Responses from legislation proponents — Report 13 of 2018

The Hon Ken Wyatt AM, MP

Minister for Senior Australians and Aged Care
Minister for Indigenous Health
Member for Hasluck

Ref No: MS18-002210

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
PO Box 6022
House of Representatives
Parliament House
CANBERRA ACT 2600
human.rights@aph.gov.au

Dear Chair

Thank you for the correspondence from your Committee Secretary dated 17 October 2018, requesting advice about human rights issues identified in relation to the Aged Care Quality and Safety Commission Bill 2018 (Bill) and the Aged Care Quality and Safety Commission (Consequential Amendments and Transitional Provisions) Bill 2018 (Consequential and Transitional Bill).

As you may be aware, these Bills represent the first of a two stage process of legislative reform to strengthen the regulatory framework that safeguards the health, safety and wellbeing of aged care consumers, by bringing together the functions performed by the Australian Aged Care Quality Agency (Quality Agency) and the Aged Care Complaints Commissioner into a single agency. These Bills directly respond to the key recommendation from the Review of National Aged Care Quality Regulatory Processes. The second stage, as signalled in the objects of the Bill, will result in the remaining regulatory functions performed by the Department of Health transferring to the Commission.

I note the Committee seeks a range of information relating to the compatibility of Part 7 (Information sharing and confidentiality etc) of the Bill with the right to privacy and the right to be presumed innocent under articles 17 and 14(2) of the *International Covenant on Civil and Political Rights,* respectively. I have responded to the issues raised by the Committee below.

While I have sought to address the Committee's concerns in full, where they may be more appropriately or equally addressed in the context of the second stage reforms, I want to assure you that they will be taken into account.

Right to privacy

Part 7 of the Bill which regulates the protection and sharing of information, engages the right to not be subjected to arbitrary or unlawful interference with their privacy under Article 17 of the *International Covenant on Civil and Political Rights*. This right is engaged by provisions in the Bill which allow disclosures of protected information that limit the right to information privacy.

Permitted disclosures of protected information

The Committee seeks advice in relation to whether the limitations imposed on the right to privacy under clause 61 are proportionate to the objective sought. Clause 61 has the potential to limit the rights to privacy by permitting disclosures of protected information on various grounds. As noted by the Committee, the broad objective of clause 61 is to ensure that the Commissioner is in a position to disclose information as appropriate to broadly protect the welfare and interests of aged care consumers, consistent with the objectives of the Bill.

Whether the limitation on the right to privacy in clause 61 is proportionate.

Clause 61 of the Bill is intended to reflect provisions contained in Division 86 of the *Aged Care Act 1997* and Part 7 of the *Australian Aged Care Quality Agency Act 2013*. These provisions enable disclosures of protected information on similar terms to support the complementary functions of the CEO of the Quality Agency and the Secretary of the Department under the *Aged Care Act 1997*. Subclause 61(1)(a) is therefore included in the Bill to maintain consistency with the *Aged Care Act 1997*.

While the Bill imposes a range of limitations on the right to privacy under the permitted disclosures listed under subclause 61(1), to assess the proportionality of these limitations it is necessary to take into account the fact these infringements are only limited to cases where protected information contains personal information. This is because protected information is defined as information acquired in the performance of functions or exercise of powers under the Bill or rules, that either relates to a particular individual, or the affairs of a particular provider.

Of the exceptions provided in subclause 61(1), disclosures in the public interest under subclause 61(1)(a) are necessary to ensure the Bill is flexible enough to allow for disclosures where there is an unforeseen public interest need to disclose information. In this regard, permitting disclosures in the public interest is only intended to deal with a narrow category of disclosures which generally fall outside the routine administration of the Bill or Rules as provided under subclause 60(3), and where disclosure is not available for any of the other specific purposes permitted, listed under clauses 56 to 59 and subclause 61(1).

Reliance solely on these other exceptions could result in 'informational silos' that do not reflect all purposes where they may be a legitimate need to share information across other agencies or entities with common or interrelated responsibilities. For example, defences to the offence against disclosure of protected information under subclause 60(3) allow disclosures made in the course of performing functions or exercising powers under or in relation to the Bill or Rules, or the *Aged Care Act 1997* or Aged Care Principles. However, with the exception of disclosures to the Secretary, an official of the Commission (or other person exercising powers) would be generally unable to disclose protected information directly for other purposes unrelated to aged care, even though the disclosure may impact on the outcomes for aged care consumers.

In order to achieve the stated objectives, the public interest exception must be broad since it is not possible to codify the purpose and the person to whom information may be disclosed in every circumstance in which a disclosure of protected information should be permitted. This is particularly relevant given the interrelated purposes for which information is used for coordinated aged care regulation.

The Bill also imposes a number of constraints and safeguards to ensure permitted disclosure in the public interest is proportionate to the objective being sought. In particular, the Bill prohibits further disclosures for secondary or related purposes, to the primary purpose or original purpose of the disclosure. Further, any disclosure in the public interest must be determined by the Commissioner on a case by case basis, having regard to the circumstances of each particular circumstance. This ensures a level of accountability by requiring a senior officer to consider whether disclosure would be consistent with policy considerations in a particular case.

What factors the Commissioner may have regard to in determining whether a disclosure under clause 61(1)(a) is in the 'public interest'.

In determining the public interest, it is envisaged 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. In particular, where protected information contains personal information, the public interest benefit would be weighed against an individual's right to information privacy and the impact this may have in the circumstances, among any other relevant considerations.

Identifying the public interest in each case, would be undertaken with regard to the objectives of the Bill and whether they would be served or frustrated, by disclosure. These objectives includes protecting the health, and safety and wellbeing of aged care consumers, promoting consumer confidence in the aged care services and promoting engagement with aged care consumers on best practice models of engagement by providers.

In this regard, the purposes of disclosing protected information in the public interest may range from purposes related to matters affecting the rights of aged care consumers, to broader purposes related 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.

It is expected that in balancing the public interest against the right to information privacy (where the protected information includes personal information), consideration would be given to factors such as the nature, sensitivity and impacts of any disclosure of protected 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.

While potentially broad in scope, the public interest exception would only apply on a case by case basis, where the public benefit outweighs the right to privacy considerations such as those outlined above (among others), which arise depending on the factual circumstances of each case. This ensures the public interest exception is only as extensive as necessary.

Whether disclosures under clause 61 include organisations not covered by the Privacy Act, and, the sufficiency of safeguards to protect the right to privacy.

It is possible that disclosures may in some cases be made to persons who are not subject to the *Privacy Act 1988*, or equivalent state or territory privacy act regimes. However, as discussed above, these disclosures will continue to be subject to restrictions which restrict any subsequent disclosures to the purpose of the original disclosure as provided under clause 61.

Whether disclosures pursuant to rules referred to in proposed section 61(1)(j) are sufficiently circumscribed and accompanied by adequate safeguards.

Like disclosures under subclauses 61(1)(a), subclause 61(1)(j) provides additional purposes for disclosing protected information beyond the specific ones contemplated under the provisions for permitted disclosure. The rule making power conferred by clause 61(1)(j) is necessarily broad since it is not possible to prescribe the specific purposes for which rules might allow information to be disclosed.

An equivalent power under the *Aged Care Act 1997* has been necessary to ensure the seamless operation of aged care quality regulation with related legislation such as legislation relating to safety, and to the payment of aged care subsidies, pensions and other Government payments. Disclosures of this type have been used to accommodate new legislation that interacts with the *Aged Care Act 1997* to be accommodated. Principles made under corresponding provisions of the *Aged Care Act 1997* have been amended from time to time for this purpose. For example, the current *Information Principles 2014* enable the Secretary of the Department of Health to disclose information to the Repatriation Commission and to state and territory authorities responsible for fire safety, where the information relates to the functions of that organisation.

