Chapter 1

New and continuing matters

1.1 This report provides the Parliamentary Joint Committee on Human Rights' view on the compatibility with human rights of bills introduced into the Parliament from 23 February to 5 March 2015, legislative instruments received between 13 and 26 February 2015, and legislation previously deferred by the committee.

1.2 The report also includes the committee's consideration of responses arising from previous reports.

1.3 The committee generally takes an exceptions based approach to its examination of legislation. The committee therefore comments on legislation where it considers the legislation raises human rights concerns, having regard to the information provided by the legislation proponent in the explanatory memorandum (EM) and statement of compatibility.

1.4 In such cases, the committee usually seeks further information from the proponent of the legislation. In other cases, the committee may draw matters to the attention of the relevant legislation proponent on an advice-only basis. Such matters do not generally require a formal response from the legislation proponent.

1.5 This chapter includes the committee's examination of new legislation, and continuing matters in relation to which the committee has received a response to matters raised in previous reports.

Bills not raising human rights concerns

1.6 The committee has examined the following bills and concluded that they do not raise human rights concerns. The following categorisation is indicative of the committee's consideration of these bills.

1.7 The committee considers that the following bills do not require additional comment as they either do not engage human rights or engage rights (but do not promote or limit rights):

- Aboriginal and Torres Strait Islander Peoples Recognition (Sunset Extension) Bill 2015;
- Australian River Co. Limited Bill 2015;
- Customs Tariff (Anti-Dumping) Amendment Bill 2015;
- Defence Legislation Amendment (Parliamentary Approval of Overseas Service) Bill 2015;
- Imported Food Warning Labels Bill 2015;
- Offshore Petroleum and Greenhouse Gas Storage Amendment (Miscellaneous Matters) Bill 2015; and

- Offshore Petroleum and Greenhouse Gas Storage (Regulatory Levies) Amendment (Miscellaneous Matters) Bill 2015.

1.8 The committee considers that the following bills do not require additional comment as they promote human rights or contain justifiable limitations on human rights (and may include bills that contain both justifiable limitations on rights and promotion of human rights):

- Customs Amendment (Anti-dumping Measures) Bill (No. 1) 2015;
- International Aid (Promoting Gender Equality) Bill 2015;
- Landholders' Right to Refuse (Gas and Coal) Bill 2015;
- Limitation of Liability for Maritime Claims Amendment Bill 2015;
- Safety, Rehabilitation and Compensation Legislation Amendment (Exit Arrangements) Bill 2015; and
- Succession to the Crown Bill 2015.

Instruments not raising human rights concerns

1.9 The committee has examined the legislative instruments received in the relevant period, as listed in the *Journals of the Senate*.[1] Instruments raising human rights concerns are identified in this chapter.

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

Deferred bills and instruments

1.11 The committee has deferred its consideration of the following bills and instruments:

- Australian Border Force Bill 2015;
- Customs and Other Legislation Amendment (Australian Border Force) Bill 2015;
- Criminal Code Amendment (Animal Protection) Bill 2015 (deferred 3 March 2015);
- Migration Amendment (Strengthening Biometrics Integrity) Bill 2015;
- Extradition (Vietnam) Regulation 2013 [F2013L01473] (deferred 10 December 2013);

---

1 See Parliament of Australia website, 'Journals of the Senate', http://www.aph.gov.au/Parliamentary_Business/Chamber_documents/Senate_chamber_documents/Journals_of_the_Senate.

- Migration Amendment (2014 Measures No. 2) Regulation 2014 [F2014L01696] (deferred 10 February 2015);
- Migration Amendment (Subclass 050 Visas) Regulation 2014 [F2014L01460] (deferred 10 February 2015); and
- Migration Legislation Amendment (2014 Measures No. 2) Regulation 2014 [F2014L01461] (deferred 10 February 2015).

1.12 The following instruments have been deferred in connection with the committee's ongoing examination of the autonomous sanctions regime and the Charter of the United Nations sanctions regime:

- Autonomous Sanctions (Designated and Declared Persons - Former Federal Republic of Yugoslavia) Amendment List 2014 (No. 2) [F2014L00970] (deferred 2 September 2014);
- Autonomous Sanctions (Designated Persons and Entities and Declared Persons – Democratic People's Republic of Korea) Amendment List 2013 [F2013L02049] (deferred 11 February 2014);
- Autonomous Sanctions (Designated Persons and Entities and Declared Persons – Democratic People's Republic of Korea) Amendment List 2015 [F2015L00061] (deferred 3 March 2015);
- Autonomous Sanctions (Designated Persons and Entities and Declared Persons - Iran) Amendment List 2013 (No. 1) [F2013L01312] (deferred 10 December 2013);
- Autonomous Sanctions (Designated Persons and Entities and Declared Persons - Ukraine) Amendment List 2014 [F2014L01184] (deferred 24 September 2014);
- Charter of the United Nations (Sanctions - Democratic People's Republic of Korea) Amendment Regulation 2013 (No. 1) [F2013L01384] (deferred 10 December 2013); and
- Charter of the United Nations Legislation Amendment (Sanctions 2014 – Measures No. 2) Regulation 2014 [F2014L01701] (deferred 3 March 2015).

1.13 The following instruments have been deferred in connection with the committee's current review of the *Stronger Futures in the Northern Terrority Act 2012* and related legislation:

- Aboriginal Land Rights (Northern Territory) Amendment (Delegation) Regulation 2013 [F2013L02153] (deferred 10 December 2013);
- Social Security (Administration) (Declared income management area - Ceduna and surrounding region) Determination 2014 [F2014L00777] (deferred 10 February 2015);

- Social Security (Administration) (recognised State/Territory Authority - NT Alcohol Mandatory Treatment Tribunal) Determination 2013 [F2013L01949] (deferred 10 December 2013);
- Social Security (Administration) (Recognised State/Territory Authority – Qld Family Responsibilities Commission Determination 2013 [F2013L02153] (deferred 11 February 2014);
- Stronger Futures in the Northern Territory Regulation 2013 [F2013L01442] (deferred 10 December 2013); and
- Social Security (Administration) (Excluded circumstances – Queensland Commission) Specification 2014 [F2015L00002] (deferred 3 March 2015).

Appropriation Bill (No. 3) 2014-2015

Appropriation Bill (No. 4) 2014-2015

Portfolio: Finance
Introduced: House of Representatives, 12 February 2014

Purpose

1.14 The Appropriation Bill (No. 3) 2014-2015 proposes appropriations from the Consolidated Revenue Fund (CRF) for the ordinary annual services of the government.

1.15 The Appropriation Bill (No. 4) 2014-2015 proposes appropriations from the CRF for services that are not considered to be for the ordinary annual services of the government.

1.16 Together, Appropriation Bill (No. 3) 2014-2015 and Appropriation Bill (No. 4) 2014-2015 are referred to as 'the bills'.

1.17 The amounts proposed for appropriation by the bills are in addition to the amounts appropriated through the Appropriation Acts that implemented the 2014-2015 Budget.

1.18 Measures raising human rights concerns or issues are set out below.

Potential engagement and limitation of human rights by appropriations Acts

1.19 Each of the bills is accompanied by a brief and substantially identical statement of compatibility which notes that the High Court has stated that, beyond authorising the withdrawal of money for broadly identified purposes, appropriations Acts 'do not create rights and nor do they, importantly, impose any duties'.[1] The statements of compatibility conclude that, as their legal effect is limited in this way, the bills do not engage, or otherwise affect, human rights.[2] They also state that '[d]etailed information on the relevant appropriations, however, is contained in the portfolio [Budget] statements'.[3] No further assessment of the bills' compatibility with human rights is provided.

1 Explanatory memorandum, Appropriation Bill (No. 3) 2014-2015 (EM A) 4; Explanatory memorandum, Appropriation Bill (No. 4) 2014-2015 (EM B) 4.

2 EM A, 4; EM B, 4.

3 EM A, 4; EM B, 4.

1.20 The committee notes that substantially identical statements of compatibility were provided for previous appropriations bills considered by the committee.[4]

Multiple rights

1.21 In accordance with its previous assessment of appropriations bills, the committee notes that proposed government expenditure to give effect to particular policies may engage and limit and/or promote a range of human rights. This includes rights under the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic Social and Cultural Rights (ICESCR).[5]

Assessment of the compatibility of the bills with human rights

1.22 The committee considers that the High Court case which held that appropriations Acts do not create rights or duties as a matter of Australian law does not fully address the fact that appropriations bills may nevertheless engage rights according to Australia's obligations under international human rights law.

1.23 First, compliance with Australia's obligations to progressively realise economic, social and cultural rights using the maximum of resources available is reliant on government allocation of budget expenditure.

1.24 Second, specific appropriations may involve reductions in expenditure which amount to retrogression or limitations on rights. The UN Office of the High Commissioner for Human Rights has noted the following with respect to human rights and budgets:

> States are required to make use of the maximum of their available resources for the progressive realization of economic, social and cultural rights (International Covenant on Economic, Social and Cultural Rights, art. 2 (1)). Budgets (federal, national, provincial or local) are essential instruments of policymaking, and often involve various departments in the central Government as well as in the legislative bodies, regional governments and autonomous institutions. Through public budgeting, the State authorities establish priorities and express their commitment to

4 See Parliamentary Joint Committee on Human Rights, *Third Report of 2013* (13 March 2013); Parliamentary Joint Committee on Human Rights, *Seventh Report of 2013* (5 June 2013); Parliamentary Joint Committee on Human Rights, *Third Report of the 44th Parliament* (4 March 2014); and Parliamentary Joint Committee on Human Rights, *Eighth Report of the 44th Parliament* (24 June 2014).

5 See Parliamentary Joint Committee on Human Rights, *Third Report of 2013* (13 March 2013); Parliamentary Joint Committee on Human Rights, *Seventh Report of 2013* (5 June 2013); Parliamentary Joint Committee on Human Rights, *Third Report of the 44th Parliament* (4 March 2014); and Parliamentary Joint Committee on Human Rights, *Eighth Report of the 44th Parliament* (24 June 2014).

> concrete actions which may improve – or limit – the enjoyment of some social guarantees.[6]

1.25 On this basis, the appropriation of funds facilitates the taking of actions which both effect the progressive realisation of, and the failure to fulfil, Australia's obligations under the treaties listed in the *Human Rights (Parliamentary Scrutiny) Act 2011*.

1.26 Therefore, as noted in previous reports, the committee considers that, where there is a sufficiently close connection between a particular appropriations bill and the implementation of new legislation, policy or programs, or the discontinuation or reduction in support of a particular policy or program, that may engage human rights, the statement of compatibility for that bill should provide an assessment of any limitations of human rights that may arise from that engagement.[7]

1.27 However, notwithstanding the fact of the capacity of appropriations bills to engage and limit human rights, the committee acknowledges that such bills may present particular difficulties given their technical and high-level nature, and because they generally include appropriations for a wide range of programs and activities across many portfolios. The committee notes that these issues have been the subject of a constructive dialogue with the Department of Finance,[8] and that the Minister for Finance has previously invited committee members to be briefed by departmental officials in relation to these issues.[9]

1.28 Taking into account such characteristics of appropriations bills, the committee acknowledges that the approach to human rights assessment of appropriations bills for the purposes of the *Human Rights (Parliamentary Scrutiny) Act 2011* may not generally be possible at the level of individual measures.

1.29 However, the committee considers that the allocation of funds via appropriations bills is susceptible to a human rights assessment that is directed at broader questions of compatibility—namely, their impact on progressive realisation obligations and on vulnerable minorities or specific groups (such as children; women; Aboriginal and Torres Strait Islander Peoples; persons with disabilities; and ethnic minorities). The committee notes that there are some precedents in the Australian context for assessments of this nature in relation to budgetary measures by government which could inform the development of an appropriate template for the

---

6 UN Office of the High Commissioner for Human Rights, *Manual on Human Rights Monitoring*, http://www.ohchr.org/Documents/Publications/Chapter20-48pp.pdf.

7 See, for example, Parliamentary Joint Committee on Human Rights, *Eighth Report of the 44th Parliament* (24 June 2014) 7.

