 1 of 2018* (6 February 2018) p. 121; *Report 12 of 2017* (28 November 2017); *Ninth Report of the 44th Parliament* (July 2014) p. 133; *Fourth Report of the 44th Parliament* (March 2014) p. 1; *Sixth Report of 2013* (May 2013) pp. 189-191; *Third Report of 2013* (March 2013) p. 120; *First Report of 2013* (February 2013) p. 27.

8 See, Parliamentary Joint Committee on Human Rights, *Report 1 of 2018* (6 February 2018) p. 121; *Report 12 of 2017* (28 November 2017); *Report 4 of 2017* (9 May 2017) pp. 92-93; *Report 2 of 2017* (21 March 2017); *Report 1 of 2017* (16 February 2017); *Thirty-First Report of the 44th Parliament* (24 November 2015) pp. 43-44; *Twenty-Sixth Report of the 44th Parliament* (18 August 2015).

assessment of the POC Act to determine its compatibility with the right to a fair trial and right to a fair hearing. [9]

Expansion of the unexplained wealth orders regime – Schedules 2 and 3

2.380 The bill extends the scope of the commonwealth unexplained wealth restraining orders and unexplained wealth orders (defined in the bill as the 'main unexplained wealth provisions'[10]) under the POC Act to territory offences as well as 'relevant offences'[11] of 'participating states'.[12] Currently, existing provisions of the POC Act allow unexplained wealth restraining orders and unexplained wealth orders to be made in relation to commonwealth offences, foreign indictable offences and state offences that have a federal aspect. The effect of these amendments is to expand the scope of the unexplained wealth regime to provide that:

- unexplained wealth restraining orders must be made by a court if, relevantly, there are reasonable grounds to suspect that a person has committed a territory offence or a relevant offence of a participating state, or where there are reasonable grounds to suspect that the whole or any part of a person's wealth was derived from a territory offence or relevant offence of a participating state;[13] and
- unexplained wealth orders must be made by a court if, relevantly, the court is not satisfied that the whole or any part of the person's wealth was not derived from a territory offence or relevant offence of a participating state.[14]

Compatibility of the measure with the right to a fair trial and fair hearing: initial analysis

2.381 The initial analysis raised questions as to the compatibility of the measures with the right to a fair trial and fair hearing, noting that the committee has previously

---

9 Parliamentary Joint Committee on Human Rights, *Report 1 of 2018* (6 February 2018) p. 121; *Report 12 of 2017* (28 November 2017); *Report 4 of 2017* (9 May 2017) pp. 92-93; *Report 2 of 2017* (21 March 2017); *Report 1 of 2017* (16 February 2017); *Thirty-First Report of the 44th Parliament* (24 November 2015) pp. 43-44; *Twenty-Sixth Report of the 44th Parliament* (18 August 2015).

10 Proposed section 14B(3) of Schedule 1 of the bill.

11 A 'relevant offence' of a participating state is defined to mean an offence of a kind that is specified in the referral Act or adoption Act of the state: see proposed amendment to section 338 in item 2, Schedule 2 of the bill.

12 A 'participating state' is one which refers powers to the commonwealth parliament (for the purposes of paragraph 51(xxxvii) of the Constitution) so as to participate in the national unexplained wealth scheme: see proposed section 14C in Schedule 1 of the bill.

13 Items 1 and 2 of Schedule 2 and 3, proposed amendments to sections 20A(1)(g)(i) and 20A(1)(g)(ii) of the bill.

14 Item 5 of Schedule 2 and 3, proposed amendment to section 179E(1)(b)(ii) of the bill.

raised human rights concerns in relation to the underlying unexplained wealth orders regime.[15] As the amendments to the bill expand the operation of the unexplained wealth regime, these concerns apply equally to the amendments introduced by the bill.

2.382 In relation to the right to a fair trial, the committee raised questions as to whether the unexplained wealth regime (as expanded by the bill) could be characterised as 'criminal' for the purposes of international human rights law, having regard to the nature, purpose and severity of the measures.[16] A consequence of the measures being characterised as 'criminal' would be that minimum criminal process guarantees contained in Articles 14 and 15 of the International Covenant on Civil and Political Rights (ICCPR) would apply and the measures in the bill would need to be shown to be consistent with these guarantees.

2.383 In relation to the right to a fair hearing, the initial analysis noted that the right to a fair hearing appeared to be engaged and limited by the measures as a preliminary unexplained wealth order or unexplained wealth restraining order may be made against a person who does not appear at the hearing. The initial analysis raised concerns as to whether the limitation on the right to a fair hearing is proportionate.

2.384 The full initial human rights analysis is set out at *Report 7 of 2018* (14 August 2018) at pages 65-81.[17]

2.385 The committee therefore sought the advice of the minister as to whether these amendments to the POC Act are compatible with the right to a fair trial and fair hearing, in particular:

- whether the unexplained wealth provisions (as expanded by the bill) may be characterised as 'criminal' for the purposes of international human rights law, having regard in particular to the nature, purpose and severity of the measures;
- the extent to which the provisions are compatible with the criminal process guarantees in Articles 14 and 15 of the ICCPR, including any justification for any limitations on these rights where applicable; and

15 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 67-70.