Unlike disclosures permitted on a case by case basis under clause 61(1)(a), this power has the potential to impose more extensive limitations on the right to privacy given these exemptions would have general application. However, establishing these exemptions in the rules will ensure any exemptions, are subject to disallowance. This additional parliamentary oversight, provides an important safeguard against the exercise of powers under clause 61(1)(j) which impose arbitrary limitations on the right to privacy. A statement of compatibility that includes an assessment of whether this legislative instrument is compatible with human rights would be incorporated into the Explanatory Statement for any future rules made under this provision.

Information sharing arrangements

Clauses 56 and 57 of the Bill allow the Commissioner and the Secretary of the Department of Health to request from each other, information they require for the purposes of their respective functions or powers. The Secretary and Commissioner must give any information requested that is available to them.

Further, under clauses 58(1) and (2) the Minister may also require the Commissioner to provide any reports or document about the performance of its functions, within a specified timeframe. The Minister may choose to publish a report or document given in accordance with clause 58(1) or (2).

The Committee seeks advice on whether the provisions under Division 2 of Part 7 engage the right to privacy and if so, the proportionality of any limits placed on this right.

Whether personal information can be shared and published under Division 2, Part 7.
Information that is shared in accordance with Division 2 of the Part 7 may contain protected information, including personal information.

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 sufficient circumscribed and the availability of safeguards.

These provisions do not impose any additional limitations on the right to privacy since these provisions only deal with disclosures which are already permitted under the Bill.

Specifically, clauses 56(2)(a), 57(a) and 58(1)(a) and (2)(a) limit the information which 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) provides that disclosures made in the course of performing functions or exercising powers under the Bill or *Aged Care Act 1997* will be exceptions to the offence of disclosing protected information under subclause 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 power. 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 in the Bill, under the framework established by the *Aged Care Act 1997*, to promote the provision of quality of care by approved providers.

The limitations imposed by the disclosures permitted under subclause 60(3) of the Bill on the right to privacy, are also appropriately adapted and proportionate to the objectives sought. Excluding disclosures of protected information in circumstances where the use or disclosure of this information is necessary for the purposes of carrying out the functions or powers of the Commissioner, is necessary to ensure the primary policy objectives of the Bill are not undermined.

For this reason, unlike disclosures made in accordance with subclause 61(1) of the Bill – where clause 62 requires that such disclosures must not be made for any purpose other than its original purpose – disclosures for the purposes related to the Commissioner's functions and powers would not be restricted to the original purpose of the disclosure. Imposing such restrictions would directly and indirectly frustrate the performance of the Commissioner's functions and powers under the Bill and its objectives.

Reverse evidential burden of proof

Article 14(2) of the *International Covenant on Civil and Political Rights* protects the right to be presumed innocent until proven guilty according to law. As referred to above, subclause 60(1) makes it an offence for any person to record, use or disclose protected information that is acquired in the course of performing functions under the Bill, unless an exception applies. Subclauses 60(3) and (4) engage and limit the right to be presumed innocent by imposing an evidential burden of proof on the defendant to establish the disclosures occurred in the specified circumstances.

The Committee seeks an assessment of the compatibility of the reverse burden offence with human rights.

Whether the reverse burden offence is aimed at achieving a legitimate objective for the purposes of international human rights law.

The purpose of these provisions 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 generally not be made public, used or disclosed for an unrelated purpose. Given the Commissioner's functions are ultimately reliant on these exchanges for its effective operation, it is critical that there is a high level of confidence in the standards of protections afforded.

How the reverse burden is effective to achieve (that is, rationally connected to) that objective.

To this end, reversing the onus of proof in relation to establishing the existence of an exception is necessary to promoting this standard of information protection, in the performance of functions or exercise of powers under the Bill or Aged Care Act. By placing the onus 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.

Whether the limitation is a reasonable and proportionate measure to achieve the stated objective.

Imposing this burden 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 60(4). Disclosures which qualify for exception, including disclosures to specified persons, or disclosures 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.

The limitation imposed on the right to innocence is proportionate. Reversing the onus only requires the defendant to adduce evidence a defendant is expected to be able to produce, which demonstrates a possibility that an exception exists. It would then be incumbent of 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.

I thank the Committee for its consideration of this matter.

Yours sincerely

The Hon KEN WYATT AM, MP
Minister for Senior Australians and Aged Care
Minister for Indigenous Health

The Hon Dan Tehan MP
Minister for Education

Parliament House
CANBERRA ACT 2600

Telephone: 02 6277 7350

Our Ref: MS18-001283

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
PO Box 6100
Parliament House
CANBERRA ACT 2600

10 OCT 2018

Dear Mr Goodenough

I have set out below my response to comments made and questions asked by the Parliamentary Joint Committee on Human Rights in its Report 7 of 2018 in respect of the *Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018*.

Scope and Purpose of the Amendments

It is important to set out the background and context to the *Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018* (the "2018 Guidelines"). The 2018 Guidelines step through a range of grounds on which a delegate of the Secretary is able to certify that a disclosure of "protected information" is necessary in the public interest, as permitted by paragraph 168(1)(a) of the *A New Tax System (Family Assistance) (Administration) Act 1999*. This means that, at a very minimum, any disclosure made in accordance with the 2018 Guidelines can only lawfully be made where all of the following apply:

- The disclosure is necessary to further the public interest.
- A delegate at Executive Level 2, or in the Senior Executive Service, in the Department of Education and Training certifies that this is the case.
- Where the public interest reason is consistent with one of the grounds stated in the Guidelines.

These requirements ensure that disclosures are specifically linked to legitimate purposes that are necessary in the public interest and cannot be made arbitrarily.

Similar public interest disclosure regimes apply and have applied, as part of secrecy provisions in other Commonwealth legislation, including a range of social welfare legislation such as the:

- *Social Security (Administration) Act 1999* (section 208)
- *Paid Parental Leave Act 2010* (section 128)
- *Student Assistance Act 1973* (section 355).

Public interest disclosure guidelines have been made by Ministers administering the family assistance law in a series of iterations dating back to the enactment of the *A New Tax System (Family Assistance) (Administration) Act 1999* and commencement in 2000.

Prior to the establishment of the Federal Register of Legislation, guidelines were set out in the *Family Assistance (Public Interest Certificate Guidelines) Determination 2002*. The guidelines below were developed iteratively following amendments to the public interest grounds, or due to Machinery of Government changes:

- *Family Assistance (Public Interest Certificate Guidelines) Determination 2005*
- *Family Assistance (Public Interest Certificate Guidelines) Determination 2006*

- *Family Assistance (Public Interest Certificate Guidelines) (FaHCSIA) Determination 2008*
- *A New Tax System (Family Assistance) (Administration) (Public Interest Certificate Guidelines) (DEEWR) Determination 2009 (No. 1)*
- *A New Tax System (Family Assistance) (Administration) (Public Interest Certificate Guidelines) (DEEWR) Determination 2010*
- *Family Assistance (Public Interest Certificate Guidelines) Determination 2015.*

Earlier versions set out a range of grounds for disclosure which remain in the recently registered 2018 Guidelines. Each set included grounds for disclosures in the following circumstances:

- threat to life, health or welfare
- enforcement of laws
- mistake of fact
- missing and deceased persons
- research and policy development
- Homeless Young Persons.

Until the 2018 Guidelines were recently made, the Department of Social Services and the Department of Education and Training jointly administered the *Family Assistance (Public Interest Certificate Guidelines) Determination 2015*. The 2018 Guidelines are almost identical, except for the fact that, (a) they only apply for the purposes of the Department of Education and Training, which, from November 2015, administered the family assistance law in respect of child care matters only; (b) a new version of section 9 was included with consequential amendments to section 7. As such, the 2018 Guidelines deal with grounds about which information, held for the purposes of administering child care payments, may be disclosed as necessary in the public interest. The *Family Assistance (Public Interest Certificate Guidelines) Determination 2015* remain as the guidelines under which public interest disclosures may be made for the purposes of family assistance payments administered by the Department of Social Services (such as family tax benefit).