8 Parliamentary Joint Committee on Human Rights, *Seventh Report of 2013* (5 June 2013) 21.

9 Parliamentary Joint Committee on Human Rights, *Eighth Report of the 44th Parliament* (18 June 2014) 7.

assessment of appropriations bills for the purposes of the *Human Rights (Parliamentary Scrutiny) Act 2011*.[10]

1.30 The committee notes also that there are a range of international resources to assist in preparing assessments of budgets for human rights compatibility.[11]

1.31 In keeping with the past constructive engagement with the Department of Finance, the committee indicates its willingness to assist with the development of a template and approach to preparing statements of compatibility for appropriations bills that would support the assessment and examination of appropriations bills as required by the *Human Rights (Parliamentary Scrutiny) Act 2011*.

1.32 **The committee therefore considers that the appropriation of funds via annual and additional appropriations Acts may engage and potentially limit or promote a range of human rights that fall under the committee's mandate. In particular, the committee considers there may be specific appropriations bills or specific appropriations where there is an evident and substantial link to the carrying out of a policy or program under legislation that gives rise to human rights concerns. The committee considers that, where there is a sufficiently close connection between a particular appropriations bill and the implementation of new legislation, policy or programs, or the discontinuation or reduction in support of a particular policy or program that may engage human rights, the statement of compatibility for that bill should provide an assessment of any limitations of human rights that may arise from that engagement. As set out above, the statement of compatibility for the bills provides no assessment of their human rights compatibility.**

1.33 **In order to assist the Minister for Finance in assessing any limitations on human rights in relation to these bills, the committee considers that attention should be given to the following questions in assessing whether the bills are compatible with Australia's human rights obligations:**

- **whether the bills are compatible with Australia's obligations of progressive realisation with respect to economic, social and cultural rights;**

---

10 For example, from 1983 to 2013 a Women's Budget Statement was prepared by the Australian Government which set out the impact of budget measures on women and also gender equality.

11 See, for example, Diane Elson, *Budgeting for Women's Rights: Monitoring Government Budgets for Compliance with CEDAW*, (Unifem, 2006) http://www.unicef.org/spanish/socialpolicy/files/Budgeting_for_Womens_Rights.pdf; UN Practitioners' Portal on Human Rights Approaches to Programming, *Budgeting Human Rights* http://hrbaportal.org/archives/tools/budgeting-human-rights; Rory O'Connell, Aoife Nolan, Colin Harvey, Mira Dutschke, Eoin Rooney, *Applying an International Human Rights Framework to State Budget Allocations: Rights and Resources* (Routledge, 2014).

- **whether any reductions in the allocation of funding are compatible with Australia's obligations not to unjustifiably take backward steps (a retrogressive measure) in the realisation of economic, social and cultural rights; and**
- **whether the allocations are compatible with the rights of vulnerable groups (such as children; women; Aboriginal and Torres Strait Islander Peoples; persons with disabilities; and ethnic minorities).**

Defence Trade Controls Amendment Bill 2015

Portfolio: Defence
Introduced: House of Representatives, 26 February 2015

Purpose

1.34 The Defence Trade Controls Amendment Bill 2015 (the bill) seeks to amend the *Defence Trade Controls Act 2012* (the Act) to:

- delay the commencement of offence provisions by 12 months to ensure that stakeholders have sufficient time to implement appropriate compliance and licensing measures;
- provide for new offences or amend existing offences relating to export controls;
- require approvals only for sensitive military publications and remove controls on dual-use publications;
- require permits only for brokering of sensitive military items and remove controls on most dual-use brokering, subject to international obligations and national security interests; and
- provide for review of the Act, initially two years after the commencement of section 10, and for the minister to table a copy of the review report in each House of Parliament.

1.35 Measures raising human rights concerns or issues are set out below.

Reverse evidential burdens

1.36 The bill seeks to amend a number of existing offences to introduce statutory exceptions to those offences. These exceptions would reverse the onus of proof and place an evidential burden on the defendant to establish (prove) that the statutory exception applies in a particular case.

1.37 To establish that the new exceptions would apply, the defendant would be required to prove the following in respect of each offence:

- in relation to the offence of supply of technology defined in the Defence and Strategic Goods List (DSGL technology) that the offence does not apply if:
  - the supply is not the provision of access to that technology;
  - the supply is made orally; and
  - the supply is neither for a military end-use nor for use in a Weapons of Mass Destruction Program;[1]

1 See item 17 of the bill.

- in relation to the offence of supply of DSGL technology that the offence does not apply if:
  - the supply is within the scope of Part 2 of the List;
  - the supply is preparatory to the publication of the DSGL technology to the public; and
  - there is no notice in force in relation to the supplier and the technology;[2]
- in relation to the offence of publishing DSGL technology that the offence does not apply if:
  - the DSGL technology has already been lawfully made available to the public;[3]
- in relation to the offence of arranging for another person to supply specified goods or DSGL technology that the offence does not apply if:
  - the person arranges for the other person to make the supply from a foreign country; and
  - that country is a participant in certain groups and that country is specified in a legislative instrument.[4]
- in relation to the offence of arranging for another person to supply specified goods or DSGL technology that the offence does not apply if:
  - the person arranges for the supply under or in connection with a contract specified in a legislative instrument.[5]

1.38 The committee considers that reversing the burden of proof engages and limits the right to be presumed innocent.

Right to a fair trial (presumption of innocence)

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

1.40 An offence provision which requires the defendant to carry an evidential or legal burden of proof with regard to the existence of some fact will engage the

2 See item 21 of the bill.

3 See item 32 of the bill, proposed new subsection 14A(2).

4 See item 41 of the bill, proposed new subsection 15(4).

5 Seem item 41 of the bill, proposed new subsection 15(4B).

presumption of innocence because a defendant's failure to discharge the burden of proof may permit their conviction despite reasonable doubt as to their guilt.

1.41 However, reverse burden offences will not necessarily be inconsistent with the presumption of innocence provided that they are within reasonable limits which take into account the importance of the objective being sought and maintain the defendant's right to a defence. In other words, such provisions must be reasonable, necessary and proportionate to that aim.

Compatibility of the measure with the right to a fair trial (presumption of innocence)

1.42 The statement of compatibility notes that the bill includes a number of defences that reverse the onus of proof and so limit the right to be presumed innocent.

1.43 In concluding that the measure is compatible with the right to a fair trial, the statement of compatibility states that the objective of the measure is to 'enhance the export control regime which supports Australia's defence, security and international obligations'.[6] It further notes that the reason for reversing the burden of proof in each case is that the evidence for the defences would either be solely within the defendant's personal knowledge or because the defendant would have particular knowledge of the matter and it would be reasonable, more practical and less burdensome for the defendant to establish these facts.[7]

1.44 However, while the committee accepts that the offences in the Act and the amendments in the bill seek to achieve the legitimate objective of enhancing the export control regime which supports Australia's defence, security and international obligations, the committee is concerned that not all of the reverse burden provisions may be proportionate to achieving that objective.

1.45 While some aspects of the exceptions appear to be properly characterised as falling within the particular knowledge of the defendant (such as whether the defendant made the supply orally), it is not clear to the committee that it is reasonable to impose an evidential burden on the defendant in relation to all of the matters specified in the proposed new defences. In particular, it is not apparent that the following would be particularly within the knowledge of the defendant, to such an extent, as to make it reasonable in all the circumstances to reverse the burden of proof. Rather, such matters would appear more likely to be within the government's particular knowledge and expertise:

- that the supply is within the scope of Part 2 of the Defence and Strategic Goods List, which is a list formulated by the minister;[8]

6 Explanatory memorandum (EM) 45.

7 EM, 44-45.

8 See item 21 of the bill.

- that there is no notice in force in relation to the supplier and the technology;[9]
- that a country is a participating state for the purposes of the Wassenaar Arrangement; a participant in the Australia Group; a partner in the Missile Technology Control Regime; and a participant in the Nuclear Suppliers Group;[10]
- that a country is specified in a legislative instrument;[11] and
- that the supply is made under or in connection with a contract specified in a legislative instrument.[12]

1.46 In addition, reversing the burden of proof in the following instances would appear to require the defendant to prove an element of the offence, which should more properly fall on the prosecution:

- proving that the supply of DSGL technology is not the provision of access to that technology;[13] and
- proving that the supply is not for a military end-use nor for use in a Weapons of Mass Destruction Program.[14]

1.47 In relation to the exceptions listed above at [1.43] to [1.44], the committee considers that the statement of compatibility has not explained why these exceptions should be proven by the defendant. The committee appreciates that in drafting an exception to an offence it may be easier to include all elements of the exception in one subsection. However, the prosecution usually has a heavy burden of proof and reasons of ease or convenience alone will not be sufficient for the purpose of justifying a limitation on the right to be presumed innocent. For the purposes of international human rights law, the reversal of the burden of proof must only be done to the extent that it is proportionate to its stated objective, including that there is no other less restrictive way to achieve the same objective.

1.48 **The committee considers that the measures reversing the burden of proof in relation to the proposed new statutory exceptions (defences) limit the right to be presumed innocent. As set out above, the statement of compatibility does not sufficiently justify that limitation for the purpose of international human rights law, in particular that it is reasonable to reverse the burden of proof in relation to**

9 See item 21 of the bill.

10 See item 41 of the bill, proposed new subsection 15(4).

11 See item 41 of the bill, proposed new subsection 15(4).

12 See item 41 of the bill, proposed new subsection 15(4B).

13 See item 17 of the bill.

14 See item 17 of the bill.

all elements of the defence. The committee therefore seeks the advice of the Minister for Defence as to whether the limitation on the presumption of innocence is a reasonable and proportionate measure to achieve the stated objective.

Migration Amendment (Maintaining the Good Order of Immigration Detention Facilities) Bill 2015

Portfolio: Immigration and Border Protection
Introduced: House of Representatives, 25 February 2015

Purpose

1.49 The Migration Amendment (Maintaining the Good Order of Immigration Detention Facilities) Bill 2015 (the bill) seeks to amend the *Migration Act 1958* to allow an authorised officer to use such reasonable force against any person or thing as the authorised officer reasonably believes is necessary to:

- protect the life, health, or safety of any person in an immigration detention facility (IDF); or
- maintain the good order, peace or security of an IDF.

1.50 The bill also:

- provides for a statutory complaints mechanism; and
- imposes a bar on any action against the Commonwealth in the exercise of a power to use reasonable force if the power was exercised in good faith.

1.51 Measures raising human rights concerns or issues are set out below.

Use of force

1.52 Proposed section 197BA gives power to an authorised officer to use force in immigration detention facilities. An 'authorised officer' is one authorised in writing by the Minister for Immigration and Border Protection (the minister) or the Secretary of the Department of Immigration and Border Protection (the department) for that purpose.

1.53 The use of reasonable force is permitted when the 'authorised officer reasonably believes' it is necessary to protect the life, health or safety of any person or to maintain the good order, peace or security of an IDF.

1.54 Proposed new subsection 197BA(2) sets out a non-exhaustive list of factors as to when force may be used, including:

- to protect a person from harm or from a threat of harm, including self-harm;
- to prevent the escape of a detainee;
- to prevent a person from damaging, destroying or interfering with property;
- to move a detainee within the facility; and
- to prevent action in the facility by any person that endangers life, health or safety or that disturbs the good order, peace or security of the facility.

1.55 There are limitations on the exercise of the power. The bill provides that the power must not be used to give nourishment or fluids to a detainee, and an authorised officer must not subject a person to greater indignity than the officer reasonably believes is necessary in the circumstances. An authorised officer must not, in exercising the power, do anything likely to cause grievous bodily harm unless the officer reasonably believes that doing the thing is necessary to protect the life of, or to prevent serious injury to, another person (including the officer).[1]

1.56 The committee considers that this measure engages and limits a number of rights, including the right to life; the prohibition against torture, cruel, inhuman or degrading treatment; the right to humane treatment in detention; and the right to freedom of assembly.

Right to life

1.57 The right to life is protected by article 6(1) of the International Covenant on Civil and Political Rights (ICCPR) and article 1 of the Second Optional Protocol to the ICCPR. The right to life has three core elements to it:

- it prohibits the state from arbitrarily killing a person;
- it imposes an obligation on the state to protect people from being killed by others or identified risks; and
- it requires the state to undertake an effective and proper investigation into all deaths where the state is involved.

1.58 The use of force by state authorities resulting in a person's death can only be justified if the use of force was necessary, reasonable and proportionate in the circumstances. For example, the use of force may be proportionate if it is in self-defence, for the defence of others or if necessary to effect arrest or prevent escape (but only if necessary and reasonable in the circumstances).

1.59 In order to effectively meet this obligation, states must have in place adequate legislative and administrative measures to ensure police and the armed forces are adequately trained to prevent arbitrary killings.