16 See Parliamentary Joint Committee on Human Rights, *Guidance Note 2 – Offence provisions, civil penalties and human rights* (December 2014).

17 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 65-81 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_7_of_2018.

- the extent to which the provisions are compatible with the right to a fair hearing (including whether there are other, less rights restrictive, means of achieving the objectives of the bill).

2.386 The committee also recommended that, as the POC Act was introduced prior to the establishment of the committee, the minister undertake a detailed assessment of the POC Act to determine its compatibility with the right to a fair trial and right to a fair hearing.

Minister's response and analysis

The right to a fair trial

2.387 The minister's response states that the unexplained wealth provisions (as expanded by the Bill) are properly characterised as civil for the purposes of international human rights law. In particular, the minister's response states that the 'orders imposed via unexplained wealth proceedings cannot create criminal liability, do not result in any finding of criminal guilt and do not expose people to any criminal sanctions'.

2.388 The minister's response then addresses whether the measures should be characterised as 'criminal' having regard to criteria set out in the committee's *Guidance Note 2*, that is, the domestic classification of the penalty, the nature and purpose of the penalty, and the severity of the penalty. As to the first step (the domestic classification of the penalty), the minister's response reiterates that the POC Act 'expressly provides that asset recovery actions under the Commonwealth unexplained wealth regime are characterised as civil in nature under Australian law'. However, the classification of a penalty domestically as civil in nature is not determinative of whether it may be 'criminal' for the purposes of international human rights law.[18]

2.389 As to the second step (the nature and the purpose of the unexplained wealth orders), the minister's response explains:

> The unexplained wealth regime established under the POC Act is not solely focussed on deterring or punishing persons for breaching laws, but also on remedying the unjust enrichment of persons who profit at society's expense. Unexplained wealth orders also make no determination of a person's guilt or innocence and can be imposed without a finding of any form of culpability against a particular individual.

2.390 The minister's reference to 'remedying the unjust enrichment of persons who profit at society's expense' indicates that the nature of the unexplained wealth regime is, in part, remedial. The United Nations High Commissioner for Human Rights

18 *Engel v Netherlands (No.1),* European Court of Human Rights Application Nos. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72 (8 June 1976) pp. 30-31; *Gale v Serious Organised Crime Agency* [2011] UKSC 49 [16].

has stated that confiscations of proceeds of crime that are remedial in nature are generally not likely to be characterised as 'criminal' for the purposes of international human rights law.[19] Further, as noted in the initial analysis, the purpose of 'us[ing] unexplained wealth laws to undermine criminal gangs and prevent[ing] them reinvesting their profits to support further criminal activity' indicates that the unexplained wealth provisions may also have a preventative purpose.[20] Preventative measures have also not generally been characterised as 'criminal charges' or 'penalties' in international human rights law.[21]

2.391 However, as acknowledged in the minister's response, while deterrence and punishment are not the *sole* purposes of the regime, they do nonetheless form part of the rationale or purpose of the measures. Further, as noted in the initial analysis, the broader purposes of the POC Act (including unexplained wealth proceedings) are outlined in section 5 of that Act, and include to punish and deter persons from breaching laws.[22] The unexplained wealth provisions also appear to apply to the public in general, which is another factor relevant to assessing whether the measures should be characterised as 'criminal' for the purposes of international human rights law. This indicates that the provisions could be capable of being characterised as 'criminal'.

2.392 In relation to the third step (the severity of the measure), the minister's response states:

> Penalties under the POC Act cannot be commuted into a period of imprisonment. Unexplained wealth orders under the POC Act cannot of themselves create any criminal liability and do not expose people to any criminal sanction (or subsequent criminal record).
>
> Where a person can prove that their wealth was not linked to a particular offence, the value of this property will not be added to the amount to be forfeited to the Commonwealth.[23] In addition, it remains open to a court

---

19 United Nations High Commissioner for Human Rights, *Comprehensive study on the negative impact of the non-repatriation of funds of illicit origin to the countries of origin on the enjoyment of human rights, in particular economic, social and cultural rights,* UN Doc. A/HRC/19/42 (14 December 2011) [46], citing *Welch v United Kingdom,* European Court of Human Rights Application No.17440/90 (9 February 1995) and *Phillips v United Kingdom,* European Court of Human Rights Application No.41087/98 (12 December 2001).

20 SOC, [51]; Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) p. 68https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_7_of_2018.

21 *Gogitdze & Ors v. Georgia,* European Court of Human Rights Application No.36862/05 (12 May 2015) [126].

22 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) p. 69.

23 See, POC Act sections 179E(2)(b), 179J and 19L.

to divert unexplained wealth amounts in certain circumstances, including to relieve particular dependants from hardship.