Under section 9 of the 2018 Guidelines, disclosures that are necessary in the public interest are able to be made if the disclosure would facilitate an enforcement related activity (within the meaning of the *Privacy Act 1988*) and where the disclosure is made to a Commonwealth or State agency or authority or an "enforcement body" within the meaning of the *Privacy Act 1988*. This ground for disclosure reflects one of the circumstances in which the disclosure of personal information is permitted under the *Privacy Act 1988*, as set out in Australian Privacy Principle (APP) 6.2(e) and as discussed in further detail below.

Prior to new section 9 of the 2018 Guidelines, section 9 in earlier guidelines had outlined a similar ground in these terms:

> **9 Enforcement of laws**
>
> (1) Relevant information may be disclosed for the purpose of this section if:
>
> (a) the disclosure is necessary:
>
> (i) for the enforcement of a criminal law that relates to an indictable offence punishable by imprisonment of 2 years or more; or
>
> (ii) for the enforcement of a law imposing a pecuniary penalty equivalent to 40 penalty units or more; or
>
> (iii) to prevent an act that may have a significant adverse effect on the public revenue; or
>
> (b) the disclosure relates to an offence or threatened offence:
>
> (i) against a Commonwealth employee; or
>
> (ii) against Commonwealth property; or
>
> (iii) in Department premises; or
>
> (iv) in Human Services Department premises.

(2) In this section:

criminal law means:

(a) for Australia — a criminal law of the Commonwealth or of a State or Territory; and

(b) for a place outside Australia — a criminal law that may be recognised under an extradition arrangement to which Australia is a party.

penalty unit has the same meaning as in section 4AA of the *Crimes Act 1914*.

Note Subsection 4AA(1) of the *Crimes Act 1914* provides:

'In a law of the Commonwealth or a Territory Ordinance, unless the contrary intention appears:

penalty unit means $170.'.

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
  - 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 powers 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 designed 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.

Importantly, as opposed to the scope of "protected information" covered by secrecy regimes on other social welfare legislation, in the child care context, "protected information" covers information about both payment recipients as well as providers of child care services, including corporations. This is because "protected information" is defined broadly under section 3 of the Family Assistance Administration Act to include "information about a person", including a corporation or other legal entity that provides a child care service, as well as individuals, that is held for the purposes of the administration of the family assistance law. To the extent that disclosures under section 9 relate to corporations, the information may not contain any "personal information" (that is, information identifying an individual) for the purposes of privacy law.

Approved providers of child care services are subject to a range of regulatory obligations that individual welfare or payment recipients are not subject to, including: a civil penalty regime and offences that apply under Parts 8A and 8C of the *A New Tax System (Family Assistance) (Administration) Act 1999.* Regulatory obligations also apply under State and Territory legislation, including the *Education and Care Services National Law*; as well as other State and Commonwealth regulatory laws that apply to operators of businesses, including corporations. The fact that the child care provisions in the family assistance law operate in this regulatory context partly justifies the broader ambit of circumstances in which protected information may be disclosed for enforcement related activities in guidelines dealing with child care matters. This is in contrast to the circumstances in which information may be disclosed in respect of other social welfare public disclosure frameworks where the only protected information relates to individual welfare or payment recipients.

Specific questions asked by the Committee

Regarding questions posed at paragraphs 1.23 and 1.24 of the Report, the 2018 Guidelines engage the prohibition on interference with privacy. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits unlawful or arbitrary interferences with a person's privacy. It also provides that persons have a right to the protection of the law against such interference.

The measure contained in section 9 is not "unlawful" for this purpose, noting that section 9 and other grounds in the 2018 Guidelines are lawfully made under a power in Commonwealth legislation, the *A New Tax System (Family Assistance) (Administration) Act 1999*, which enables the Minister for Education and Training to specify grounds on which disclosures may be made in the public interest. Further, the measure works in conjunction with and in support of, Commonwealth and State/Territory laws under which enforcement bodies derive their powers.

The use of the term "arbitrary" in Article 17 means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in all the circumstances. It is recognised that limitations may be imposed on the general prohibition on interference with privacy, provided that such limitations are reasonable, necessary and proportionate to the right of privacy.

An example of an "arbitrary" interference with privacy as found by the Human Rights Committee was in the case of *Toonen v Australia* (1994) in which a criminal law had the arbitrary effect of applying to same sex partners in a different way to opposite sex partners in circumstances where there was no justification for the differential operation of the law.

The amended version of section 9 of the 2018 Guidelines is not "arbitrary" for this purpose. The measure is proportionate, reasonable and necessary to enable information held by the Department of Education and Training or the Human Services Department to be provided in genuine cases where doing so is necessary in the public interest to regulatory bodies or agencies to assist them in exercising their regulatory powers and performing their regulatory functions under Commonwealth or State law.

Disclosures under the amended ground set out in section 9 is a legitimate objective for the purposes of human rights law because it will also promote a range of other human rights, including:

- The right to social security, as stated in Article 9 of the International Covenant on Economic, Social and Cultural Rights (ICESCR), including by requiring that a system be established under domestic law and that public authorities must take responsibility for the effective administration of the system.
- Disclosures under new section 9 will ensure that the Commonwealth's expenditure on child care payments remains targeted for their intended purpose and in particular, that misuse of child care payments by child care providers, including fraud, can be disclosed to appropriate enforcement bodies where doing so is necessary in the public interest.
- The rights of parents and children as stated in Articles 3, 18 and 19 of the Convention of the Rights of the Child (CRC) and Article 17 of the ICCPR. New section 9 will enable disclosure to Child Protection agencies, other State child welfare agencies or authorities, police, or other enforcement bodies where doing so is necessary to ensure the welfare of children.

While the Committee's Report notes that adherence with the Commonwealth *Privacy Act* 1988 is not sufficient to ensure compatibility with the right to privacy under human rights law, the Committee's Report at paragraph 1.19 and 1.20, in particular, notes that it remains unclear how the measure interacts with protections in the *Privacy Act 1988*.

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.

Further, due to section 95B 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.

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.

Furthermore, where 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.

The Australian Privacy Commissioner was not consulted in relation to the 2018 Determination. This was because, as outlined in detail above, the new 2018 Guidelines predominantly remake existing measures that had been. The 2018 Guidelines are therefore not a significant new measure.

Although the focus of the Committee's comments appear to be on the measure contained in section 9 relevant to "enforcement bodies", for completeness it is noted that the 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 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.

Regarding the question at paragraph 1.31 of the Report, as noted above, the "homeless young person" measure has 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. The measure applies to persons under 18 who have sought family assistance "on the ground of being a homeless person". Similar measures apply under public interest guidelines made under the social security law (see Part 3 of the *Social Security (Public Interest Certificate Guidelines) (DSS) Determination 2015*). Like other grounds in the 2018 Guidelines, this measure only permits disclosures that are necessary in the public interest, including, as set out in section 27, to address abuse or violence experienced by young persons.

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.

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.

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.

I trust this information addresses the Committee's comments.

Yours sincerely

DAN TEHAN

PARLIAMENT OF AUSTRALIA • HOUSE OF REPRESENTATIVES

PAUL FLETCHER MP

Federal Member for Bradfield

Minister for Families and Social Services

MC18-006606

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear Mr Goodenough

Thank you for your email dated 12 September 2018 on behalf of the Parliamentary Joint Committee on Human Rights. I appreciate the time you have taken to bring this matter to my attention.

The committee has requested further information on the human rights compatibility of the National Disability Insurance Scheme (Restrictive Practices and Behaviour Support) Rules 2018 (the Rules), as assessed in the committee's Report 9 of 2018. In particular, the committee has sought further advice on safeguards to prevent the 'first use' and 'single emergency use' of a regulated restrictive practice.

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.