Compatibility of the measure with the right to life

1.60 The committee notes that empowering officers to use force against a person in an immigration detention facility engages and limits the right to life, as force may be used that could lead to a loss of life. However, a measure that limits the right to life may be justifiable if it is demonstrated that it addresses a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

1 See proposed new subsections 197BA(4) and (5).

1.61 The statement of compatibility acknowledges that the bill engages the right to life, noting that 'circumstances may arise in the detention context where a degree of force may be necessary, such as where a person in a detention centre threatens to harm him or herself, or others'. However, it concludes that the measure is compatible with the right to life because '[a]ny use of force pursuant to the Bill would be lawful' and 'would not be arbitrary, because it is necessary, reasonable and proportionate in the circumstances'.[2]

1.62 However, the committee considers that the statement of compatibility does not provide a sufficiently reasoned and evidence-based explanation of how the measure supports a legitimate objective for the purposes of international human rights law.[3] The committee notes that to be capable of justifying a proposed limitation of human rights, a legitimate objective must address a pressing or substantial concern and not simply seek an outcome regarded as desirable or convenient.

1.63 In this respect, the statement of compatibility states that the objective of the bill is to remove uncertainty for employees of an Immigration Detention Services Provider (IDSP) concerning their authority to use reasonable force. It explains:

> The amendments in this Bill address issues arising from incidents at a number of IDFs, which highlighted uncertainty, on the part of the IDSP, as to when it may act when confronted with public order disturbances in IDFs and how it may act in relation to the police.
>
> In the absence of provisions in the Act that authorise the use of reasonable force to protect the life, health or safety of a person within an IDF, the IDSP relies on the common law powers, as conferred on ordinary citizens, to exercise reasonable force when necessary to protect their officers and others from harm within an IDF. However, the extent of this authority is limited. Under common law, it is only possible after the event, to say whether the force used was reasonable in the circumstances. That is, reasonable force can only be used to suppress a disturbance where, objectively, it is deemed necessary.

---

2 EM, Attachment A, 20.

3 See the committee's Guidance Note 1 (Appendix II; See Parliamentary Joint Committee on Human Rights, Guidance Note 1 - Drafting Statements of Compatibility (December 2014) http://www.aph.gov.au/~/media/Committees/Senate/committee/humanrights_ctte/guidance_notes/guidance_note_1/guidance_note_1.pdf) and the Attorney-General's Department's guidance on the preparation of statements of compatibility, which states that the 'existence of a legitimate objective must be identified clearly with supporting reasons and, generally, empirical data to demonstrate that [it is] important': Attorney-General's Department, Template 2: Statement of compatibility for a bill or legislative instrument that raises human rights issues at http://www.ag.gov.au/RightsAndProtections/HumanRights/PublicSector/Pages/Statementofcompatibilitytemplates.aspx.

1.64 The statement of compatibility also references the recommendation of the Independent Review of the Incidents at the Christmas Island Immigration Detention Centre and Villawood Immigration Detention Centre (the Hawke-Williams Report), conducted by Dr Allan Hawke AC and Ms Helen Williams AO in 2011, that the department more clearly articulate the responsibility of public order management between the department, the IDSP, the Australian Federal Police and other police forces who may attend an IDF. It observes:

> The amendments…specifically permit use of reasonable force by authorised officers for certain purposes, including for the purpose of maintaining the good order, peace and security of an IDF. The Bill would thereby remove uncertainty on the part of employees of the IDSP concerning their authority to use reasonable force to prevent or contain disturbances in an IDF.[4]

1.65 The statement of compatibility also points to a range of safeguards to support its conclusion that the proposed measures are proportionate to their stated objective, such as that force may only be used where the authorised officer reasonably believes it is necessary in the circumstances.

1.66 However, it is unclear to the committee that the objective of removing uncertainty for employees of an IDSP concerning their authority to use reasonable force, in and of itself, addresses a pressing or substantial concern. In particular, the statement of compatibility does not specify any particular instances or circumstances where the current requirement that IDSP officers may only use force when objectively necessary has been uncertain in its application; and does not explain what the consequences of any such cases have been.

1.67 Further, the committee notes that the Hawke-Williams Report, which is cited in support of the stated objective of the measure, does not contain any reference to the inadequacy of the common law regarding the use of force and did not recommend creating a statutory use of force power for employees of an IDSP. Rather, it focused on ensuring appropriate arrangements to clarify the respective roles and responsibilities of managing security between the department, the IDSP and the police; and recommended a protocol be developed to support the hand-over of incidents to the police and consideration be given whether the contract with the IDSP needed to be amended.[5] The committee therefore does not consider that the report provides evidence in support of the measure as addressing a substantial or pressing concern.

---

4 EM, Attachment A, 20.

5 *Independent Review of the Incidents at the Christmas Island Immigration Detention Centre and Villawood Immigration Detention Centre*, conducted by Dr Allan Hawke AC and Ms Helen Williams AO (31 August 2011) 88-91.

1.68 The committee also considers that the proposed measures may not be a proportionate way to achieve their stated objective, and particularly that they are the least restrictive way to achieve the stated objective.

1.69 First, the bill appears to lack a number of safeguards that apply to analogous state and territory legislation governing the use of force in prisons. For example, there is no requirement that:

- the use of force only be used as a last resort;
- force should be used only if the purpose sought to be achieved cannot be achieved in a manner not requiring the use of force;
- the infliction of injury is to be avoided if possible;
- use of force to protect a person from a 'threat of harm' applies only to an 'imminent' threat;
- the use of force to 'prevent a person from damaging, destroying or interfering with property' is permissible only if the person is in the process of damaging the property and, if not, there must be a reasonable apprehension of an immediate attack; and
- the use of force be limited to situations where the officer cannot otherwise protect him or herself or others from harm.

1.70 The committee notes that the bill does not define the expression 'reasonable force', and that 'policy' rather than legislation, will set out what constitutes reasonable force:

> Under policy, reasonable force must be no more than that required to ensure the life, health or safety of any person in the facility, be consistent with the seriousness of the incident, be proportional to the level of resistance offered by the person, avoid inflicting injury if possible, and be used only as a measure of last resort.[6]

1.71 While this policy guidance incorporates some elements of the safeguards identified above as contained in analogous cases, the committee considers that the placing of such safeguards on a policy, rather than a statutory, footing is insufficient to provide a justification for limitations on human rights.

1.72 Further, the committee notes that the bill would allow force to be used to prevent any action that disturbs the good order, peace or security of the facility, which provides an ill-defined and extremely broad authorisation for the use of force by IDSP officers. In contrast, analogous state and territory legislation governing the use of force in prisons generally limits the use of force to preventing or quelling a riot or disturbance.[7] The potential breadth of the circumstances in which the powers

6 EM, Attachment A, 20.

7 See, for example, r 121 of the Crimes (Administration of Sentences) Regulation 2008 (NSW).

may be used could, in practice, also reduce the effectiveness of other safeguards in the bill, such as the requirement in proposed paragraph 197BA(5)(b) that an authorised officer must not do anything likely to cause grievous bodily harm unless the officer reasonably believes doing the thing is necessary to protect the life of, or prevent serious injury to, another person (including the officer). The committee considers that this important safeguard could be less effective where force may be used in a broad range of circumstances in which the likelihood of grievous bodily harm is less foreseeable.

1.73 Second, the committee notes that the bill replaces the current test that reasonable force can only be used where it is objectively necessary,[8] with a test that incorporates a subjective element, being the officer's 'reasonable belief' that the use of force is necessary. The committee notes that a number of analogous state and territory laws governing the use of force in prisons do not enable force to be used based on the officer's belief, but apply objective tests such as that force may be used when it is 'reasonably necessary in the circumstances' or that the officer may 'where necessary, use reasonable force'.[9] To the extent that the move away from a purely objective test may impose a lower threshold for the use of force, the committee considers that the measure may also not be proportionate to the objective sought to be achieved.

1.74 Third, the committee notes that international human rights law requires that the state train relevant personnel to minimise the chance that a person's rights will be violated. The obligation here, therefore, is to ensure authorised officers are appropriately trained to minimise the chance that the use of force will result in loss of life.

1.75 In this respect, subsection 197BA(7) will require the minister to determine in writing the training and qualification requirements that an officer must satisfy in order to be authorised to use force. The statement of compatibility notes that IDSP officers are responsible for general security and safety of detainees and must hold a Certificate Level II in Security Operations or equivalent (or obtain this qualification within six months of commencing work). It is not clear to the committee that this level of training, which is the same as is required by crowd controllers and security guards, is sufficient to ensure that IDSP officers exercise the proposed use of force powers compatibly with the right to life.

1.76 More generally, the committee notes that immigration detention facilities are currently privately operated, with services provided under contract to the

8 See EM, Attachment A.

9 See, for example, r. 121 of the Crimes (Administration of Sentences) Regulation 2008 (NSW); ss 9CB and 23 of the *Corrections Act 1986* (Victoria); s 138(1) of the *Corrections Management Act 2007* (ACT); s. 86 of the *Correctional Services Act 1982* (SA); s 143 of the *Corrective Services Act 2006* (Qld).

Commonwealth. However, under international human rights law the State remains responsible in all circumstances for adherence to Australia's human rights obligations.[10] In this respect, the system of privately run detention centres provides less opportunity for state control to be exercised as a matter of practice. The conferral of use of force powers on employees of private detention centre operators therefore may not be sufficient to ensure that Australia effectively meets its international human rights obligations, to the extent that there may be inadequate oversight and control of private detention facilities by the Australian government.

1.77 The committee notes that further information on the matters set out above is required to properly assess whether the proposed use of force powers may be regarded as proportionate to their stated objective.

1.78 **The committee considers that the conferral of power on IDSP officers to use force in immigration detention facilities on the basis of their reasonable belief engages and limits the right to life. As set out above, the statement of compatibility has not, for the purposes of international human rights law, established that the measure is aimed at achieving a legitimate objective and, if so, whether it may be regarded as a proportionate means of achieving that objective. The committee therefore seeks the advice of the Minister for Immigration and Border Protection as to:**

- **whether there is reasoning or evidence that establishes that the stated objective addresses a pressing or substantial concern;**
- **whether there is a rational connection between the limitation and that objective; and**
- **whether the limitation is a reasonable and proportionate measure for the achievement of that objective.**

Prohibition against torture, cruel, inhuman or degrading treatment

1.79 Article 7 of the ICCPR and the Convention against Torture provide an absolute prohibition against torture, cruel, inhuman or degrading treatment or punishment. This means torture can never be justified under any circumstances. The aim of the prohibition is to protect the dignity of the person and relates not only to acts causing physical pain but also those that cause mental suffering. Prolonged solitary confinement, indefinite detention without charge, corporal punishment, and medical or scientific experiment without the free consent of the patient, have all been found to breach the prohibition on torture or cruel, inhuman or degrading treatment.

10 See, for example, the Human Rights Committee, Concluding Observations on the United Kingdom, 1995, CCPR/C/79/Add. 55 and Concluding Observations on New Zealand, 2010, CCPR/C/NZL/CO/5.

1.80 The prohibition contains a number of elements, including:

- it prohibits the state from subjecting a person to torture or cruel, inhuman or degrading practices, particularly in places of detention; and
- it requires an effective investigation into any allegations of such treatment and steps to prevent such treatment occurring.

Compatibility of the measure with the prohibition against torture, cruel, inhuman or degrading treatment

1.81 In assessing the bill as compatible with the prohibition against torture, cruel, inhuman or degrading treatment, the statement of compatibility states that the use of force provisions will not breach the prohibition because the bill specifically defines the circumstances in which reasonable force may be used, and the limits on its use:

> The use of force and circumstances under which it is authorised by the Bill would not amount to torture, cruel, inhuman or degrading treatment or punishment. The Bill only authorises force where it achieves a specific legislative outcome, that is, to protect the life, health or safety of any persons in an IDF and to maintain the good order, peace and security of an IDF.[11]
>
> Further, the intention is that use of force is to be consistent with the seriousness of the incident, proportional to the level of resistance offered by the persons involved and used only as a measure of last resort. The Bill prescribes limitations on the exercise of the power to use reasonable force, namely:
>
> - an authorised officer must not use force to give nourishment or fluids to a detainee in an IDF; and
> - an authorised officer must not subject a person to greater indignity than the authorised officer reasonably believes is necessary in the circumstances;
> - an authorised officer must not cause grievous bodily harm to an individual unless the authorised officer reasonably believes that doing so is necessary to protect the life of, or to prevent serious injury to, another person (including the authorised officer).