2.393 That an unexplained wealth order cannot, of itself, create criminal liability or result in imprisonment is relevant in assessing the severity of the measure.[24] The ability of the court to pay amounts to dependants of persons subject to unexplained wealth orders if satisfied the orders would cause hardship to the dependant is also relevant.[25] Other relevant factors that have been considered in international human rights jurisprudence when assessing whether a civil confiscation scheme may be characterised as 'criminal' include whether the degree of culpability of the offender impacts the amount of the order,[26] and whether proceedings are initiated after the relevant criminal proceedings have ended with an outcome other than conviction (such as acquittal or discontinuation of criminal proceedings as being statute-barred).[27] It is ultimately determined on the particular facts of a case in question.[28]

2.394 However, as noted in the initial analysis unexplained wealth orders and unexplained wealth restraining orders can involve significant sums of money.[29] This raises concerns that the cumulative effect of the purpose and severity of the measures could lead to them being characterised as 'criminal'.

2.395 Therefore, having regard to the broader punitive and deterrent purposes of the POC Act (within which the unexplained wealth orders regimes operate), and the potential severity of the measures, some concerns remain that the unexplained wealth order regime could be characterised as 'criminal' for the purposes of international human rights law. However, in the absence of a broader foundational review of the POC Act (including the unexplained wealth regime), it is not possible to conclude on this point.

2.396 To the extent that fair trial rights may be engaged by the unexplained wealth orders regime, there are questions as to whether the unexplained wealth provisions are compatible with these rights, in particular the presumption of innocence. This is because, where the court is considering whether to make an unexplained wealth order, the burden of proving that the person's wealth is not derived, directly or indirectly, from one or more of the relevant offences would lie on the person against

---

24 *Jamil v France,* European Court of Human Rights Application No.15917/89 (8 June 1995) [30].

25 POC Act, section 179L.

26 *Dassa Foundation v Lichtenstein,* European Court of Human Rights Application No.696/05 (10 July 1997); *Butler v United Kingdom,* European Court of Human Rights Application No.41661/98 (27 June 2002).

27 *Gogitdze & Ors v. Georgia,* European Court of Human Rights Application No.36862/05 (12 May 2015) [125].

28 *Welch v United Kingdom,* European Court of Human Rights Application No.17440/90 (9 February 1995).

29 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) p. 69.

whom an order is being sought.[30] This raises concerns insofar as placing the burden of proof on the respondent may effectively give rise to a presumption of unlawful conduct.[31] Insofar as the amendments introduced by the bill operate retrospectively, if the measures were characterised as 'criminal' this may also raise concerns in relation to Article 15 of the ICCPR, which prohibits the retrospective application of criminal laws.

2.397 The UN High Commissioner for Human Rights has stated that limitations on the presumption of innocence through confiscation and asset freezing are not necessarily incompatible with due process guarantees 'so long as States take into account the importance of what is at stake, and respect the right of the defence'.[32] However, the minister's response states that 'as the unexplained wealth regime under the POC Act is civil in nature the criminal justice guarantees…are not relevant'. Therefore, no assessment has been provided as to whether the potential limitation on the right to the presumption of innocence is permissible, or whether the measure is otherwise compatible with criminal process guarantees in Articles 14 and 15 of the ICCPR.

The right to a fair hearing

2.398 In relation to the right to a fair hearing, the minister's response states:

> Proceedings under the unexplained wealth provisions are proceedings heard by Commonwealth, State and Territory courts in accordance with relevant procedures of those courts. This affords an affected person adequate opportunity to present his or her case, such that the right to a fair hearing will generally not be limited.

2.399 In the initial analysis the committee raised specific concerns as to the proportionality of the limitation on the right to a fair hearing. In particular, the committee raised concerns that a preliminary unexplained wealth order or unexplained wealth restraining order may be made against a person who does not appear at the hearing, and so may not have an opportunity to be heard. The POC Act also provides that a court may make an unexplained wealth order even when the person failed to appear as required by the preliminary unexplained wealth order.[33] This raised questions as to whether the safeguards in place to protect the right to a fair hearing would be sufficient from the perspective of international human rights

30 POC Act, section 179E.

31 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 67-70; *Report 1 of 2018* (6 February 2018) p. 121.

32 United Nations High Commissioner for Human Rights, *Comprehensive study on the negative impact of the non-repatriation of funds of illicit origin to the countries of origin on the enjoyment of human rights, in particular economic, social and cultural rights,* UN Doc. A/HRC/19/42 (14 December 2011) [46].

33 POC Act, section 179E(4).

law, and whether there may be other, less rights restrictive means of achieving the legitimate objective of the measures. The minister's response addresses this concern and states:

> This protection, however, must be discretionary to ensure the court can accommodate the circumstances of a case to arrive at an appropriate outcome and to ensure that the court has the ability to manage the proceedings before it. For example, even where a person has a good reason for not appearing, it may be appropriate for the Court not to give a suspect leave to revoke a restraining order where their delay in seeking revocation is considerable and designed to frustrate ongoing proceedings.