Further, as mentioned in Minister Tehan's letter dated 28 August 2018, service providers are required to notify the Commission through the reportable incident obligations of the use of restrictive practices, including 'first use' and 'single emergency use' of a restrictive practice. This will allow the Commission to take appropriate action in response to the use of a restrictive practice in these circumstances.

Level 2, 280 Pacific Highway, Lindfield NSW 2070 • T 02 9465 3950
P O Box 6022 Parliament House, Canberra ACT 2600 • T 02 6277 7560
paul.fletcher.mp@aph.gov.au • www.paulfletcher.com.au • Liberal Member for Bradfield

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. 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.

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 (UNCRPD). 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.

Thank you again for bringing the committee's concerns to my attention.

Yours sincerely

Paul Fletcher

26 / 9 /2018

THE HON PETER DUTTON MP
MINISTER FOR HOME AFFAIRS

Ref No: MS18-009381

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear Ian, Mr Goodenough

Thank you for your correspondence of 17 October 2018 requesting further information on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018.

I have attached my response to the Parliamentary Joint Committee on Human Rights' Report 11 of 2018, as requested in your correspondence.

Yours sincerely

PETER DUTTON 01/11/18

Parliament House Canberra ACT 2600 Telephone: (02) 6277 7860 Facsimile: (02) 6273 4144

Response to Parliamentary Joint Committee on Human Rights report into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Schedule 1–Industry Assistance

The committee has raised a number of concerns about the compatibility of Technical Assistance Notices (TANs), Technical Capability Notices (TCNs) and Technical Assistance Requests (TARs) with the rights to privacy, freedom of expression and the right to an effective remedy. A response to these concerns is set out below.

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

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

1. ***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).***

The modern communications environment is rapidly moving towards the ubiquitous use of encryption to protect personal, commercial and government information. A corollary of this protection is that terrorist and criminal communications can be obscured from the traditional law enforcement and national security agency surveillance powers. Law enforcement and security agencies have definitively stated that this is negatively affecting their ability to detect and disrupt crime and terrorism.

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.

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.

Parliament has granted agencies powers to seize devices and access communications, provided there is a warrant issued by a judge or other relevant authority. However, agencies have reported that intercepted or accessed communications via warrant issued by an eligible Judge or AAT member are difficult, expensive, time-consuming and sometimes impossible to decrypt and effectively use for intelligence or investigation. The inability of agencies to use obtained communications has a significant impact on public safety and national security.

The requests and notices under Schedule 1 are designed to facilitate assistance, not require decryption. The reality is that agencies can leverage the broader cooperation of industry agencies to achieve results that mitigate the impact of 'going dark' (i.e. loss of visibility for communications). This may include seeking technical information to allow indigenous capabilities to be used more effectively, or enable access to facilities that allow existing warrants to be executed more effectively. 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).

Paragraph 4 of the Explanatory memorandum to the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill) sums up the problem:

> The increasing use of encryption has significantly degraded law enforcement and intelligence agencies' ability to access communications and collect intelligence, conduct investigations into organised crime, terrorism, smuggling, sexual exploitation of children and other crimes, and detect intrusions into Australian computer networks.

This shows that the '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.

Schedule 1 of the Bill introduces a framework for industry to provide technical assistance to law enforcement and national security agencies on either a voluntary or mandatory basis. The framework was drafted in a technologically agnostic way that will allow it to remain effective as communications technology advances. However, necessary safeguards and immunities ensure that the assistance is provided in a way that remains rationally connected and proportionate to its objectives is also incorporated.

2. 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;

A technical assistance request (TARs) is issued on a voluntary basis. Given that it is not a coercive power, the ability to issue a TAR was extended to the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD) as well as ASIO and the interception agencies.

TARs can only be issued to assist a relevant agency perform functions or powers conferred on it by law, and then only as far as it relates to a 'relevant objective'. This ensures that TARs are limited firstly to the lawful functions of the agency, and then only as they relate to a relevant objective. Where a TAR issuing agency has no function under law that can be exercised in relation to economic well-being or foreign relations it, by definition, could not make a request using the relevant objective.

Section 11(1) of the *Intelligence Services Act 2001* (the IS Act) sets out that the functions of ASIO, ASD and ASIS are to be performed 'only in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia'

Further, any act by an IS Act agency must be necessary for the proper performance of a function of that agency. This means that the limitations in the IS Act to these agencies will continue to apply, including the need to obtain Ministerial authorisation, as well as the requirement to seek a warrant where required under Australian law.

The relevant objective in relation to 'the interests of Australia's foreign relations or the interests of Australia's national economic well-being' directly reflects the functions under law of those intelligence agencies. Economic wellbeing and foreign relations must be considered as they relate to the role of intelligence agencies. In this context, the protection of Australia's foreign relations and economic well-being is intentionally linked with the protection of Australia's national security.

The serious nature of issues considered by these intelligence agencies, including intelligence gathering on a wide array of threats, in a national security context creates a permissible ground on which the right to freedom of expression can be restricted.

3. 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;

In the Statement of Compatibility with Human Rights, the purpose of the Bill is stated as 'to protect national security, public safety, address crime and terrorism', under paragraph 7 of the Bill's Explanatory Memorandum. 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 definition of '*interception agencies'* is not 'very broad'. The agencies captured are limited to those select agencies that have been deemed fit by Parliament to exercise telecommunications interception, which is by its nature one of the most intrusive powers granted to agencies. These agencies are subject to significant oversight and accountability mechanisms.

Interception agencies are also a limited subset of agencies that are able to access the content of communications under the TIA Act. In order to access communications content, a lawfully issued warrant (e.g. an interception warrant) will still be required. The assistance provisions do not allow access to personal content or data.

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.

4. 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

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). Requirements consistent with each form of assistance will always be set with reference to the decision-making criteria, the limitations against systemic weaknesses and accessing content. Importantly, any assistance given to conceal agency activities can't require providers to actively lie to a customer, as set out in section 317E(2).

The government asserts that each of the listed acts or things under section 317E demonstrate a rational connection, and are effective in resolving the core issue of degraded access to lawfully accessed communications. The table below outlines ways in which all the items at s317E might be used to assist agencies.

EXAMPLES OF ALL THE LISTED ACT OR THINGS AT S317E THAT MIGHT BE USED TO ASSIST AGENCIES

Operational examples from law enforcement agencies

Sub section 317E(1)	Listed act or thing	Examples
(a)	Removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider.	- Requesting an ISP provide the password they have enabled on a customer supplied home modem to facilitate a review of its logs during a search warrant to identify connected devices. - Requesting a cloud storage provider changes the password on a remotely hosted account to assist with the execution of an overt account based warrant.
(b)	Providing technical information	- An application provider providing technical information about how data is stored on a device (including the location of the encryption key) to enable forensically extracted data to be reconstructed. - An international cloud hosted storage provider providing details of where a customer's data is hosted to enable a MLAT process to be progressed to the host country seeking lawful access. - A mobile device provider providing a copy of their WiFi AP location maps generated through bulk analysis of customers data to correlate with location records extracted during a forensic examination of a device.
(d)	Ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format.	- Requesting a cloud service provider provide a copy of the contents of a hosted account in a particular format pursuant to the execution of an overt account based warrant. - Requesting that data held in a proprietary file format extracted from a device during a forensic examination pursuant to an overt

Sub section 317E(1)	Listed act or thing	Examples
		search warrant is converted into a standard file format.
(e)	Facilitating or assisting access to that which is the subject of eligible activities of the provider including, a facility, customer equipment, an electronic service etc.	- Requesting a shared data centre provide access to customers computer rack to enable the execution of a computer access warrant or installation of a data surveillance device under warrant.
(f)	Assisting with the testing, modification, development or maintenance of a technology or capability.	- Requesting that a social media platform assist with testing or development of a tool to automate the creation of online personas and historical content to facilitate online engagement.
(g)	Notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation.	- Requesting an ISP advise of any technical changes to their network which could impact on an existing interception.
(h)	Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider.	- Requesting 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 targets data. - Temporarily blocking internet messaging to force a device to send the messages as unencrypted SMS's.
(i)	Substituting, or facilitating the substitution of, a service provided by the designated communications provider for: another service	- Requesting a carrier force a roaming device to another carriers network to enable the enhanced metadata collection capabilities of the new carrier to collect information pursuant to a prospective data authorisation.