1.82 The committee notes that the prohibition against torture, cruel, inhuman or degrading treatment is an absolute obligation, which means that such treatment cannot be justified in any circumstance, regardless of the objective sought to be achieved.

1.83 The committee notes that proposed paragraph 197BA(5)(a) provides that in exercising the use of force power an authorised officer must not subject a person 'to greater indignity' than the officer reasonably believes is necessary. It appears then

11 EM, Attachment A, 21.

that an officer may therefore subject a person to a degree of indignity, dependent on the circumstances and the officer's reasonable belief.

1.84 As set out above at [1.69] to [1.76], the committee is concerned that the powers in the bill are not sufficiently circumscribed (that is, may not be proportionate), and that there is insufficient oversight of the powers to be exercised by IDSP officers in private detention facilities. Further, while the statement of compatibility notes the 'intention' that the use of force is to be used consistently with the seriousness of the incident, proportionate to the level of resistance and only as a measure of last resort, these safeguards are not placed on a statutory footing, and are likely to be insufficient as a safeguard against potential breaches of the prohibition against torture, cruel, inhuman or degrading treatment.

1.85 The committee is therefore concerned that the breadth of the proposed powers may lead to an officer taking action that may constitute degrading treatment for the purposes of international human rights law. This risk is compounded given that what amounts to degrading treatment depends on all the circumstances of the case (including the particular vulnerabilities of the victim), and that people detained in immigration detention in many cases may be particularly vulnerable (such as persons seeking asylum).

1.86 In addition, the committee is concerned that the bill makes inadequate provision for the monitoring and investigation of any instances or allegations of cruel, inhuman or degrading practices in detention.

1.87 With regard to the monitoring of the use of force in immigration detention facilities, the statement of compatibility states that the contract for the provision of detention services sets out governance mechanisms, including video-recording the event when there is a planned use of force and the provision of a written report. However, there is no legislated requirement for an independent review of the use of force. Rather, the bill provides that a complaint may be made to the Secretary of the department. This arrangement may be contrasted with arrangements for independent oversight such as in New South Wales and Western Australia where there is an independent inspectorate providing external scrutiny of the standards and operational practices of custodial services.[12]

1.88 The committee notes that the contract for the provision of detention services will also require the notification of the use of force for the purposes of the *Work Health and Safety Act 2011*,[13] relating to ensuring a safe workplace for the employees of an IDSP. However, there is no such requirement in relation to ensuring the safety of detainees.

---

12 See *Inspector of Custodial Services Act 2003* (WA) and *Inspector of Custodial Services Act 2012* (NSW).

13 See EM, Attachment A, 19.

1.89 In respect of these elements of monitoring and oversight, the committee considers that including safeguards in private contracts and policies do not constitute appropriate or sufficient safeguards for the purpose of international human rights law. Further, it is unclear to the committee that these proposed arrangements for monitoring the use of force provisions are sufficient to support the effective investigation of any allegations of torture or cruel, inhuman or degrading practices arising from their use.

1.90 In relation to the requirement to investigate credible allegations of degrading treatment, the statement of compatibility states that the bill provides for a statutory complaints mechanism, which, as noted above, will enable complaints to be made to the Secretary of the Department. The investigation of complaints will be at the discretion of the Secretary, who may decide not to investigate the complaint on a number of grounds, including the broad ground that the investigation 'is not justified in all the circumstances'. At the conclusion of the investigation the Secretary may refer the complaint to the Ombudsman, but does not have the power to grant any other remedies. The Ombudsman may make non-enforceable recommendations to government, which are not enforceable.[14]

1.91 The committee also notes that proposed section 197BF provides that no proceedings may be instituted or continued in any court against the Commonwealth in relation to the use of force if it was exercised in good faith. The definition of the Commonwealth includes an officer of the Commonwealth or any other person acting on behalf of the Commonwealth. This would exempt an authorised officer from both criminal and civil liability as long as they were acting in good faith in the use of force. The committee considers that this immunity, which, for example, could prevent the prosecution of an authorised officer accused of inflicting degrading treatment, may limit the obligation to investigate and prosecute alleged violations of the prohibition on degrading treatment.

1.92 **The committee considers that the use of force provisions in the bill as currently drafted are insufficiently circumscribed and risk empowering an authorised officer to use force against detainees in a way that may be incompatible with the prohibition on degrading treatment. The committee therefore seeks the advice of the Minister for Immigration and Border Protection as to whether the use of force provisions in the bill are sufficiently circumscribed to ensure that they are compatible with the prohibition on degrading treatment.**

1.93 **The committee considers that the basis for monitoring the use of force provisions and the bar on criminal proceedings in proposed section 197BF may limit the obligation to investigate and prosecute acts of torture, cruel, inhuman or degrading treatment. The committee therefore seeks the advice of the Minister for Immigration and Border Protection as to whether the arrangements for monitoring**

14 See *Ombudsman Act 1976*.

the use of force and the bar on proceedings in proposed section 197BF are compatible with the obligation to investigate and prosecute acts of torture, cruel, inhuman or degrading treatment.

Right to humane treatment in detention

1.94 The right to humane treatment in detention is protected by article 10 of the ICCPR. It provides that all people deprived of their liberty must be treated with humanity and dignity.

1.95 The right applies to everyone in any form of state detention, including prisons, immigration detention and forced hospital detention (including psychiatric wards). It also applies to private detention centres where it is administered under the law and authority of the state (for example, privately run prisons). The right provides extra protection for persons in detention who are particularly vulnerable as they have been deprived of their liberty.

1.96 The obligation on the state includes:

- a prohibition on subjecting a person in detention to inhumane treatment (including lengthy solitary confinement or unreasonable restrictions on contact with family and friends);
- monitoring and supervision of places of detention to ensure detainees are treated appropriately;
- instruction and training for officers with authority over people deprived of their liberty;
- complaint and review mechanisms for people deprived of their liberty; and
- adequate medical facilities and health care for people deprived of their liberty, particularly people with a disability and pregnant women.

Compatibility of the measure with the right to humane treatment in detention

1.97 The statement of compatibility acknowledges that the right to humane treatment in detention is engaged by the bill, to the extent that force is employed. In concluding that the bill is compatible with the right, it states:

> The implicit requirement of the Bill is that where reasonable force is required, the level of force applied must be no more than what is required to achieve the specific legislative outcome, be consistent with the seriousness of the matter, be proportionate to the level of resistance being offered by the person, be required to ensure the safety of officers, clients and third parties; and not be excessive. To the extent that these amendments may limit Article 10(1), the limitations are both reasonable and proportionate to achieving the legitimate objective to protect public order, safety or health, and the rights and freedoms of others.[15]

15 EM, Attachment A, 24.

1.98 However, as set out above at [1.62] to [1.67], the committee is of the view that the statement of compatibility does not provide a reasoned and evidence-based explanation of how the use of force provisions support a legitimate objective for the purposes of international human rights law.

1.99 As set out above at [1.69] to [1.76], it is unclear to the committee that the safeguards in the bill and the level of training for officers are adequate to ensure that force will only be used as a last resort.

1.100 As set out above at [1.86] to [1.89], the committee is also concerned that there may be inadequate monitoring of the use of force to ensure that detainees are treated appropriately and to support effective complaint and review mechanisms for any allegations of inhuman treatment.

1.101 On the basis of the reasoning set out above in relation to the right to life and the prohibition on torture, cruel, inhuman or degrading treatment, the committee considers that the bill may not be a proportionate limit on the right to humane treatment in detention.

1.102 **The committee considers that the use of force provisions limit the right to humane treatment in detention. As set out above, the statement of compatibility does not sufficiently justify that limitation for the purpose of international human rights law. The committee therefore seeks the advice of the Minister for Immigration and Border Protection as to:**

- **whether there is reasoning or evidence that establishes that the stated objective addresses a pressing or substantial concern or whether the proposed changes are otherwise aimed at achieving a legitimate objective;**
- **whether there is a rational connection between the limitation and that objective; and**
- **whether the limitation is a reasonable and proportionate measure for the achievement of that objective, and particularly, whether there are any less restrictive ways to achieve the objective, whether the training provided to authorised officers will be sufficient to minimise the risk of violation and whether there is adequate monitoring and supervision of the exercise of the use of force.**

Right to freedom of assembly

1.103 The right to freedom of assembly is protected by article 21 of the ICCPR. It provides that all people have the right to peaceful assembly. This is the right of people to gather as a group for a specific purpose. It is strongly linked to the right to freedom of expression, as it is a means for people together to express their views.

1.104 The right applies regardless of where people are assembling – it may be inside or outside, on public or private property, it may be a protest march or demonstration that moves from place to place or it may be stationary, such as sit-ins,

meetings or motionless protests. The right prevents the state from imposing unreasonable and disproportionate restrictions on assemblies.

1.105 The right only applies to peaceful protest and does not protect intentionally violent protests.

1.106 The right to freedom of assembly may be limited for certain prescribed purposes. Any limitation of the right must be necessary to respect the rights of others, to protect national security, public safety, public order, public health or morals. Additionally, such limitations must be prescribed by law, reasonable, necessary and proportionate to achieving the prescribed purpose.

Compatibility of the measure with the right to freedom of assembly

1.107 In concluding that the bill is compatible with the right to freedom of assembly, the statement of compatibility states that the proposed measures do not interfere with the right because the use of reasonable force falls within the permitted restrictions to article 21:

> The use of reasonable force in the circumstances outlined above clearly fall within the permitted restrictions to Article 21, in particular, to protect persons from an actual or perceived attack or harm, to prevent any threats to unlawful damage, destruction, or interference with Commonwealth property and protecting all persons from an actual or perceived attack or harm. The measures are defensive in nature and are predicated on any use of force being reasonable and proportionate to the threat and harm and for the purpose of protecting the rights of people and protection of property in an IDF.
>
> Therefore, reasonable force, or the authorised use of the powers under the Bill, would not breach the Article 21 obligations where they are imposed in conformity with the law for reasons of public order or the protection of the rights or freedoms of others.[16]

1.108 The committee notes that the use of force provisions would allow force to be used by an authorised officer when they reasonably believe it is necessary to maintain the good order of an immigration detention facility. However, what constitutes the 'good order' of the facility is not defined in the legislation. This could mean, for example, that an authorised officer could use force in relation to a peaceful protest if the authorised officer reasonably believes force is necessary to maintain good order. The committee notes that a peaceful protest within the facility may be considered by the detention centre operators to affect the 'good order' of the facility. Further, proposed subsection 197BA(2)(e) specifically provides that force may be used to move a detainee within the facility, which could include moving someone who is, for example, forming part of a peaceful 'sit-in'. There are no additional constraints on the exercise of the power for this purpose, such as a

16 EM, Attachment A, 24-25.

requirement that the person is unreasonably refusing to move or that the officer has first issued a lawful request for the person to move.

1.109 **The committee considers that the use of force provisions limit the right to freedom of association. As set out above, the statement of compatibility does not justify that limitation for the purpose of international human rights law. The committee therefore seeks the advice of the Minister for Immigration and Border Protection as to:**

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

Bar on proceedings relating to use of force

1.110 The bill also includes a provision that would impose a bar on proceedings relating to the use of force in immigration detention facilities. Proposed new section 197BF provides that no proceedings may be instituted or continued against the Commonwealth in relation to the use of force if the power was exercised in good faith. The 'Commonwealth' is defined as including any officer of the Commonwealth and any other person acting on behalf of the Commonwealth.

1.111 As set out above, the bill engages a number of human rights which include a concomitant obligation to ensure the right to an effective remedy for any violation of those rights. The bill, in imposing a bar on proceedings against the Commonwealth when an authorised officer uses force, therefore engages and limits the right to an effective remedy.

Right to an effective remedy

1.112 Article 2 of the ICCPR requires state parties to ensure access to an effective remedy for violations of human rights. State parties are required to establish appropriate judicial and administrative mechanisms for addressing claims of human rights violations under domestic law. Where public officials have committed violations of rights, state parties may not relieve perpetrators from personal responsibility through amnesties or legal immunities and indemnities.

1.113 State parties are required to make reparation to individuals whose rights have been violated. Reparation can involve restitution, rehabilitation and measures of satisfaction—such as public apologies, public memorials, guarantees of non-repetition and changes in relevant laws and practices—as well as bringing to justice the perpetrators of human rights violations.

1.114 Effective remedies should be appropriately adapted to take account of the special vulnerability of certain categories of persons including, and particularly, children.