2.400 It is acknowledged that there may be circumstances in which it may not be appropriate to revoke a restraining order notwithstanding a person's non-appearance at the hearing, including where a person may not be appearing before the hearing so as to frustrate ongoing proceedings. The discretion of the court to grant leave where a person has a good reason for not appearing may be capable, in practice, of addressing fair hearing concerns. However, a less rights restrictive means of achieving the objectives could be, for example, requiring a court to give leave to revoke the restraining order *unless* the court is satisfied that the person did not have a good reason for appearing or that the person was attempting to frustrate proceedings by their non-appearance. Ultimately, the sufficiency of the safeguards will depend on how the provisions operate in practice.

2.401 The minister's response also notes the committee's recommendation that the POC Act would benefit from an inquiry and states that the 'Government continually reviews the POC Act to ensure the provisions are fit for purpose and appropriate and will continue to undertake a human rights compatibility assessment when developing Bills to amend the Act'.

Committee response

2.402 The committee thanks the minister for his response and has concluded its examination of this issue.

2.403 To the extent the measures may be considered 'criminal' for the purposes of international human rights law, the committee cannot conclude that the measures in Schedules 2 and 3 of the bill are compatible with the right to a fair trial.

2.404 In relation to the right to a fair hearing, the safeguards identified by the minister in the bill and in the POC Act may be capable, in practice, of ensuring that any limitation on the right to a fair hearing is proportionate. However, it is noted that much may depend on the adequacy of the applicable safeguards in practice.

2.405 The committee reiterates its previous view that the POC Act (including the unexplained wealth regime) would benefit from a foundational human rights assessment by the minister to determine its compatibility with the right to a fair trial and right to a fair hearing. This would inform the committee's consideration of

any amendments to the POC Act in the context of the legislative scheme as a whole.

Compatibility of the measure with the right to privacy: initial analysis

2.406 The initial analysis raised questions as to the compatibility of the measures with the right to privacy, which prohibits arbitrary or unlawful interference with one's privacy, family, home or correspondence. This is because the unexplained wealth regime affects the rights of individuals in relation to property (including real property, such as a home) which they own.

2.407 The initial analysis raised questions as to whether unexplained wealth restraining orders and unexplained wealth orders, which could apply where a person has not been convicted of any crime, were rationally connected to the legitimate objective of 'ensuring that criminals are not able to profit from their crimes and are deterred from further criminal activity'.[34] The initial analysis also raised questions as to the proportionality of the measures.

2.408 The full initial human rights analysis is set out at *Report 7 of 2018* (14 August 2018) at pages 71-73.[35]

2.409 The committee therefore sought the advice of the minister as to:

- whether the measures in Schedules 2 and 3 are rationally connected to (that is, effective to achieve) the legitimate objective of the measures; and
- the proportionality of the limitation on the right to privacy (including whether the safeguards in the POC Act referred to in the statement of compatibility ensure that the measures are the least rights restrictive means of achieving the legitimate objective).

Minister's response and analysis

2.410 As to whether the measures pursue a legitimate objective and are rationally connected to the objectives of the bill, the minister's response states:

> As the Committee points out, the measures in Schedules 2 and 3 support the legitimate objective of 'ensuring that criminals are not able to profit from their crimes and are deterred from further criminal activity'. The measures are also being progressed to support many of the objectives outlined at section 5 of the POC Act, including depriving persons of unexplained wealth amounts and preventing reinvestment of these amounts in further criminal activity. These objectives are also legitimate,

34 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) p. 72.

35 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 71-73 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_7_of_2018.

> as they are necessary to reduce the influence of serious and organised crime and thereby preserve public order.
>
> The measures are rationally connected to these objectives as they allow Commonwealth orders to be used to seize a greater range of unexplained wealth, including wealth that can be linked to a Territory or relevant *'participating State'* offence, thereby depriving persons of unexplained wealth amounts and preventing the reinvestment of these amounts in further criminal activity.

2.411 Based on this information it appears the measures pursue a legitimate objective and may be rationally connected to the stated objectives of the bill.

2.412 In relation to proportionality, the statement of compatibility identified the following safeguards:

- courts may refuse to make an unexplained wealth restraining order, a preliminary unexplained wealth order or an unexplained wealth order if there are not reasonable grounds to suspect that a person's total wealth exceeds by $100,000 or more the value of their wealth that was 'lawfully acquired';[36]
- a court may refuse to make an unexplained wealth restraining order or unexplained wealth order if the court is satisfied that it is not in the public interest to make the order;[37]
- courts may exclude property from the scope of some of these orders or revoke these orders in a range of situations, including where it is in the public interest or the interests of justice to do so;[38] and
- courts may make orders relieving dependents from hardship caused by unexplained wealth orders[39] and allow for reasonable expenses to be paid out of funds restrained under unexplained wealth restraining orders.[40]

2.413 As to whether these safeguards are sufficient for the purposes of human rights law, the minister's response states:

> The safeguards outlined in the statement of compatibility to the Bill ensure that these measures remain proportionate and are the least rights restrictive means of achieving these objectives. These safeguards are discretionary to ensure that a court is able to reach an appropriate outcome in each case.