Sub section 317E(1)	Listed act or thing	Examples
	provided by the provider; or a service provided by another designated communications provider.	
(j)	An act or thing done to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to: - enforcing the criminal law and laws imposing pecuniary penalties; or - assisting the enforcement of the criminal laws in force in a foreign country; or - the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.	- Requesting that the provider not inform the customer of the assistance provided to enable a computer access warrant. - Requesting that the provider delete an audit log in a customer's device relating to a computer access warrant. - Requesting a provider restore a password that was temporarily changed to enable a computer access warrant. - Requesting a provider allocate a specific dynamic IP address relating to remote access pursuant to a computer access warrant to conceal the access.

Operational examples from intelligence agencies

Sub section 317E(1)	Listed act or thing	Examples
(a)	Removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider.	ASIO establishes physical access to a target's mobile phone and manages to acquire a copy of the phone's contents. The opportunity is rare and unique in that the target normally employs fairly good security awareness and tradecraft. Stored within the database of an application on the phone are historical conversations with other subjects of interest that indicate the group are in the initial stages of planning a mass casualty attack at an upcoming music festival. Unfortunately the copy of the phone's contents only reveals a snapshot in time of the targets' intentions and ASIO cannot formulate an informed assessment of the group's intended activities. The application used by the group stores messages on a server in the cloud and makes use of various authentication mechanisms to authorise access to user accounts, limiting ASIO's ability to establish contemporary coverage of the group. On seeking appropriate warrants authorising ASIO to lawfully gain coverage of the target's communications, ASIO seeks out the designated communications provider (DCP) with capacity to deactivate the relevant authentication mechanisms allowing, ASIO to authenticate the target's account to provide up-to-date and ongoing coverage of the group's intentions and threat to Australia's security.
(b)	Providing technical information	In the example above, once ASIO overcomes the relevant protection mechanisms to access the relevant communications, without further technical assistance from the DCP, ASIO could expend significant time and resources attempting to understand the structure of the database associated with the chat application. The database may be complex with messages, parties to a conversation and associated attached media all stored in different portions of the database making an assessment of the subjects involved in the plan and their intentions quite difficult. It could take ASIO months to organise the data in a legible format. Using a Technical Assistance Notice, ASIO would seek out the DCP responsible

Sub section 317E(1)	Listed act or thing	Examples
		for the application to gather technical information about how the application makes use of a database to store local copies of communications that have been sent and received by the application, enabling efficient and timely analysis of the relevant communications.
(C)	Installing, maintaining, testing or using software or equipment	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 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 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.
(d)	Ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format.	ASIO may require that information data obtained by a carrier in response to a warrant be provided in a format that is compatible with ASIO's systems and allows for appropriate analysis.
(e)	Facilitating or assisting access to that which is the subject of eligible activities of the provider including, a facility, customer equipment, an electronic service etc.	Further to the example above, ASIO, in conjunction with the DCP, identifies a physical data centre that represents the best location to acquire copies of the target's unencrypted communications; however, the data centre is owned and operated by a third-party company. ASIO in conjunction with the chat application DCP work with the data centre DCP to arrange

Sub section 317E(1)	Listed act or thing	Examples
		appropriate rack space, power and cabling for the ASIO server equipment.
(f)	Assisting with the testing, modification, development or maintenance of a technology or capability.	Further to the example above, ASIO assesses that any perceivable impact on the target's electronic service (the chat application) may result in an acceleration of the target's attack planning because ASIO assess the target exhibits a heightened level of paranoia, is erratic and prone to violence. ASIO works carefully with the DCP to ensure that the installed equipment has no perceivable effects on the target's usage of the app and is entirely covert in its operation.
(g)	Notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation.	In the above example, the DCP intends to change the physical location of their infrastructure and notifies ASIO in advance of the change so ASIO can plan for the relocation of the ASIO equipment to ensure coverage of the target's communications is maintained.
(h)	Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider.	It's feasible, in the example above, that ASIO's work with the DCP, ensuring that the installed equipment has no perceivable effects on the target's usage of the application, could require some modification, or substitution of, characteristics of a service provided by the DCP – or indeed, substitution of the service itself - in order to ensure the ongoing covert nature of ASIO's operation.
(i)	Substituting, or facilitating the substitution of, a service provided by the designated communications provider for: another service provided by the provider; or a service provided by another designated communications provider.	
(j)	An act or thing done to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or	Further to the above example, it's also feasible that various other activities would be required to ensure the ASIO's operation remains covert, including: - Requiring that the assistance provided is kept confidential by the provider.

Sub section 317E(1)	Listed act or thing	Examples
	a Territory, so far as the function or power relates to: - enforcing the criminal law and laws imposing pecuniary penalties - assisting the enforcement of the criminal laws in force in a foreign country; or - the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.	- Asking the staff involved in providing the service to sign confidentiality agreements. - Requesting that a cover story to be adopted when explaining the nature of assistance being provided. - Adjusting billing, account access, data transfer logs etc. to hide evidence of access to a target device or service. - Facilitating covert physical access to a facility.

5. whether the measures are proportionate to the stated objectives, including:

Each of the committee's queries in regards to proportionality are addressed in turn below.

a. 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;

The powers enabling interception agencies to issue notices and requests for assistance under the Bill are not vehicles for evidence collection in their own right and safeguards in the Bill prevent them from being used in substitution of an established warrant or authorisation. Proposed section 317ZH states that a TAN or TCN has no effect to the extent it requires a provider to do a thing for which a warrant or authorisation would otherwise be required, including:

- interception warrants;
- surveillance device warrants; and
- proposed and existing computer access warrants (CAWs).

This limitation reinforces a key purpose of the industry assistance framework – it supports existing warrants and does not independently allow access to personal communications. Therefore, the issue is not an insufficiency in the primary warrant framework, but rather the technical barriers that are being employed by criminals and terrorists in order to evade the lawful access of their communications.

Current obligations of industry to assist agencies are clearly insufficient. As noted in the Department's submission to the Parliamentary Joint Committee on Intelligence and Security, current obligations to

assist agencies with their lawful activities are located in the now inadequate section 313 of the *Telecommunications Act 1997*. This requires that a very limited subset of providers in the modern communications market, carriers and carriage service providers, provide 'reasonably necessary' assistance to a broader array of agencies. This includes assistance with giving effect to interception warrants or stored communications warrants. However, given the evolution of communications these traditional providers are often no longer best placed to ensure that the outcome sought by a warrant can be achieved. The current industry assistance framework also suffers from considerable ambiguity that has impacted agencies and providers alike. The measures seek to clarify and modernise existing industry assistance frameworks, introduce new safeguards into their exercise and ensure that underlying warrant and authorisation schemes remain fit for purpose.

b. safeguards relevant to the decision to issue technical assistance requests;

TARs are voluntary instruments that can be issued to a DCP to provide them with civil immunities for voluntary assistance provided consistent with the request. As the requests are voluntary in nature, the listed acts or things are non-exhaustive.