Compatibility of the measure with the right to an effective remedy

1.115 The committee considers that imposing a bar on proceedings relating to the use of force in immigration detention facilities limits the right to an effective remedy. This is because, as set out above, the use of force provisions engage and limit a number of human rights, and, under article 2 of the ICCPR, a person is entitled to an effective remedy if their human rights are violated. The bar on proceedings for action occurring in immigration detention facilities therefore limits this right.

1.116 The committee notes that the UN Human Rights Committee has stated that the right to an effective remedy is an obligation inherent in the ICCPR as a whole and so, while limitations may be placed in particular circumstances on the nature of the remedy provided (judicial or otherwise), there is an absolute obligation to provide a remedy that is effective.[17] The UN Human Rights Committee has explained the nature of the obligation as follows:

> Without reparation to individuals whose Covenant rights have been violated, the obligation to provide an effective remedy, which is central to the efficacy of article 2, paragraph 3, is not discharged…[T]he Committee considers that the Covenant generally entails appropriate compensation. The Committee notes that, where appropriate, reparation can involve restitution, rehabilitation and measures of satisfaction, such as public apologies, public memorials, guarantees of non-repetition and changes in relevant laws and practices, as well as bringing to justice the perpetrators of human rights violations.[18]

1.117 While, as set out above, the bill provides for complaints to be made to the Secretary, the investigation of complaints will be at the discretion of the Secretary, who may decide not to investigate the complaint on a number of grounds, including the broad ground that the investigation 'is not justified in all the circumstances'. At the conclusion of the investigation the Secretary may refer the complaint to the Ombudsman, but does not have the power to grant any other remedies. The Ombudsman may make non-enforceable recommendations to government.

1.118 The committee does not consider that the complaint mechanism provided by the bill (when considered together with the bar on proceedings against the Commonwealth) meets the obligation to provide an effective remedy.

---

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

18 UN Human Rights Committee, *General Comment No. 31, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, (2004) [16].

1.119 The statement of compatibility provides no assessment of the compatibility of imposing a bar on proceedings relating to the use of force in immigration detention facilities with the right to an effective remedy.

1.120 It does, however, consider this provision in relation to all persons being treated equally before the courts and tribunals (article 14 of the ICCPR). In relation to that right, the statement of compatibility explained the purpose of the amendment:

> The purpose of the amendment … is to provide immunity from legal action to the Commonwealth (including an officer of the Commonwealth and any other person acting on behalf of the Commonwealth), except in the High Court under section 75 of the Constitution, in respect of the use of reasonable force in immigration detention facilities, provided the authorised officer did so in good faith.
>
> As authorised officers for the purposes of section 197BA, employees of the IDSP may be required to exercise police-like powers to protect the life, health or safety of people in the immigration detention facility and maintain the good order, peace and security of the facility. However, in so doing, they would not be afforded the same protection against criminal or civil action that police officers have.[19]

1.121 Barring proceedings against the Commonwealth as a whole in relation to the exercise of the use of force, unless not exercised in good faith, removes the opportunity for an affected person to seek compensation in a broad range of circumstances. The statement of compatibility states that authorised officers, in exercising the use of force, 'would not be afforded the same protection against criminal or civil action that police officers have'. However, the relevant state laws that give protection against liability for prison guards using force (in analogous situations) gives personal immunity to the officer but does not bar the bringing of proceedings more generally, including against government authorities.[20] It is unclear to the committee why it is necessary to bar proceedings against the Commonwealth as a whole if the intention of the provision is to provide personal immunity to the authorised officer.

1.122 **The committee therefore considers that the bar on proceedings relating to the use of force in immigration detention facilities limits the right to an effective remedy. As set out above, the statement of compatibility does not address the limitation on the right to an effective remedy. The committee therefore seeks the advice of the Minister for Immigration and Border Protection as to whether the measure is compatible with the right to an effective remedy. In particular, the committee wishes to understand why it is necessary to provide immunity for the**

19 EM, Attachment A, 25.

20 See, for example, s 263 of the *Crimes (Administration of Sentences) Act 1999* (NSW) or s 23 of the *Corrections Act 1986* (Vic).

Commonwealth as a whole rather than personal immunity for the authorised officer, and what remedies (including compensation) are available to a person whose complaint about the use of force is substantiated.

National Vocational Education and Training Regulator Amendment Bill 2015

Portfolio: Education and Training
Introduced: House of Representatives, 25 February 2015

Purpose

1.123 The National Vocational Education and Training Regulator Amendment Bill 2015 (the bill) seeks to amend the *National Vocational Education and Training Regulator Act 2011* (the Act) and the *National Vocational Education and Training Regulator (Transitional Provisions) Act 2011* to:

- extend registration periods from five to seven years;
- require any person advertising or representing a nationally recognised training course to clearly identify the provider responsible for the qualification in their marketing material;
- establish the capacity of the minister to make standards in relation to quality in vocational education and training sector;
- clarify the National Vocational Education and Training (VET) Regulator's (the regulator) ability to share information collected in the course of its operations; and
- make minor administrative amendments to clarify the Act and include transitional provisions.

1.124 Measures raising human rights concerns or issues are set out below.

Disclosure of information by the regulator

1.125 Part 4 of the bill seeks to amend the definition of 'VET information' to include all information and documents collected by the regulator in the course of exercising its functions or powers under the Act or in administering the Act.

1.126 The bill would also widen information disclosure provisions to allow the regulator to disclose VET information to a Commonwealth or state or territory authority if necessary to enable that authority to perform or exercise its functions or powers, or to a royal commission. The bill provides that if personal information is disclosed to a royal commission the regulator must advise the person whose information is disclosed of the details of the information disclosed.

1.127 The committee considers that the disclosure of personal information engages and limits the right to privacy.

Right to privacy

1.128 Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary or unlawful interferences with an individual's privacy, family, correspondence or home. The right to privacy includes respect for informational privacy, including:

- the right to respect for private and confidential information, particularly the storing, use and sharing of such information; and
- the right to control the dissemination of information about one's private life.

1.129 However, this right may be subject to permissible limitations which are provided by law and are not arbitrary. In order for limitations not to be arbitrary, they must seek to achieve a legitimate objective and be reasonable, necessary and proportionate to achieving that objective

Compatibility of the measure with the right to privacy

1.130 The statement of compatibility acknowledges that the bill engages the right to privacy by enabling the regulator to disclose information, but explains:

> It is necessary to amend the provision so that the Regulator can share VET information beyond [the Tertiary Education Quality and Standards Agency]. This will improve the Regulator's ability to cooperate with other government entities, such as the Australian Competition and Consumer Commission, in removing dishonest providers from the VET sector. New Section 205A contains an additional safeguard – namely that when the Regulator discloses VET information that is personal information to a Royal Commission, it must provide details to the person concerned.[1]

1.131 The committee notes that the definition of 'VET information' is very broad and captures all information and documents collected by the regulator in the performance of its functions. Under the Act the regulator's functions include, in addition to registering and accrediting courses and organisations, the issuing of VET qualifications to students.[2] The Act also provides that VET student records are to be provided to the regulator.[3] This includes a document or object that has been kept because of its connection to a current or former VET student.[4]

1.132 The committee notes that the information able to be disclosed by the regulator could apparently include information about students, including personal

1 Explanatory memorandum (EM) 4-5.

2 Section 55 of the *National Vocational Education and Training Regulator Act 2011.*

3 Section 211 of the *National Vocational Education and Training Regulator Act 2011.*

4 See definition of 'VET student records' in section 3 of the *National Vocational Education and Training Regulator Act 2011.*

information, and as such the committee considers that the bill limits the right to privacy.

1.133 The statement of compatibility states that it is necessary to allow for broader disclosure of VET information to improve the regulator's ability to cooperate with other government entities to remove dishonest providers from the VET sector.

1.134 While the committee notes that improving the ability of the regulator to cooperate with other government entities to remove dishonest providers is likely to be a legitimate objective for the purposes of international human rights law, it is unclear, on the basis of the information provided in the statement of compatibility, whether the measure may be regarded as proportionate to this objective.

1.135 In particular, the statement of compatibility lists only one safeguard in the legislation—namely, that if personal information is disclosed to a royal commission the regulator must advise the affected person that the information has been disclosed and give details of the information disclosed. However, this requirement does not apply when personal information is disclosed to a Commonwealth, state or territory authority.

1.136 The committee notes that the definition of a Commonwealth or state or territory authority in the Act includes any Commonwealth department, the state or territory (as a whole) or a body established under law. This is extremely broad, and could include hundreds of bodies or entities. While the statement of compatibility states that these amendments would improve the regulator's ability to cooperate with other government entities, such as the Australian Competition Consumer Commissioner, it does not explain why it is necessary in this case to enable disclosure to all Commonwealth, state or territory authorities, rather than to a specified list of relevant authorities.

1.137 In addition, the statement of compatibility does not describe the specific types of personal information that might be disclosed under the bill. As noted above, the information to be disclosed could apparently include information about former or current VET students, and it is unclear to the committee whether this information could contain, for example, records of the student's results or allegations of academic misconduct made against the student, such as plagiarism.

1.138 In order to complete its assessment of the compatibility of the measure with the right to privacy, the committee therefore requires further information on the specific types of personal information subject to the disclosure scheme, and why it is regarded as proportionate to enable the disclosure of information to any Commonwealth, state or territory authority.

1.139 **The committee considers that disclosure of VET information limits the right to privacy. As set out above, the statement of compatibility for the bill does not provide sufficient information to establish that the breadth of the measure may be regarded as proportionate to its stated objective of improving the regulator's ability to cooperate with other government entities to remove dishonest VET**

providers. The committee therefore seeks the advice of the Minister for Education and Training as to whether the limitation on the right to privacy imposed by the breadth of the measure is proportionate to the measure's stated objective.

Seafarers Rehabilitation and Compensation and Other Legislation Amendment Bill 2015

Portfolio: Employment
Introduced: House of Representatives, 26 February 2015

Purpose

1.140 The Seafarers Rehabilitation and Compensation and Other Legislation Amendment Bill 2015 (the bill) seeks to amend the *Seafarers Rehabilitation and Compensation Act 1992* (the Seafarers Act) and the *Occupational Health and Safety (Maritime Industry) Act 1993* (the OHS(MI) Act) to clarify coverage of those Acts.

1.141 Currently, the Seafarers Act provides workers compensation and rehabilitation arrangements for seafarers in a defined part of the Australian maritime industry. The OHS(MI) Act regulates work, health and safety for a defined part of the maritime industry. Together, these Acts are referred to as the 'Seacare scheme'.

1.142 The proposed amendments would:

- repeal provisions that apply the Seacare scheme to any employees employed by a trading, financial or foreign corporation;
- provide that the Seacare scheme applies to the employment of employees on a prescribed ship that is 'directly and substantially' engaged in interstate or international trade or commerce; and
- make technical amendments to ensure that, where an employee's employment is not covered by the Seacare scheme, their employer will not be liable for a levy in respect of that employee.

1.143 Measures raising human rights concerns or issues are set out below.

Alteration of coverage of persons eligible for workers' compensation

1.144 The bill would amend the existing legislation to ensure that workers on ships engaged in intra-state voyages are not covered by the Seacare scheme. This would result in such workers no longer having an entitlement to compensation under the Seafarers Act. Instead, such workers would be covered by the relevant workers' compensation and work health and safety legislation of the state in which they work.

1.145 The committee considers that amending the Seacare scheme to remove an entitlement to compensation engages and may limit the right to social security.

Right to social security

1.146 The right to social security is protected by article 9 of the International Covenant on Economic, Social and Cultural Rights (ICESCR). This right recognises the importance of adequate social benefits in reducing the effects of poverty and plays an important role in realising many other economic, social and cultural rights, particularly the right to an adequate standard of living and the right to health.

1.147 Specific situations and statuses which are recognised as engaging a person's right to social security, include health care and sickness; old age; unemployment and workplace injury; family and child support; paid maternity leave; and disability support. It also includes the protection of workers injured in the course of employment.