---

36 POC Act, sections 20A(4), 179B(4) and 179E(6).

37 POC Act, sections 20A(4) and 179E(6).

38 POC Act, sections 24A, 29A, 42 and 179C.

39 POC Act, section 179L.

40 POC Act, section 24.

> For example, the court may not make an unexplained wealth order in relation to wealth that can be shown to have been derived from legitimate sources.[41] These protections ensure that the regime is proportionate as an order is directly linked to the amount of unexplained wealth.
>
> Further, a court may refuse to make an unexplained wealth restraining order, a preliminary unexplained wealth order or an unexplained wealth order if there are not reasonable grounds to suspect that a person's total wealth exceeds, by $100,000 or more, the value of their wealth that was lawfully acquired. This discretion is important to ensure the appropriate application of the regime and its efficacy, by allowing the court to consider all the relevant facts in reaching their decision. For example, the court may consider it appropriate to make an order where there is a significant likelihood that the subject of the order will reinvest this wealth in criminal activity in the future or has a history of accumulating the proceeds of crime.

2.414 The safeguards identified in the minister's response may be capable of addressing some of the concerns in relation to the proportionality of the limitation on the right to privacy. However, the minister's response does not address all of the specific concerns raised in the initial analysis as to the sufficiency of the safeguards. In particular, some of the safeguards identified in the statement of compatibility, such as the ability to allow reasonable expenses to be paid out of funds restrained pursuant to unexplained wealth restraining orders, and the ability to refuse to make orders if the court is satisfied it is not in the public interest to do so, are discretionary.[42] It therefore appears possible that a court could refuse to allow reasonable expenses to be paid out of funds restrained pursuant to an unexplained wealth restraining order,[43] or could still make an unexplained wealth order, notwithstanding that the court is satisfied it is not in the public interest to do so.[44] A mandatory rather than discretionary requirement for a court to refuse to make an unexplained wealth order when it is not in the public interest to make such an order, or a mandatory requirement to allow reasonable expenses to be paid out of funds restrained pursuant to unexplained wealth restraining orders, would appear to be a less rights restrictive approach. Therefore, there is a risk that the measure may not be a proportionate limitation on the right to privacy in all circumstances.

Committee response

2.415 The committee thanks the minister for his response and has concluded its examination of this issue.

---

41 POC Act, section 179E.

42 POC Act, section 24(1). In contrast, the court *must* relieve certain dependants from hardship caused by unexplained wealth orders if certain criteria are satisfied: section 179L(1).

43 POC Act, section 24(1).

44 POC Act, section 179E(6).

2.416 The safeguards identified by the minister in the bill and in the POC Act may be capable, in practice, of ensuring that any limitation on the right to privacy is proportionate in a range of circumstances. However, much may depend on the adequacy of the applicable safeguards in practice and there appears to be a risk that the measure may operate in a manner which is not a proportionate limitation on the right to privacy in some individual cases.

Information gathering powers under the national cooperative scheme on unexplained wealth – Schedule 4

2.417 Schedule 4 of the bill allows specified officers in territories and participating states to apply for production orders, which would require a person to produce or make available documents relevant to identifying, locating or quantifying property of a person for the purposes of unexplained wealth proceedings that have commenced or deciding whether to institute such proceedings.[45] Such orders can only require production of documents that are in the possession, or under the control, of a corporation or are used, or intended to be used, in the carrying on of a business.[46]

2.418 A person is not excused from producing or making available a document made under such an order on the ground that producing the document would tend to incriminate the person or expose the person to a penalty.[47] In this respect, a 'use immunity' is provided, such that any document produced or made available is not admissible in evidence in a criminal proceeding against the person except for the offences of giving false or misleading information or documents under the *Criminal Code*.[48] However, no derivative use immunity is provided.[49]

2.419 A person who obtains information as a direct result of the exercise of the production order power or function may disclose the information to a number of specified authorities for a number of specified purposes, if the person believes on reasonable grounds that the disclosure will serve that purpose and a court has not made an order prohibiting disclosure.[50] This includes disclosure to authorities of a state or territory for the purposes of engaging in proceedings under the state or

---

45 Schedule 4, section 1 of proposed Part 1 of Schedule 1 of the POC Act. Documents relevant to identifying or locating any document necessary for the transfer of property and documents that would assist in the reading or interpretation of documents referred to in section 1(6)(a) and (b) would also be subject to production orders: section 1(6)(c).

46 Schedule 4, section 1(3)(b)-(c) of proposed Part 1 of Schedule 1 of the POC Act.

47 Schedule 4, section 5(1)(a) of proposed Part 1 of Schedule 1 of the POC Act.

48 Schedule 4, section 5(2) of proposed Part 1 of Schedule 1 of the POC Act; see also proposed section 18(3) and (4) of Part 3 of Schedule 1 of the POC Act.

49 Schedule 4, section 18(3) and (4) of proposed Part 3 of Schedule 1 of the POC Act. A derivative use immunity would prevent information or evidence indirectly obtained from being used in criminal proceedings against the person.