A DCP retains the legal capacity to refuse a request made by an agency, and agencies are required to notify the DCP that the request is voluntary. In addition, the purposes for which assistance may be requested are limited to the functions under law of the requesting agency, and then only as they relate to:

- enforcing the criminal law and laws imposing pecuniary penalties;
- assisting the enforcement of the criminal laws in force in a foreign country; and
- the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

A TAR can be issued by the various Directors-General of ASIO, ASIS and ASD, and chief officers of an interception agency. This ensures that issuing a TAR is done by the most senior officer of the relevant agencies. This power is delegable to appropriately senior officers of those agencies (generally an equivalent SES employee).

c. 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;

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. Parliament has rightly established strict oversight and accountability measures for statutory powers that intrude on the privacy of the community in that way. This Bill does not change that existing regime. These existing regimes, including those under the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* are subject to oversight by the Inspector-General of Intelligence and Security, Ombudsman, Parliament and Ministers. Accordingly, the powers that new requests and notices will be used in conjunction with are already subject to intense scrutiny.

However, oversight and review are still key considerations of the Bill. The issue of both TCNs and TANs are all subject to oversight by the highest levels of Government. A TAN may only be issued by the Director-General of ASIO, the chief officer of an interception agency or their senior delegate. A TCN may only be issued by the Attorney-General. It is important to note that subject to an urgent exception, the 28 day consultation period enables a DCP subject to a TCN to make a submissions to the Attorney-General that must be considered.

The agencies that can issue TAN's and TCN are all subject to strict oversight regimes by integrity bodies. The Bill allows for disclosure to the Commonwealth Ombudsman, State Ombudsman, integrity bodies in response to lawful requirements and explicit disclosure to the Inspector-General of

Intelligence and Security. These bodies retain the capacity to initiate investigations into agency misconduct.

Furthermore, depending on the body issuing a TAN or TCN, the Australian Constitution and the *Judiciary Act 1903* provide clear avenues for judicial review of the exercise of powers under new Part 15 of the *Telecommunications Act 1997*. For example, where a TAN has been issued by a Commonwealth interception agency (i.e. the AFP) or a TCN by the Attorney-General, these would be reviewable under the original jurisdiction of the High Court. In practice, this would mean review in the Federal Court through operation of the *Judiciary Act 1903*. Where a State interception agency issues a TAN (i.e. NSW Police), this would be reviewable by the Federal Court or State Supreme Courts through the *Judiciary Act 1903*. The issuance of a TAN by a Territory interception agency (i.e. NT Police) would be reviewable by the Federal Court through the *Judiciary Act 1903*.

Grounds for review are broad and may be on the basis that a requirement would create a systemic weakness into a form of encryption, contrary to the prohibition, or that in the circumstances the decision-maker could not have been satisfied that requirements in the notice were reasonable, proportionate, practical or technically feasible.

d. 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 industry assistance measures do not alter the underlying warrant or authorisation scheme of the *Telecommunications (Interception and Access) Act 1979*.

Legislation established prior to the enactment of the *Human Rights (Parliamentary Scrutiny) Act 2011* is not required to be subject to a human rights compatibility assessment. However, the Attorney-General's Department has provided extensive advice regarding the operation of the TIA Act to this Committee and other Parliamentary bodies. The privacy implications of the TIA Act were discussed in detail in Government responses to the Committee's scrutiny of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

Further, in response to recommendation 18 of the Report of the Inquiry into Potential Reforms of Australia's National Security Legislation by the Parliamentary Joint Committee on Intelligence and Security in 2013, the Government agreed to comprehensively revise the Act in a progressive manner. If legislation is introduced to reform the Act, the Department will undertake a human rights compatibility assessment.

e. 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);

Section 317ZH explicitly prohibits the use of notices to obtain information for which a warrant or authorisation would be required. A notice issued which purported to request access to such information would have no effect. For example under the *Telecommunications (Interception and Access) Act 1979* a warrant is required for the content of communications and an authorisation required for the disclosure of metadata; this prohibition clearly prevents the new measures from requiring both.

Further, the list of acts or things contained under section 317E, which applies to Schedule 1, does not include the disclosure of personal information as a form of assistance, as clearly specified in the Explanatory Memorandum.

For this reason, the Government does not consider it appropriate 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.

f. 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;

Existing prohibitions in legislation, like the prohibition against interception absent a warrant in section 7 of the *Telecommunications (Interception and Access) Act 1979* or the prohibition against disclosing data in section 276 of the *Telecommunications Act 1997* are still in effect. A voluntary TAR is not an avenue to overcome these provisions and allow agencies to do things that they are currently not authorised to do.

TAR's 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, such as the TIA Act, the *Surveillance Devices Act 2004*, the *Crimes Act 1914*, the *Australian Security Intelligence Organisation Act 1979*, the IS Act or equivalent State and Territory laws.

g. 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;

Because compliance with a TAR is voluntary, it could not be used to compel a provider to implement or build a systemic weakness or vulnerability. Section 317HAA requires that the agency issuing a TAR must advise the DCP that compliance with the request is voluntary.

It is not in the interests of the Australian Government to introduce systemic weaknesses and undermine the security of communications. The Government is considering whether amendments are necessary to extend the prohibition in 317ZG to technical assistance requests.

h. 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;

As above, Government is currently considering the possibility of amending sections 317ZG and 317ZH to also apply to technical assistance requests. However, government does note that the voluntary nature of TAR's may make this amendment unnecessary, as the DCP 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. Furthermore, as explained above, TARs do not overcome existing prohibitions against access content and data located elsewhere in statute. Government notes that the limitations set under sections 317ZG and 317ZH already apply to variations to technical assistance notices and technical capability notices.

i. 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

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 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.

j. any other information relevant to determining the proportionality of compatibility of the measures with the rights to privacy and expression.

The Government undertook extensive consultation, including a two stage consultation process on the text of the Bill. This process was productive and led to significant amendments that addressed key concerns, and reinforced the policy intent of the Bill. Importantly, the consultation process allowed government to clarify the strong safeguards and limitations in the Bill that carefully ensure that the privacy of Australians is not compromised, the security of digital systems is maintained and agency powers are utilised appropriately, which also assisted in ensuring the compatibility of the measures with the rights to privacy and expression.

6. Compatibility of the measures with the right to an effective remedy

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

The Committee has noted that there is an express exclusion of judicial review under the ADJR Act. The exclusion of review under the ADJR Act is consistent with the existing exclusion of other national security and law enforcement legislation and reflect the serious circumstances in which these powers are used and the need for timely execution.

In the event a DCP wishes to seek judicial review of any administrative decision to issue a notice, there are a number of grounds for challenging the decision (noted above), as well as specific defences. For example, a defence to enforcement is available where compliance with a notice would contravene a law of a foreign country. By way of example, a TAN or a TCN can be challenged if it were deemed to create broad vulnerabilities in a network or where it is infeasible that the decision-maker could have considered the requirements of the TAN or TCN to be reasonable or proportionate. Accordingly, judicial review is available for decisions under this Schedule. Merits review remains excluded: consistent with the Administrative Review Council's recommendations that certain national security and law enforcement powers may be unsuitable for merits review.[1]

As noted by the committee, both an affected person, and a provider on behalf of an affected person would have standing to challenge unlawful decision making. However, the 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.

Schedule 2

Compatibility of the measures with the right to privacy

[1] See Administrative Review Council Guide to '*What decisions should be subject to merit review*?' 1999.

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

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

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

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.

The Bill permits law enforcement, security and intelligence agencies to seek CAWs under a range of circumstances, such as the investigation of serious crimes (defined as offences with a minimum penalty of 3 years' imprisonment or above), monitoring compliance with control orders, integrity operations and recovery orders to assist in the location and safe recovery of children. The execution of a CAW is done covertly and remotely, limiting the interference with property and risk of harm to law enforcement officers.

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. As identified in the report and the explanatory memorandum of the Bill, these provisions engage the protection against arbitrary or unlawful interference with privacy contained within Article 17 of the ICCPR. Article 17 provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation, and that everyone has the right to the protection of the law against such interference or attacks.