Compatibility of the measure with the right to social security

1.148 The statement of compatibility explains that the bill has been introduced as a result of the Full Court of the Federal Court's decision in *Samson Maritime Pty Ltd v Aucote* [2014] FCAFC 182 (the *Aucote* decision). The *Aucote* decision held that the coverage provisions in the Seafarers Act apply to all seafarers employed by a trading, financial or foreign corporation, including ships engaged in purely intra-state trade. However, prior to the *Aucote* decision, it had been understood by regulators, maritime industry employers and maritime unions that the Seacare scheme did not apply to ships engaged in purely intra-state trade.[1]

1.149 The statement of compatibility states that the bill is intended to align the coverage of the Seafarers Act with the understanding of the scheme prior to the *Aucote* decision, and that as a consequence some workers will no longer have an entitlement to compensation under the Seafarers Act. While this is acknowledged to be a potential limitation of the right to social security, the statement of compatibility assesses the measure as compatible with the right as follows:

> Any such limitations are, however, reasonable and proportionate, as affected employees will retain entitlements to compensation and any limitations are necessary to achieve the legitimate objective of ensuring the long-term viability of maritime industry employers and sustainability of the Seacare scheme.
>
> …these employees will continue to be covered by the workers' compensation legislation of the state in which they work — as they had been understood to be, prior to the *Aucote* decision. While the precise quantum of entitlements available under each scheme varies, every workers' compensation scheme in Australia provides protection and support to injured employees, as required by the right to social security. Further, the change to the rights of these employees to workers' compensation will align their actual rights with those which they had been understood to have had prior to the Aucote decision. As such, any limitation to the right to social security which results from this change would be reasonable and proportionate.[2]

1.150 The committee notes that, to the extent that the state schemes are less generous than the Seacare scheme the measure may be regarded as a retrogressive

1 Explanatory memorandum (EM) v-vi.

2 EM, vii.

measure. Under article 2(1) of the ICESCR, Australia has certain obligations in relation to economic and social rights. These include an obligation not to unjustifiably take any backwards steps (retrogressive measures) that might affect the right to social security. A reduction in compensation available to an injured worker may be a retrogressive measure for human rights purposes. A retrogressive measure is any measure that directly or indirectly leads to a backwards step being taken in the level of rights protection. A retrogressive measure is not prohibited so long as it can be demonstrated that the measure is justified. That is, it addresses a legitimate objective, it is rationally connected to that objective and it is a proportionate means of achieving that objective.

1.151 While the committee notes that ensuring the long-term viability of maritime industry employers and sustainability of the Seacare scheme is likely to be a legitimate objective for the purposes of international human rights law, it is unclear, on the basis of the information provided in the statement of compatibility, whether the measure may be regarded as proportionate to this objective.

1.152 The statement of compatibility characterises the measure as proportionate on the basis that 'affected employees will retain entitlements to compensation',[3] noting that every workers' compensation scheme does provide protection and support to injured employees as required by the right to social security.[4] However, the statement of compatibility also states that workers' compensation premiums under the Seacare scheme are, on average, significantly more expensive than those of the state and territory schemes, which could suggest that those schemes provide for lesser coverage or entitlements. Given this, the committee considers that specific information on the extent of any differences in levels of coverage and compensation between the Seacare scheme and the state and territory schemes is needed to fully assess the proportionality of the measure.

1.153 **The committee considers that the amendment to exclude workers on ships engaged in intra-state voyages engages and may limit the right to social security and may be regarded as a retrogressive measure under international human rights law. As set out above, the statement of compatibility for the bill does not provide sufficient information to establish that the measure may be regarded as proportionate to its stated objective. The committee therefore seeks the advice of the Minister for Employment as to the extent of differences in levels of coverage and compensation between the Seacare scheme and state and territory workers' compensation schemes.**

3 EM, vii.

4 EM, vii.

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Portfolio: Attorney-General
Introduced: House of Representatives, 30 October 2014

Purpose

1.154 The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the bill) would amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to introduce a mandatory data retention scheme. This scheme would require service providers to retain types of telecommunications data under the TIA Act for two years. The bill will also provide that:

- mandatory data retention would only apply to telecommunications data (not content);
- mandatory data retention would be reviewed by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) three years after its commencement;
- the Commonwealth Ombudsman would have oversight of the mandatory data retention scheme and, more broadly, the exercise by law enforcement agencies of powers under chapters 3 and 4 of the TIA Act; and
- the number of agencies which would be able to access the data would be confined.

1.155 Measures raising human rights concerns or issues are set out below.

Background

1.156 The TIA Act has not previously been subject to an assessment of human rights compatibility as it was introduced prior to the inception of the committee. However, the aims of the proposed amendments to the TIA Act should be understood in terms of the key objective of the TIA Act, which is:

- to protect the privacy of telecommunications by criminalising the interception or accessing of communications; and
- to provide a framework to enable law enforcement and national security agencies to apply for warrants to intercept communications when investigating serious crimes and threats to national security in prescribed circumstances.[1]

1 Australian Attorney-General's Department, *Submission 26*, Inquiry into the comprehensive revision of the *Telecommunications (Interception and Access) Act 1979,* Senate Legal and Constitutional Affairs References Committee, 4 http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act/Submissions (accessed 10 November 2014).

1.157 Under the TIA Act, access to communications (content) requires a warrant while access to telecommunications data (metadata) does not. However, technology has significantly developed since the TIA Act was enacted with the development of new forms of communications technologies and, consequently, new forms of metadata. In this respect, the committee notes that the assessment of this bill brings into sharper focus potential inadequacies of the TIA Act in terms of specific safeguards around access to telecommunications data and content.

1.158 The committee first commented on the bill in its *Fifteenth Report of the 44th Parliament*.[2] The committee noted that metadata can reveal quite personal information about an individual, even without the content of the data being made available, by revealing who a person is in contact with, how often and where. This in turn could reveal, for example, the person's political opinions, sexual habits, religion or medical concerns. The committee was therefore of the view that the proposed mandatory data retention scheme engages and limits the right to privacy.

1.159 A limitation on the right to privacy will be permissible under international human rights law where it addresses a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective. The committee considered that the statement of compatibility had generally established why particular categories of data are considered necessary for law enforcement agencies. That is, the committee considered that the proposed scheme pursued a legitimate objective.

1.160 However, the committee noted that a mandatory data retention scheme with a requirement to collect and retain data on every customer is very intrusive of privacy, and accordingly focused its analysis on the question proportionality.

1.161 The committee considered that the scheme must be sufficiently circumscribed to ensure that limitations on the right to privacy are proportionate (that is, are only as extensive as is strictly necessary). The committee requested further information from the Attorney-General in relation to the proportionality of the mandatory data retention scheme, including making specific recommendations as to the scope of the data set to be retained, the two year retention period, access to information and oversight and accountability).

1.162 The committee considered that the scheme also engaged the right to freedom of opinion and expression and the right to an effective remedy, and requested further information from the Attorney-General in relation to these rights.

2 Parliamentary Joint Committee on Human Rights, *Fifteenth Report of the 44th Parliament* (14 November 2014) 10-22.

Committee view on compatibility

Attorney-General's response

Thank you for the 15th report of the Parliamentary Joint Committee on Human Rights to the 44th Parliament, in which the Committee requested further advice in relation to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. I greatly appreciate your Committee's interest in the Bill and support for the Government's objective to increase both public safety and the ability for victims of crime to have recourse to justice.

I have attached detailed responses to the Committee's suggestions. In short, the Government firmly believes that the Bill represents a reasonable, necessary and proportionate limitation on the right to privacy for the protection of national security, public safety and for addressing crime. These measures are critical to protecting the right to life, security of the person and public confidence in communications technology. The scheme will not undermine legal professional privilege in any way.

The Government believes that a two year retention period is appropriate, particularly given the long term nature of many national security and complex criminal investigations and the fact that many victims of crimes, such as sexual assault, do not immediately report their allegations. In this regard, I note that the security and law enforcement agencies have expressed a strong preference for a longer retention period.

In addition, requiring criminal law enforcement agencies to obtain a warrant for every metadata request, or allowing an individual to challenge access to their metadata would be impractical and frustrate law enforcement efforts. Such access restrictions would only serve to adversely affect victims of crime, the very people governments and our law enforcement and security agencies are entrusted to protect. Further, limiting metadata access to investigation of serious crimes, or its use to the purpose for which it was obtained, would be inconsistent with our international obligations, including under the Convention on Cybercrime.

The Government has published the data set proposed to be prescribed by regulation, and has referred the proposed data set to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) alongside the Bill. The Government has also worked with industry through a joint Government-industry working group on possible refinements to the data set, and provided a report to the PJCIS to assist its consideration. The Government looks forward to receiving the PJCIS report, which is due to be tabled on 27 February 2015.

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) supplements oversight mechanisms which

are already in place to ensure privacy and human rights are protected. Existing safeguards will be maintained under the mandatory data retention scheme. For instance, the Privacy Commissioner will continue to assess industry's compliance with the Australian Privacy Principles, and monitor its non-disclosure obligations under the Telecommunications Act. The Inspector General of Intelligence and Security currently inspects and reports on ASIO's access to data.

The Bill protects privacy and human rights by limiting the range of agencies permitted to access telecommunications data and introducing several new oversight mechanisms. They include:

- Agencies to maintain comprehensive records relating to their access, use and disclosure of stored communications and telecommunications data;
- The Commonwealth Ombudsman to inspect access to, and the use of, telecommunications data by Commonwealth, State and Territory enforcement agencies to ensure their compliance with the TIA Act;
- The Attorney-General's Department to include information on the operation of the scheme in its annual report to Parliament.
- The Parliamentary Joint Committee on Intelligence and Security will review the operation of the data retention scheme after 3 years of the scheme's full implementation.

These safeguards are consistent with the bipartisan recommendations from the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*.

Proportionality of collecting metadata

The Committee has expressed a view that the proposed data retention arrangements are intrusive of privacy and that this raises an issue of proportionality.

The Australian Government believes that requiring telecommunications providers to retain a limited subset of telecommunications data about all customers is a proportionate response to the threat posed by terrorism, and serious and other crimes such as sexual assault and paedophilia. Case-by-case access to telecommunications data provides the foundational information critical to investigations with the minimum possible intrusion on privacy that is practicable.

Telecommunications data is critical to the investigation of almost any criminal activity, serious or otherwise, where that activity that has been facilitated, enabled or carried out via communications technology. It is essential for investigations into criminal activities and activities prejudicial to security that are conducted exclusively online, such as hacking and cyber-espionage, and activities with a physical manifestation that are further enabled by the internet, such as identity theft and child

exploitation. Where an investigation involves an internet-based communication, metadata is often the only investigative lead as such communications leave no physical evidence.

Access to metadata is often the least-privacy intrusive tool available to agencies to undertake the foundational steps in an investigation. It can help build a picture of a how a suspect communicates with criminal associates. Importantly, from a privacy perspective, it allows investigators to identify suspects and exclude others from suspicion and therefore from further, more intrusive, investigation techniques such as telecommunications interception or search warrants. The use of physical surveillance or a surveillance device to identify with · whom a suspect has been communicating can result in the collection of the content of communications involving that person, as well as the content of conversations occurring in their vicinity.

The Bill has been drafted to protect individual privacy and human rights while ensuring that data retention remains of practical utility for national security and law enforcement purposes. The Bill entirely excludes a large number of communications services where the privacy or compliance impact would be disproportionate to the investigative benefit. Additionally, the Bill entirely excludes telecommunications data relating to a person's web-browsing from the scope of data retention obligations and significantly limits the volume and detail of location records that are required to be kept.

The *Telecommunications (Interception and Access) Act 1979* and the *Australian Security and Intelligence Organisation Act 1979* strictly control the circumstances in which agencies may access, use and disclose telecommunications data and impose criminal penalties for the misuse of such information. This will not change. Additionally, the Bill significantly limits the range of agencies permitted to access telecommunications data and introduces comprehensive independent oversight of all aspects of the access to, and use and disclosure of, telecommunications data by enforcement agencies.

Any privacy implications associated with the increased volume of data which may be generated by the new requirements are mitigated by the obligations imposed by the *Privacy Act 1988*.

The Australian Privacy Principles apply to personal information held by regulated entities. Service providers covered by the Privacy Act must ensure the quality and/or correctness of any personal information and keep personal information secure. The Act imposes obligations regarding the destruction of personal information. The Act also requires regulated service providers to put in place risk-based safeguards against unauthorised access to and misuse of personal information held by industry. The Privacy Commissioner will continue to have oversight of carriers' collection and retention of personal information for regulated service providers.

To the extent that some providers would not be required to comply with the Australian Privacy Principles, retained data would be subject to the same security standards as other data on a service providers' network, including the application of technical and organisational measures to ensure confidentiality, integrity and availability, so that the retained data can only be accessed by authorised personnel. Service providers which are non-APP entities are also subject to data protection obligations under the *Telecommunications Act 1997*.