50 Schedule 4, section 18 of proposed Part 3 of Schedule 1 of the POC Act.

territory law; disclosure to an 'authority of the Commonwealth with one or more functions under [the POC] Act' for the purpose of 'facilitating the authority's performance of its functions under this Act'; disclosure to authorities of the commonwealth, state or territory to assist in the prevention, investigation or prosecution of an offence against that law that is punishable on conviction by imprisonment for at least three years; and disclosure to the Australian Taxation Office for the purpose of protecting public revenue.[51]

Compatibility of the measure with the right not to incriminate oneself: initial analysis

2.420 The initial analysis raised questions as to the compatibility of the measures with the right not to incriminate oneself. This is because the measures require a person to produce or make available documents notwithstanding that to do so might incriminate that person. The right not to incriminate oneself may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate way of achieving that objective.

2.421 The initial analysis considered that the purported objective of overriding the privilege against self-incrimination, namely to address the concern that 'criminals regularly seek to hide their ill-gotten gains behind a web of complex, legal, contractual and business arrangements', was likely to be a legitimate objective for the purposes of international human rights law. The committee also considered that requiring the production of documents was likely to be rationally connected to this objective.

2.422 However, the committee's initial analysis raised questions as to the proportionality of the measures. The full initial human rights analysis is set out at *Report 7 of 2018* (14 August 2018) at pages 74-75.[52]

2.423 The committee therefore sought the advice of the minister as to the compatibility of the measures with this right, including advice as to whether a 'derivative use' immunity could be reasonably available as a less rights restrictive alternative.

Minister's response and analysis

2.424 The minister's response provided the following information as to the scope of the proposed production orders and how this is relevant to the proportionality of any limitation on the right not to incriminate oneself:

---

51 Schedule 4, section 18(2) of proposed Part 3 of Schedule 1 of the POC Act.

52 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 74-75 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_7_of_2018.

> The measures are a proportionate means of achieving the legitimate objective of 'enhancing law enforcement's ability to effectively trace, restrain and confiscate unexplained wealth amounts'. Effective protections exist to ensure these measures can only be exercised in an appropriate and proportionate manner.
>
> Production orders must be made by the courts, and a magistrate retains the discretion not to make a production order under subclause 1(1) of proposed Schedule 1 of the POC Act. These production orders can also only require the production of documents which are in the possession, or under the control, of a body corporate or are used, or intended to be used, in the carrying on of a business. The narrow scope of these orders minimises the possibility that the privilege against self-incrimination will be abrogated, as corporations do not benefit from the privilege and documents which do not relate to the carrying on of a business are not required to be produced.

2.425 The minister also provides the following information as to why it is necessary not to have a 'derivative use' immunity available:

> Applying a derivative use immunity to civil investigations would defeat the central purpose of production orders under subparagraph 1(6)(a)(i) of proposed Schedule 1 to the POC Act, which is to gain information required to determine whether to take further civil action, including investigative action, under State and Territory 'unexplained wealth legislation'.
>
> If a derivative use immunity was applied to criminal investigations, this would have the potential to severely undermine the existing ability of authorities to investigate and prosecute serious criminal conduct.
>
> For example, if a derivative use immunity was included, where an investigator in a criminal matter could potentially have access to privileged material, the prosecution may be required to prove the provenance of all subsequent evidentiary material before it can be admitted. This creates an unworkable position wherein pre-trial arguments could be used to inappropriately undermine and delay the resolution of charges against the accused.
>
> Further, this would be contrary to the aims of the existing production order regime, the proposed production order regime and the associated information sharing provisions under existing section 266A of the POC Act and proposed clause 18 of Schedule 1 to the POC Act.
>
> These provisions only allow for the derivative use and sharing of produced documents where the documents are shared with a specific authority for a legitimate purpose. For example, a document obtained under a production order may be given to an investigative authority of a State under item 3 of subclause 28(2) only if the person giving the document believes on reasonable grounds that the document will assist in the prevention, investigation or prosecution of an offence punishable by at least 3 years or life imprisonment.

2.426 The production orders do not apply to documents in the custody of an individual which relate to the affairs of an individual; instead, the proposed production orders apply to documents which are in the possession, or under the control, of a body corporate or are used, or intended to be used, in the carrying on of a business. The minister's response also indicates that there is no less rights restrictive alternative reasonably available. Noting the narrow scope of these orders and based on the information provided by the minister, on balance the limitation on the right not to incriminate oneself may be proportionate to the legitimate objective of the measures.

Committee response

2.427 The committee thanks the minister for his response and has concluded its examination of the issue.

2.428 In light of the information provided by the minister and noting in particular the narrow scope of the production orders, the committee considers that the proposed production orders provisions in Schedule 4 of the bill may be a proportionate limitation on the right not to incriminate oneself.

Compatibility of the measure with the right to privacy: initial analysis

2.429 The initial analysis raised questions as to the compatibility of the production orders powers with the right to privacy, which protects informational privacy. This was because the compulsory production of documents relating to the carrying on of a business, and subsequent disclosure to authorities of those documents, may involve the disclosure of personal information.

2.430 The initial analysis stated that the purported objective of limiting the right to privacy, namely 'disrupting and combating serious and organised crime', was likely to be a legitimate objective for the purposes of international human rights law. The committee also considered that the compulsory production orders powers appeared to be rationally connected to this objective.