However, the right to privacy under Article 17 can be permissibly limited in order to achieve a legitimate objective and where the limitations are lawful and not arbitrary. The term 'unlawful' in Article 17 of the ICCPR means that no interference can take place except as authorised under domestic law. Additionally, the term 'arbitrary' in Article 17(1) of the ICCPR means that any interference with privacy must be in accordance with the provisions, aims and objectives of the

ICCPR and should be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted 'reasonableness' to mean that any limitation must be proportionate and necessary in the circumstances.

The principal objectives of the Bill, and the associated limitations to the right to privacy, are to protect national security, public safety, and to address crime and terrorism. The Bill aims to protect the rights and freedoms of individuals by providing law enforcement and national security agencies with the tools they need to keep Australians safe.

Safeguards, oversight and proportionality

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.

Interference with data

Interference is not authorised when executing a CAW. 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 which may later that data.

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.

Emergency authorisations and CAWs

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.

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.

Lack of human rights compatibility statement for the SD Act

As the SD Act was enacted before the *Human Rights (Parliamentary Scrutiny) Act 2011*, it was not required to be subject to a human rights compatibility assessment.

However, the Government notes that the SD regime is subject to numerous broader safeguards which apply to the SD Act as a whole. These include:

- '*serious offence'* offence threshold (offences which attract a maximum penalty of 3 years' of imprisonment or more);
- Judicial oversight and approval for warrant powers;
- Oversight arrangements by the Commonwealth Ombudsman or the Inspector-General of Security and Intelligence (in the case of ASIO);
- Legislated reporting requirements for agencies; and
- Use and disclosure provisions (including offences for misuse and disclosure, and restrictions on the use of '*protected information'*[2]).

These mechanisms stand as significant safeguards to ensure that surveillance device powers continue to be exercised by law enforcement and national security agencies reasonably, proportionately and

[2] '*Protected information'* is a class of information protected under the SD Act which relates to information obtained from the use of a surveillance device, or relates to the use of the surveillance device (e.g. warrant information); see, section 44 of the SD Act.

only as necessary. Safeguards and oversight mechanisms which have been previously supported by Parliament given the passage of the SD Act in 2004.

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

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

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

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

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.

Compatibility of the use of force power with multiple rights

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

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

- **Whether the measure is aimed at achieving a legitimate objective for the purposes of human rights law;**

- **How the measure is effective to achieve (that is, rationally connected to) that objective; and**
- **Whether the limitation is a proportionate measure to achieve the stated objective.**

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

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), 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.

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.

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

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

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

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 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*.

Concealment of access powers Compatibility of the measures with the right to privacy

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

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

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

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.

The Government views there is a clear rational connection between the availability of concealment provisions both under this Bill and within the ASIO Act and the necessary pursuit of the legitimate objectives of public safety, public order and national security.

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.

Compatibility of the measures with the right to privacy

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

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

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

Importance of assistance orders to investigating serious crime and terrorism

Existing and proposed assistance orders are important to ensure that there is a mechanism to compel a person to provide assistance in certain circumstances. The use of an assistance order is an essential tool in the investigation 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. An example is the 2016 prosecution of an individual who was convicted of 13 charges relating to the control of multiple child sexual abuse websites on the 'dark web' which he used to access a network where he controlled, distributed and facilitated the production of child pornography material. He received total effective sentence of 15 years six months' imprisonment with a non-parole period of 10 years. For the offence under section 3LA, he was sentenced to six months' imprisonment, which must be considered in the context of the overall sentence.

Under the current section 3LA, a magistrate can compel certain persons (including owners and users of a device) to assist in providing access to data held in, or accessible from, a device that has been seized, moved or found in the course of a search authorised by a warrant. An order may also require a person to assist in copying data to another device and converting data into an intelligible form. Section 3LA also imposes an obligation, in limited circumstances, upon a person with knowledge of a computer or a computer system to assist law enforcement for the purposes of accessing the computer or computer system.

However, recent law enforcement experiences have highlighted that current assistance order powers are significantly outdated as they can only be issued pursuant only to a premises search warrant. Law enforcement can't compel that assistance in relation to a device, such as a mobile device, found on a person. Schedule 3 amends the *Crimes Act 1914* (Cth) to address this gap and to ensure existing assistance orders reflect the prevalence of devices such as smart phones and tablets being carried by people.

To reflect the importance of assistance orders to investigations and the deficiencies in the current regime, Schedule 3 also increases the penalties for not complying with orders from a judicial officer requiring assistance in accessing electronic devices where a warrant is in force. The Crimes Act assistance order will now be subject to a tiered penalty. Firstly, the existing penalty (lower offence) will increase from a maximum of two years imprisonment to a maximum five years imprisonment for

a ‘simple’ offence. A second higher offence of up to ten years imprisonment will be introduced for contravention of a ‘*serious offence’*[3] or a ‘*serious terrorism offence’*[4].

Engagement with human rights

There has been a previous assertion that assistance orders breach the right to not incriminate oneself under Article 14 of the ICCPR. The Government views that assistance orders do not engage this right on the basis that an assistance order does not prevent a person from remaining silent, or compel a person to confess guilt, but allows a device to be searched. This is not dissimilar from a search warrant on a premises where access to the premises cannot be denied or frustrated on the basis of self-incrimination. Assistance orders do not compel an individual to go into their device and disclose information or documents, it simply provides an avenue for law enforcement and national security agencies to lawfully gain access to that device, so that a lawful search of the device may be conducted as necessary. Further, assistance orders must be judicially authorised.

Where there is refusal, the Australian Federal Police/Commonwealth Director of Public Prosecutions may seek to pursue a criminal prosecution for non-compliance with the order. The penalties set as maximums will provide a range in which judicial officers will have discretion to decide what penalty is appropriate given the circumstances of the case.

Assistance orders do place limits on the right to privacy. However, much like many of the abovementioned investigatory powers, the right to privacy may be limited as long as it can be demonstrated that the limitation is necessary, proportionate and reasonable to achieving a legitimate objective. In this instance, the stated objective is to ensure that law enforcement have access to devices subject to protections such as passwords, or criminal accountability in the event that a person refuses and a prosecution is in the public interest. It is necessary, as discussed above, so that law enforcement are able to access devices that are used in the commission of criminal offences. It is necessary and proportionate given this process will require a lawful warrant as the basis for the order (e.g. is subject to the review and supervision by an independent and impartial body) to assure the Australian community that this power (both existing and proposed orders) will be based on the public interest.

Safeguards and oversight mechanisms of assistance orders

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. This Bill does not amend the existing robust safeguards and applies similar safeguards to the proposed new assistance orders in Schedules 2 and 5.

[3] A ‘*serious offence’* as defined under section 3C of the *Crimes Act 1914* includes any Commonwealth, State (with a federal aspect) or Territory offence that is punishable by imprisonment for 2 years or more.
[4] A ‘*serious terrorism offence’* as defined under the *Crimes Act 1914* includes various terrorism offences, such as providing support to a terrorism organisation, associating with a terrorism organisation.

The Government views both the proposed and existing assistance orders as reasonable, proportionate and necessary in achieving the legitimate objective of public safety, public order and national security.

Interception of communications under ASIO computer access warrants

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

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

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

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 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.

Incidental interception to give effect to a CAW 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.

Safeguards and oversight mechanisms

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[5] 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.

Assistance to foreign countries in relation to data held in computers

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

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

Review of Mutual Assistance in Criminal Matters Act 1987 (MACMA)

Australia's mutual assistance regime and procedures are frequently considered and assessed. The Government is satisfied with the current operation of MACMA. 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.

How the amendments under MACMA engage with human rights

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.

The stated objective of these amendments 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. 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.

For example, Article 6 of the ICCPR protects the right to life of a person. MACMA provides that where a person has been charged, arrested, detained or convicted of an offence that could result in the death penalty, mutual assistance must be refused unless there are '*special circumstances*'. The term

[5] Intercepted information obtained due to assisting in the execution of a CAW 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.