There are other important safeguards and oversight mechanisms in place. Telecommunications data is protected information. The Telecommunications Act makes it an offence for a service provider and its employees to disclose metadata without consent. Similarly, it is a criminal offence for a police officer or official to use or disclose telecommunications data that has been obtained by their agency, except for one of the limited purposes set out in the Act. ASIO's access to, and use and disclosure of, metadata is subject to oversight by the Inspector-General of Intelligence and Security. Further, the activities of Federal law enforcement agencies, for example, are subject to Ministerial oversight, scrutiny during Senate Estimates hearings and Parliamentary Committee inquiries and investigations by the Australian Commission for Law Enforcement Integrity. In addition, statistical information on requests for data by law enforcement from telecommunications service providers are reported on annually by the Attorney-General.

The extensive oversight regime contained in the Bill will also empower the Commonwealth Ombudsman to assess agency compliance with their obligations under the *Telecommunications (Interception and Access) Act 1979*. The regime supports effective oversight of agencies by providing precise compliance obligations and more consistent reporting on access to telecommunications data.

The Bill also includes a mechanism for the Communications Access Coordinator to grant an exemption to a service provider from some or all of the mandatory data retention obligations. This exemption mechanism indirectly strengthens the right to privacy by providing a means of reducing data retention obligations, such as where the volume of data to be retained is disproportionate to the interests of law enforcement and national security in that data.

Legislating for mandatory data retention is a necessity. Australia's law enforcement and national security agencies are facing several challenges which have increased their need to reliably access telecommunications data. There has been a long-term decline, and significant industry inconsistency, in the retention of relevant telecommunications data. Without legislative obligations, the Government does not have the ability to address changes in retention practices that significantly degrade agencies' investigative capabilities.

> There are no practical alternatives to a data retention scheme that would provide the information agencies need. International counterparts have considered the expansion of existing 'quick freeze' preservation notices to cover non-content data as an alternative to data retention. Unfortunately, service providers cannot preserve information that no longer exists. The purpose of data retention is to introduce a consistent industry standard to ensure that certain limited types of telecommunications data are consistently available.
>
> If the relevant metadata has not been retained, a range of crimes will go unsolved. For example, in a current major child exploitation investigation, the Australian Federal Police (AFP) has been unable to identify 156 out of 463 potential suspects, because certain providers do not retain the necessary Internet Protocol (IP) address allocation records. These records are essential to link criminal activity online back to a real-world person.
>
> For these reasons, the Government believes that a mandatory data retention regime applying to all customers is reasonable, necessary and proportionate.[3]

Committee response

1.163 **The committee thanks the Attorney-General for this further information.**

1.164 The committee notes that generally even measures which impose quite substantial intrusions or limitations on human rights (such as the right to privacy) may be permissible under international human rights law where they are necessary in pursuit of a legitimate objective, and are rationally connected to and a proportionate means of achieving that objective.[4]

1.165 The committee notes that a range of evidence has been provided as to why particular categories of data are necessary for law enforcement agencies. On this basis, the committee remains of the view that the Attorney-General has generally established that the proposed scheme addresses a pressing and substantial concern such as may be regarded as a legitimate objective under international human rights law. The committee acknowledges the fundamental and legitimate interests of government in ensuring that there are adequate tools for law enforcement agencies to ensure 'public safety and the ability for victims of crime to have recourse to justice'.[5]

---

3 See, Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 1-5.

4 Most human rights can be permissibly limited providing that limitation is justifiable. Rights that are absolute and cannot be justifiability limited include the prohibition on torture and the obligation of non-refoulement.

5 See, Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 1-5.

1.166 As noted above, the particular concern of the committee has been that the proposed data retention scheme must be sufficiently circumscribed to ensure that any limitations it imposes on human rights are proportionate (that is, are only as extensive as is strictly necessary). Accordingly, each of the committee's specific requests for advice from the Attorney-General and recommendations were aimed at determining or ensuring that the scheme was sufficiently circumscribed so as to be proportionate.

1.167 The Attorney-General's responses to the committee's specific requests and recommendations going to the proportionality of the scheme are addressed below.

Mandatory data retention scheme—scope of data set to be retained

Definition of data to be retained - right to privacy

1.168 Under the scheme as proposed in the bill, categories of data to be collected and retained by service providers are not specified, but would be set out in regulations at a later date.

1.169 The committee recommended that, to avoid the arbitrary interference with the right to privacy that would result from reliance on regulations, the bill be amended to define the types of data that are to be retained.

1.170 In the event that the bill were not amended, the committee recommended that the government release for consultation an exposure draft of the regulation specifying the types of data to be retained for the purposes of the scheme.

Attorney-General's response

> The Committee has expressed concern that the types of data to be retained will be specified by a regulation made pursuant to proposed section 187A(l)(a) in the Bill. The Government believes the combination of primary and delegated legislation is appropriate in this context. However, I acknowledge that several submitters to the current PJCIS inquiry have raised this issue and that the PJCIS is giving further consideration to both the data set and the mechanism through which it should be prescribed. I look forward to that Committee's views and will give further consideration to the range of views expressed in this regard.[6]

Committee response

1.171 **The committee thanks the Attorney-General for his response.**

1.172 The committee considers that the scope of the dataset to be retained is an important issue in relation to whether the scheme is proportionate to its stated legitimate objective. As noted previously, the categories of data identified in the statement of compatibility as likely to be included in any regulation may provide

6 See, Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 5.

significant identifying details about an individual and will, accordingly, limit the right to privacy. As noted in a recent decision of the European Court of Justice:

> …[metadata when]…taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[7]

1.173 The committee notes that, given such privacy implications, if the scope of the prescribed data to be collected goes beyond what is required to achieve the stated legitimate objective of the scheme, then the scheme will not be proportionate. The committee is concerned that, if the types of data to be collected remain unspecified until the relevant regulation is made, it is impossible to say that the dataset is sufficiently circumscribed such that it may be regarded as a permissible limitation under human rights law. There is therefore a serious risk that the scope of the dataset in subsequent regulations may be broader than what is required to achieve the stated objective (that is, that the scope of the dataset may be disproportionate). The committee notes that in order for a measure to be a proportionate limitation on the right to privacy it must be the least rights intrusive option available.

1.174 The committee notes that the Parliamentary Joint Committee on Intelligence and Security (PJCIS) has similarly recommended that the bill be amended to include the dataset in primary legislation and, further, that some types of data be expressly excluded from retention requirements. The committee notes that the Attorney-General has responded to this recommendation by the PJCIS and indicated the government will amend the bill to include the proposed dataset.[8]

1.175 **The committee welcomes the Attorney-General's commitment to give further consideration to the scope of the dataset to be retained and to prescribing the retained dataset in primary as opposed to delegated legislation. As set out above, unless the scope of the dataset to be retained is sufficiently circumscribed, there is a serious risk that the scheme will not be proportionate to its stated legitimate objective of ensuring public safety and the ability for victims of crime to have recourse to justice. If the scope of the data set to be retained is not proportionate, it will be incompatible with the right to privacy. The committee therefore reiterates its previous recommendations that:**

---

7 See *Digital Rights Ireland Ltd (C-293/12) and Kärntner Landesregierung ors (C-594/12), v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014) [27].

8 See Government Response to Committee report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (3 March 2015).

- **to avoid the arbitrary interference with the right to privacy that would result from reliance on regulations, the bill be amended to define the types of data that are to be retained; and**
- **if the bill is not amended, the government release for consultation an exposure draft of the regulation specifying the types of data to be retained for the purposes of the scheme.**

1.176 **The committee notes that the Parliamentary Joint Committee on Intelligence and Security has similarly recommended that the bill be amended to include the dataset in primary legislation and, further, that some types of data be expressly excluded from retention requirements.**

Definition of content—right to privacy

1.177 The proposed scheme provides that 'content' is to be excluded from collection. However, what constitutes content is not defined by the bill. The committee recommended that, to avoid the arbitrary interference with the right to privacy that would result from not defining the content that is excluded from required retention, the bill be amended to include an exclusive definition of 'content' for the purposes of the scheme.

Attorney-General's response

> The Committee has recommended that the Bill be amended to provide a clear definition of 'content' in the primary legislation.
>
> This recommendation would likely result in the opposite of the Committee's desired effect. The Australian Law Reform Commission effectively recognised this risk in its report on Australian Privacy Law and Practice (ALRC Report 108). The report concluded that the *Telecommunications (Interception and Access) Act 1979* (TIA Act) should not exhaustively define what constitutes telecommunications data, in order to allow it to continue to apply in the face of rapid technological change within the telecommunications industry. The merits of technological neutrality in the context of data are equally applicable to defining content. The broad definition in the TIA Act is capable of being interpreted in light of rapid changes in communications technology in a way that an exhaustive, static definition would not.
>
> If the legislation were to include an exhaustive list of that which comprises 'content', it would likely result in the legislation failing to keep pace with rapid changes in the technology offered by the telecommunications industry. Any new types of information that emerge as a result of rapid technological change would fall outside the defined list and would be excluded from the meaning of content.
>
> The TIA Act includes provisions which, when read in conjunction with a broad definition of content, create a strong incentive for telecommunications industry and agencies to take a conservative approach to accessing content. In particular:

- any person who believes that the content or substance of their communications has been unlawfully accessed under a data authorisation can challenge that access and, if successful, to seek remedies under Part 3-7 of the TIA Act
- except for limited exceptions, it is a criminal offence for a service provider to disclose the content or substance of a communication without lawful authority, and
- it is a criminal offence for officials of law enforcement and national security agencies to use or disclose unlawfully accessed stored communications except in strictly limited circumstances.

The TIA Act will continue to maintain a general and effective prohibition on the interception of, and other access to, telecommunications content except in limited circumstances.[9]

Committee response

1.178 **The committee thanks the Attorney-General for his response.**

1.179 The committee acknowledges the desirability of having a definition of 'content' (which would therefore be excluded from collection) that is capable of keeping pace with technological changes. However, without a clear definition of 'content' there is the potential that what constitutes 'content' could be interpreted restrictively so that the scope of data to be retained is broader than what is required to achieve the stated objective (that is, that the scope of the dataset may be disproportionate).

1.180 As noted previously, the bill could potentially see data retained that does include aspects of content. For instance, meta-tags are used by website developers to provide search engines with information about their sites, and may contain significant information about a website including aspects of its content. However, it is unclear whether it is intended that meta-tags will be prescribed in the regulations as data to be retained for the purposes of the scheme.

1.181 The committee was particularly concerned about this in a context where categories of data to be collected and retained by service providers are not specified in the proposed legislation, but would be set out in regulations at a later date. Based on the information provided, the committee considers that an exclusive definition of 'content' may not be required if the bill is amended to prescribe the scope of the dataset to be retained.

1.182 The committee further notes that a clear definition of the type of data that would constitute 'content' for the purposes of the scheme could still be capable of keeping pace with technological changes. For example, a non-exclusive definition of

9 See, Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 6.

content could set out examples of types of data that do constitute content and thereby prescribe a minimum level of privacy protection while keeping pace with technological changes. Such a definition could assist in ensuring the proposed scheme is sufficiently circumscribed so as to be proportionate to its stated legitimate objective.

1.183 **The committee considers that an exclusive definition of 'content' may not be required if the bill is amended to prescribe the scope of the dataset to be retained in accordance with its above recommendation. However, the committee recommends that, to avoid the arbitrary interference with the right to privacy that would result from not defining the content that is excluded from required retention, the bill be amended to include a non-exclusive definition of what type of data would constitute 'content' for the purposes of the scheme.**

Mandatory data retention scheme—two year retention period

Right to privacy

1.184 As noted at [1.153] above, Schedule 1 of the bill would require data retention for a period of two years. The committee requested the further advice of the Attorney-General as to whether the two year retention period is necessary and proportionate in pursuit of a legitimate objective.

Attorney-General's response

> The Government believes a two year retention period is reasonable, necessary and proportionate, and is supported by international evidence and the domestic experience of law enforcement and national security agencies.
>
> Criminal investigations are often complex. Agencies are generally trying to solve crimes that have already happened, or are attempting to investigate crimes that are in progress. Valuable information and evidence is constantly at risk of being lost with the passage of time. For telecommunications data, there is an additional risk that business practices will destroy valuable evidence.
>
> A consistent, two-year retention period is necessary to ensure that critical information is available, particularly for complex and serious law enforcement, national security and anti-corruption investigations, and is based on both the advice of Australian agencies and the findings of international reviews of data retention laws.
>
> Telecommunications data is often used at the early stages of investigations to build a picture of a suspect and their network of associates. Agencies begin their investigations several steps behind perpetrators. The ability to reconstruct events leading up to and surrounding a crime allows agencies to rapidly determine the size and scope of an investigation. Alternative methods, such as physical surveillance, cannot provide essential historical information required in criminal investigations.