2.431 However, the committee raised questions as to the proportionality of the limitation on the right to privacy. The full initial human rights analysis is set out at *Report 7 of 2018* (14 August 2018) at pages 76-77.[53]

2.432 The committee therefore sought further information from the minister as to the proportionality of the limitation on this right, including whether the measure is sufficiently circumscribed and whether there are adequate safeguards in place with respect to the use, disclosure, storage and retention of information obtained pursuant to production orders.

53 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 71-73 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_7_of_2018.

Minister's response and analysis

2.433 As noted in the initial analysis, the documents that can be subject to production orders are limited to those documents in possession of a corporation that are used in carrying on a business. Therefore the measure only engages and limits the right to privacy to the limited extent that personal information could be disclosed about a person in relation to, for example, the carrying on of a business. This is relevant in determining the proportionality of the measure.

2.434 The initial analysis raised questions in relation to specific safeguards included in the bill relating to the disclosure of any information obtained pursuant to the production orders. The committee raised questions in particular as to the breadth of purposes for which information may be disclosed by a person to authorities. For example, under proposed Part 3 of Schedule 1 of the POC Act (contained in Schedule 4 of the bill), information may be disclosed to an 'authority of the commonwealth with one or more functions under [the POC] Act' for the broad purpose of 'facilitating the authority's performance of its functions under this Act'.[54]

2.435 The minister's response provided the following information in relation to this safeguard:

> The Committee has asked specifically as to the proportionality of Part 3 of proposed Schedule 1 to the POC Act, which allows information gained through production orders to be disclosed to specific Commonwealth, State and Territory authorities for particular purposes.
>
> Part 3 is appropriately confined to purposes connected to the preservation of public order, allowing for disclosures to appropriate agencies to further the investigation, prevention and prosecution of criminal matters, the targeting of proceeds and instruments of crime, and the protection of public revenue.
>
> A person who receives information due to a disclosure under Part 3 will continue to be limited in any further disclosure of that information to the recipients, and for the purposes, outlined in subclause 18(2). If this information originated from a production order, this person will also be unable to use it directly in a criminal proceeding against the person who produced it under subclause 18(5).
>
> Each agency that receives this disclosure will need to ensure that its disclosure, storage and retention policies for information ensure conformity with these legal limitations.
>
> The measure is therefore proportionate in any limitation it places on the right to privacy.

2.436 The minister's response clarifies that the purposes for which disclosure could be made, while broad, are connected with the preservation of public order and are

54 Schedule 4, section 18(2) of proposed Part 3 of Schedule 1 of the POC Act.

directed towards facilitating investigations, prevention and prosecutions of criminal matters and matters under the Act. While these purposes are quite broad, in light of the limited circumstances in which personal information could be obtained through the production orders powers (that is, being limited to personal information in documents in possession of a corporation that are used in carrying on a business), on balance and in these particular circumstances the measures appear to be a proportionate limitation on the right to privacy.

Committee response

2.437 The committee thanks the minister for his response and has concluded its examination of the issue.

2.438 In light of the information provided by the minister and noting in particular the narrow scope of the production orders, the committee considers that the disclosure of information obtained as a result of production orders in Schedule 4 of the bill may be a proportionate limitation on the right to privacy.

Information sharing provisions – amendments to the TIA Act – Schedule 6

2.439 Currently, lawfully intercepted information and interception warrant information may be used in unexplained wealth proceedings only where the proceedings are 'in connection with the commission of a prescribed offence'.[55] Similarly, agencies may only 'deal' in interception information for certain prescribed purposes and proceedings, which do not currently include unexplained wealth provisions or proceedings.[56] Schedule 6 of the bill would allow officers in Commonwealth, territory and participating state agencies to use, record or communicate lawfully intercepted information or interception warrant information under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) for purposes connected with unexplained wealth proceedings, without having to show a link to a prescribed offence. This amendment would override the general prohibition in the TIA Act on using, disclosing, recording and giving in evidence lawfully intercepted information.[57]

2.440 The bill would also amend section 68 of the TIA Act to allow the chief officer of an agency to communicate lawfully intercepted information to the relevant Commissioner of Police if it relates to the unexplained wealth provisions of that jurisdiction.[58]

---

55 *Telecommunications (Interception and Access) Act 1979*, section 5B(1)(b).

56 'Dealing' for permitted purposes in relation to an agency allows an officer or staff member of an agency, for a permitted purpose, or permitted purposes, in relation to the agency and for no other purpose, to communicate to another person, make use of, or make a record of specified information: see TIA Act, section 67.

57 Item 2 of Schedule 6, proposed sections 5B(1)(be) and (bf) of the TIA Act.

58 Item 7 and 8 of Schedule 6, proposed section 68(c)(ia) of the TIA Act.

Compatibility of the measure with the right to privacy: initial analysis

2.441 As noted in the initial analysis, as the TIA 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.* A full human rights assessment of proposed measures which extend or amend existing legislation requires an assessment of how such measures interact with the existing legislation. The committee is therefore faced with the difficult task of assessing the human rights compatibility of an amendment to the TIA Act without the benefit of a foundational human rights assessment of the Act.