'special circumstances' is not defined in the MACMA but its Explanatory Memorandum 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. Where a person has not yet been charged, arrested, detained or convicted, there is a general discretion to refuse assistance.

Section 8 of MACMA provides for various other protections including the ability to refuse requests:

- which would involve investigating, prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, sex, sexual orientation, religion, nationality or political opinions.
- where there are substantial grounds for believing that if the request was granted the person would be in danger of being subject to torture. The discretion in paragraph 8(2)(g) of MACMA can cover any concerns about cruel, inhuman or degrading treatment of punishment.
- where the person has already been acquitted, pardoned or undergone punishment for the offence.

The Bill also provides for appropriate safeguards for the use of personal information collected and disclosed. 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, 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.

Including information obtained from a domestic investigation as part of the definition of 'Protected 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.

Schedules 3 to 5

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

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

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

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.

A CAW is an evidence-gathering tool and is not intended to be used to arbitrarily access data or prevent access to a computer in relation to an innocent third party. As a result, 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.

The Bill includes strong safeguards to ensure that CAWs are only issued to meet the legitimate objectives of law enforcement and the ABF, and that these measures do not adversely affect privacy and the integrity of the data or device. Importantly, the Bill requires the issuing officer to consider alternate means to obtaining evidence. Providing an exhaustive list in legislation for when CAWs can be issued 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.

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

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

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.
- 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.

As detailed above, the Bill includes provisions to minimise the impact on the right to privacy of innocent third-parties during the execution of a warrant. There are provisions which expressly prohibit 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.

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

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

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

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 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.

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.

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

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

The stated 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. The measure will also provide that a person or body is not subject to civil liability for, or in relation to, conduct that consists of, or is connected with giving, or is connected with giving information to ASIO, or giving or producing a document to ASIO, or making one or more copies of a document and giving those copies to ASIO.

Given this voluntary assistance relates to unsolicited help, the policy intention is to ensure that someone who reasonably believes that their help will assist benefits from the immunity.

It is likely that the proposed measure will engage and limit the right to an effective remedy where the acts of the person or body would ordinarily give rise to civil liability. This limitation is to ensure 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 Bill provides for a limitation to exemption from civil liability which is circumscribed and, once the Bill is passed, will be prescribed by law. In particular the limitation provides a list of activities that are excluded from the application of the civil immunity. This limitation is also shaped around the

restriction of being rationally connected to achieving the legitimate objective of protecting Australia's national security and proportionate.

The proposed measure does not provide immunity from criminal liability.

THE HON PETER DUTTON MP
MINISTER FOR HOME AFFAIRS

MS18-006298

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear ~~Mr~~ Ian, Goodenough

Thank you for your letter of 15 August 2018 in which further information was requested on the Unexplained Wealth Legislation Amendment Bill 2018.

I have attached my response to the Parliamentary Joint Committee on Human Rights' Report 7 of 2018 as requested in your letter.

I trust the information provided is helpful.

Yours sincerely

PETER DUTTON 11/09/18

Parliament House Canberra ACT 2600 Telephone: (02) 6277 7860 Facsimile: (02) 6273 4144

Unexplained Wealth Legislation Amendment Bill 2018

1.245 The preceding analysis of the proposed amendments to the unexplained wealth provisions in schedules 2 and 3 of the bill raise questions as to whether expanding the application of the POC Act is compatible with the right to a fair trial and the right to a fair hearing.

1.246 The committee seeks the advice of the minister as to whether these amendments to the POC Act are compatible with these rights, including:

- 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
- 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).

<u>The unexplained wealth provisions are civil in character</u>

The Commonwealth unexplained wealth provisions (as expanded by the Bill) are properly characterised as civil for the purposes of international human rights law. Unexplained wealth 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.

The Committee's Guidance Note 2 states that the test for whether a penalty can be classified as 'criminal' relies on three criteria: the domestic classification of the penalty, the nature and purpose of the penalty, and the severity of the penalty.

The *Proceeds of Crime Act 2002* (POC Act) expressly provides that asset recovery actions under the Commonwealth unexplained wealth regime are characterised as civil in nature under Australian law.[1]

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.[2] 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.[3]

The Committee's Guidance Note 2 provides that a penalty is likely to be considered criminal for the purposes of human rights law if the penalty is imprisonment or a substantial pecuniary sanction. Penalties under the POC Act cannot be commuted into a period of imprisonment. Unexplained

---

[1] *Proceeds of Crime Act 2002* (POC Act) s 315.

[2] Ibid s 5.

[3] See asset-directed restraint under the POC Act at s 20A(1)(g)(ii).

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. In addition, it remains open to a court to divert unexplained wealth amounts in certain circumstances, including to relieve particular dependants from hardship.[4]

Compatibility with criminal justice guarantees

As the unexplained wealth regime under the POC Act is civil in nature the criminal justice guarantees set out in Articles 14 and 15 of the International Covenant on Civil and Political Rights (ICCPR) are not relevant.

Compatible with the right to a fair hearing

As Schedules 2 and 3 amend a civil law, they engage the right to a fair hearing under Article 14(1) of the ICCPR. This right guarantees equality before courts and tribunals and, in the determination of any suit at law, the right to a fair and public hearing before a competent, independent and impartial court or tribunal established by law.

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.

The Committee has, however, raised concerns that laws which limit the right to a fair hearing may not be proportionate in doing so. In particular, the Committee raised concerns with protections provided to persons who are notified of an application for a restraining order but are not present at the hearing of that application. The Committee pointed out that the court may give the person leave to apply to revoke this order if the person had good reason for not appearing, but criticised this protection for its discretionary nature.[5]

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 at a hearing, it may be appropriate for the Court to not give a suspect leave to apply to revoke a restraining order where their delay in seeking revocation is considerable and designed to frustrate ongoing proceedings.

Schedules 2 and 3, and the expanded Commonwealth unexplained wealth regime, are therefore compatible with the relevant right to a fair hearing.

1.247 As the POC Act was introduced prior to the establishment of the committee, the committee recommends that 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. This would inform the committee's consideration of the compatibility of the amendments in the context of the legislative scheme as a whole.

---

[4] POC Act ss 179E(2)(b), 179J and 19L.

[5] POC Act s 31(3)(a).

I note this recommendation and reiterate that legislation established prior to the enactment of the *Human Rights (Parliamentary Scrutiny) Act 2011* is not required to be subject to a human rights compatibility assessment. 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.

1.255 The committee seeks the advice of the minister as to:

- **whether the measures in schedules 2 and 3 are rationally connected (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 are the least rights restrictive means of achieving the objective).**

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, 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.

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.

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.[6] 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.

1.265 The preceding analysis raises questions as to the compatibility of the abrogation of the privilege against self-incrimination with the right not to incriminate oneself in Article 14(3)(g) of the ICCPR.

---

[6] POC Act s 179E.

1.266 The committee seeks the advice of the minister as to whether the measures are a proportionate means of achieving the stated objective. This includes information as to whether a 'derivative use' immunity is reasonably available as a less rights restrictive alternative.

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.

As the Committee has pointed out, documents obtained through production orders are subject to a 'use immunity' preventing these documents from being used as evidence in criminal proceedings, but are not subject to a 'derivative use' immunity. This is appropriate, however, for the reasons outlined below.

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.

Where the proposed measures impact on the privilege against self-incrimination, this narrow limitation is therefore proportionate and permissible.

1.275 The committee seeks the advice of the minister as to the proportionality of the limitation on the right to privacy (including whether the measure is sufficiently circumscribed and whether there are safeguards in place with respect to the use, disclosure, storage and retention of information obtained pursuant to production orders).

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.

1.288 The committee therefore seeks the advice of 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 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).**

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.

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 going 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.

Human rights compatibility statement

I note this recommendation and reiterate that legislation established prior to the enactment of the *Human Rights (Parliamentary Scrutiny) Act 2011* is not required to be subject to a human rights compatibility assessment. 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.