2.442 The initial analysis stated that schedule 6 of the bill engages and limits the right to privacy by allowing officers in Commonwealth, territory and participating state agencies to use, record or communicate lawfully intercepted information or interception warrant information for a purpose connected with unexplained wealth proceedings.[59] This may include private communications, including potentially the content of private telephone conversations and emails. The committee raised questions as to whether the measure pursues a legitimate objective, and is rationally connected and proportionate to that objective.

2.443 The full initial human rights analysis is set out at *Report 7 of 2018* (14 August 2018) at pages 77-80.[60]

2.444 The initial analysis therefore sought further information from the minister as to the compatibility with the right to privacy of allowing officers in Commonwealth, territory and participating state agencies to use, record or communicate lawfully intercepted information or interception warrant information under the TIA Act in an unexplained wealth proceeding without having to show a link to a prescribed offence, 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;
- how the measure is effective to achieve (that is, rationally connected to) that objective;
- whether the limitation is a reasonable and proportionate measure for the achievement of that objective (including whether the measure is necessary

59 SOC, [72]-[75].

60 Parliamentary Joint Committee on Human Rights, *Report 7 of 2018* (14 August 2018) pp. 77-80 at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2018/Report_7_of_2018.

and sufficiently circumscribed and whether it is accompanied by adequate and effective safeguards); and

- whether an assessment of the TIA Act could be undertaken to determine its compatibility with the right to privacy (including in respect of matters previously raised by the committee).

Minister's response and analysis

2.445 As to whether the measures pursue a legitimate objective and are rationally connected to the objective, the minister's response states:

> The amendments to the *Telecommunications (Interception and Access) Act 1979* (TIA Act) are aimed at achieving the legitimate objective of preserving public order through improving the investigation and litigation of unexplained wealth matters targeting serious and organised crime.
>
> These amendments are rationally connected to this objective and are necessary as they allow information obtained under the TIA Act to be shared between law enforcement agencies, thereby facilitating the effective investigation of unexplained wealth matters, which often involve the movement of funds across State and Territory borders using complex and multifaceted methods. Telecommunications information is vital to tracing and uncovering these movements of funds. The information obtained under the TIA Act is also currently used by investigators in some proceeds of crime investigations, and can be invaluable in proving offending conduct and identifying assets of interest.

2.446 Based on the information provided in the minister's response, it appears the measures pursue a legitimate objective and are rationally connected to this objective.

2.447 In relation to whether the measures are proportionate, the minister's response states:

> These measures are reasonable and proportionate in achieving the above objective. Communications can only be intercepted in limited circumstances under the TIA Act, including in emergency situations and only under warrant. The proposed amendments will not change the thresholds applying to interception, but go … only to the use of this information rather than the circumstances in which it can be collected.
>
> The use and disclosure of information gathered under the TIA Act is also subject to extensive protections to ensure they are reasonable and proportionate. These protections are incorporated within the TIA Act and include, but are not limited to:
>
> - restrictions which prevent agencies from using and disclosing intercepted communications except for lawfully permitted purposes prescribed under the TIA Act

- a mandated requirement to consider the privacy of a person before authorising the disclosure of telecommunications data or allowing an agency access to stored communications, and
- prohibitions on people in the telecommunications industry disclosing any information or document relating to a communication.

2.448 The minister's response also notes the committee's recommendation in relation to a review of the TIA Act and states that 'the Government continually reviews the TIA Act to ensure the provisions are fit for purpose and appropriate and will continue to undertake a human rights compatibility assessment when developing Bills to amend the Act'.

2.449 As noted in the initial analysis, the safeguards identified in the statement of compatibility (and repeated in the minister's response) relating to warranted access to information are found in Chapters 2 and 3 of the TIA Act. The committee has not previously considered Chapters 2 and 3 of the TIA Act in detail. The committee has previously noted, however, that while the warrant regime may assist to ensure that access to private communications is sufficiently circumscribed, the use of warrants does not provide a complete answer as to whether Chapters 2 and 3 of the TIA Act constitute a proportionate limit on the right to privacy, as questions arise as to the proportionality of the broad access that may be granted in relation to 'services' or 'devices' under these chapters of the TIA Act.[61] This raises particular concerns in the context of the present amendments as there would be no requirement to show a link to a prescribed offence before using the information, which affects the proportionality of the measure. Therefore, while the measures in the bill go to the use of information rather than the circumstances in which it can be collected, it is difficult to assess the proportionality of the measures in the absence of a broader assessment of the human rights compatibility of the TIA Act. Concerns therefore remain regarding the proportionality of the measures in Schedule 6.

61 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.

Committee response

2.450 The committee thanks the minister for his response and has concluded its examination of the issue.

2.451 The committee is unable to conclude whether the amendments to the TIA Act introduced by the bill are compatible with the right to privacy.

2.452 Noting that the TIA Act was legislated prior to the establishment of the committee, the committee reiterates its previous view that the TIA Act would benefit from a foundational review of its human rights compatibility.

Mr Ian Goodenough MP

Chair