Each of the foundational steps in an investigation takes time and delays outside of the control of law enforcement and security agencies are commonly experienced. There may be delays in the matter being brought to the attention of the relevant agency, either by the victim or by another authority that has been conducting a separate investigation. A witness or victim may only come forward after an extended period of time. Alleged offenders may be unwilling to cooperate. Investigators may take time to identify a key piece of evidence. Expert analysis and input may be required, resulting in the investigation being effectively placed on hold for a period of time. Investigative resources can be temporarily diverted to higher priority matters. Consequently, security and law enforcement agencies may not identify the need to access metadata relating to a specific person, service, device or account for an extended period after the commencement of an investigation or after a relevant incident.

More broadly, many crimes are not brought to the attention of the relevant authorities until well after the fact, and the normal variability in criminal investigations means that some investigations will continue for considerably longer than average. In such cases, reliable access to telecommunications data can be particularly important, as physical and forensic evidence will frequently degrade with the passage of time.

In 2011, the European Commission conducted a review of the European Union Data Retention Directive. This review was conducted five years after the Directive came into force. The table below shows the breakdown of requests for telecommunications data made by law enforcement agencies under the Directive by age in countries that implemented a two year retention period over the five year period considered by the review.

Age of telecommunications data requested (months)								
	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24
Percentage of requests	57.81%	19.59%	8.03%	5.03%	2.80%	2.00%	1.51%	3.24%
Cumulative percentage of requests	57.81%	77.40%	85.43%	90.46%	93.25%	95.25%	96.76%	100.00%

Summary of age of telecommunications data requested under the EU Data Retention Directive in countries with two-year data retention periods, 2008-12

Commonwealth law enforcement agencies have advised that their usage of telecommunications data closely matches the above profile.

While the review found that approximately 90 per cent of requests for access relate to telecommunications data less than twelve months old, this number is skewed heavily by the use of telecommunications data in more straight-forward 'volume crime' investigations that, despite being serious in nature, can frequently be resolved in a shorter period of time.

The above summary obscures the fact that certain types of law enforcement investigations frequently involve longer investigatory periods

and therefore require a disproportionate level of access to older telecommunications data. It is also essential to distinguish between the frequency with which agencies access older data and the importance of that data to investigations when it is accessed: where agencies require access to telecommunications data, its value docs not decrease with age. Investigations of particularly serious crimes and series of crimes tend to rely on older retained data given the length of time taken to plan and/or commit these offences or series of offences, the need to identify patterns of criminal behaviour and relations between accomplices to a crime, and the need to establish criminal intent. These types of investigations include, but are not limited to:

- counter-terrorism and organised crime investigations, which are often characterised by long periods of preparation. These investigations often require time to establish a clear pattern of relationships between multiple events to expose not just individual suspects, but entire criminal networks, especially where suspects are practicing sophisticated counter-surveillance techniques
- investigations into 'lone actor' terrorists - in which metadata retained over an extended period of time can point to contact with other extremists, or other involvement with authorities
- counter-espionage investigations into activities which arc long-term, strategic, slow and considered in order to hide activities. There is often no known or specific incident or starting point with espionage investigations. ASIO must baseline the activities and threat posed by adversaries over an extended period to identify indicators of activity and then review historical data to understand the extent and scope of the activity and harm.

- series of related crimes, where agencies are required to piece together evidence from a wide range of sources, not all of which may be immediately evident
- cyber-crimes and other crimes where access to IP-based telecommunications data is required, due to the greater complexity of these investigations- the EU statistics show agencies are up to 7 times more likely to access IP-based data that is more than 12 months old than mobile telephony data
- trafficking in human beings and drug trafficking, where there is often a complex division of labour between accomplices
- serious corruption of public officials, financial crime and tax fraud, where offences are often only detected following audits, or are only reported to law enforcement agencies following internal investigations, requiring agencies to often access data that is already considerably dated
- repeated extortion, where victims are in a relationship with the offender and often only seek help months or even years after the exploitation commenced

- serious sexual offences, where victims may not report the offence for a considerable period of time after the event serious and the passage of time frequently means that other primary evidence (such as medical or forensic evidence) may no longer be available. The United Kingdom Government has provided advice that over half of the telecommunications data used by its agencies in the investigation of serious sexual offences is more than six months old
- serious criminal offences, particularly in relation to murder investigations, where extensive historical evidence must be assembled to prove intent or premeditation, and
- transnational investigations, which involve significant challenges for agencies attempting to coordinate investigations across multiple jurisdictions, frequently resulting in delays while preliminary information is obtained from foreign agencies.
- financial crimes, which are often only detected well after-the-fact, and investigators may take many months to review relevant evidence before they are in a position to identify suspects and/or their associates and request metadata.[10]

Committee response

1.185 **The committee thanks the Attorney-General for his response.**

1.186 The committee notes that a range of information has been provided to support the proposed two year data retention period as necessary in relation to investigations of serious crime or specific national security threats. In particular, the response lists a range of cases where a two year data retention period may be needed.

1.187 However, the response acknowledges the low frequency of use of data that is more than six months old, and that the proposed two year retention period is essentially required to ensure that older data is available for the investigation of national security and complex criminal offences. The committee notes that, despite this, the scheme does not limit access to data which is older than six months to the investigation of national security and complex criminal offences. Indeed, the scheme would in practice allow access to all retained data for the investigation of less serious crimes, including crimes punishable only by monetary penalties. However, limited information has been provided as to why the two year data retention period is necessary for the investigation of these less serious crimes.

1.188 In addition, the committee notes that the two year data retention period is at the upper end of the mandatory data retention periods in comparable

10 See, Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 6-8.

jurisdictions, such as the United Kingdom and Germany, which have retention periods of twelve months and six months respectively.

1.189 Given this, the committee considers that the blanket two year data retention period appears to be broader than is strictly required to achieve its stated objectives. That is, the scheme is not a proportionate way to achieve its ends, as is required under international law to justify a limitation of human rights.

1.190 **The committee acknowledges that the two year data retention period may be necessary for investigations of complex or serious crimes. However, the committee considers that the case has not been made as to the proportionality of the two year mandatory data retention period in relation to less serious crimes. The committee therefore recommends that, to avoid the disproportionate limitation on the right to privacy that would result from a two year mandatory data retention, the bill be amended to limit access to data to investigations of complex or serious crimes, specific serious threats or the investigation of serious matters by the Australian Securities and Investments Commission (ASIC), the Australian Taxation Office (ATO) and the Australian Competition and Consumer Commission (ACCC).**

Mandatory data retention scheme—access to information

Access to data—right to privacy

1.191 Currently under the TIA Act a broad number of agencies may access telecommunications data (metadata). These agencies do not require a warrant to access this data. Chapter 4 of the TIA Act permits an 'authorised officer' of an 'enforcement agency' to authorise a service provider to disclose existing telecommunications data where it is 'reasonably necessary' for the enforcement of, 'a law imposing a pecuniary penalty or the protection of the public revenue'. The disclosure of prospective data may be authorised when it is considered 'reasonably necessary' for the investigation of an offence with a maximum prison term of at least three years. The TIA Act also allows senior Australian Security Intelligence Organisation (ASIO) officers to authorise access to existing telecommunications data and prospective data in the performance of its functions. Schedule 2 of the bill would amend the definition of 'enforcement agency' under the TIA Act to confine the number of agencies that are able to access such data. The listed agencies would include the Australian Federal Police, a police force of a state and the Australian Commission for Law Enforcement Integrity. The minister would have the power under proposed section 110A to declare further authorities or bodies to be a 'criminal law enforcement agency' according to criteria specified in the bill. Provisions in relation to ASIO's access to telecommunications data remain unchanged under the proposed scheme.

1.192 The committee noted that there appeared to be no significant limits on the type of investigation to which a valid disclosure authorisation for existing data may apply. For example, there is no requirement that the disclosure of

telecommunications data be related to a serious crime, and the scheme may allow a disclosure authorisation where it is 'reasonably necessary' for the enforcement of minor offences. The committee noted that the lack of a threshold, relating to the nature and seriousness of the offence, for access to retained data appears to be a disproportionate limitation on the right to privacy. The committee considered that to ensure a proportionate limitation on the right to privacy, an appropriate threshold should be established to restrict access to retained data to investigations of specified threatened or actual crimes that are serious, or to categories of serious crimes such as major indictable offences (as is the current threshold for requiring the option of trial by jury).

1.193 The committee therefore recommended that the bill, so as to avoid the disproportionate limitation on the right to privacy that would result from disclosing telecommunications data for the investigation of any offence, be amended to limit disclosure authorisation for existing data to where it is 'necessary' for the investigation of specified serious crimes, or categories of serious crimes.

Attorney-General's response

> The Committee has suggested that the 'reasonably necessary' test be replaced with a 'necessary' test in the context of the Bill, on the basis that it lacks the requisite degree of precision.
>
> Enforcement agencies may only authorise access to specified metadata where access to that specified metadata is 'reasonably necessary' for a legitimate investigation. Service providers are only required, pursuant to subsection 313(3) of the *Telecommunications Act 1997*, to comply with a data authorisation to the extent that it is 'reasonably necessary' for a prescribed purpose. Service providers may refuse requests that do not meet this requirement.
>
> Amending the test for authorising the disclosure of metadata to circumstances where the disclosure is 'necessary' as opposed to 'reasonably necessary' would result in the privacy protections contained in Chapter 4 of the TIA Act diverging from those contained in the *Privacy Act 1988*.
>
> 'Reasonably necessary' is the test under Australian privacy law for the collection, use and disclosure of personal and sensitive information. It is an objective test requiring an assessment as to whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. The 'reasonably necessary' test is used throughout the Australian Privacy Principles, including in relation to the collection of personal and sensitive information, and in relation to enforcement-related activities.
>
> By contrast, the 'necessary' test is used only rarely throughout the Privacy Act, in relation to a limited number of permitted general situations - including where it is qualified by the requirement that the entity 'reasonably believes' that the collection, use or disclosure is 'necessary' -

permitted health situations, and certain contractual situations. The Privacy Commissioner has confirmed that the usage of the 'necessary' test as opposed to the 'reasonably necessary' test is explained by the context in which the test is used.

There is no suggestion that the 'necessary' test is more certain, narrow or strict than the 'reasonably necessary' test. By contrast, the High Court has observed 'that there is, in Australia, a long history of judicial and legislative use of the term "necessary", not as meaning essential or indispensable, but as meaning reasonably appropriate and adapted'.[11]

The Australian Law Reform Commission has observed, in the context of the former National Privacy Principles, that the term 'necessary' implies an objective test.[12]

The replacement of the 'necessary' test from the National Privacy Principles with the 'reasonably necessary' test in the Australian Privacy Principles requires the collection of personal information to be justifiable on objective grounds, rather than on the subjective views of the entity itself and is intended to expressly clarify that the test is objective (rather than implied) and to enhance privacy protection. For the same reasons, it is preferable that access to telecommunications data be based on the 'reasonably necessary' test.

Likewise, the Government does not agree with the Committee's recommendation that access to and use of metadata should be limited to certain categories of serious crimes. The Government believes that it is preferable to restrict access by specifying the agencies that are empowered to authorise the disclosure of data, rather than raise the access threshold to an arbitrarily imposed 'serious crime' threshold. Accordingly, Schedules 2 and 3 introduce provisions to reduce the range of agencies that may access telecommunications data, replacing the general descriptors of the types of agencies that may do so.

In addition, Australia is required to make metadata available for all criminal investigations by virtue of being a party to the Convention on Cybercrime. Article 14 of that Convention requires that Australia and other States parties establish powers and procedures, including access to historical telecommunications data, to enable the collection of evidence in electronic form of a criminal offence.

Telecommunications data is valuable to combatting all crimes, is less intrusive than other investigative techniques, and should not be arbitrarily limited to a narrow selection of crimes.[13]

---

11 *Mulholland v Australian Electoral Commission* (2004) 220 CLR 181, (39).

12 Ibid, 21.75.

13 See, Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 8-10.

Committee response

1.194 **The committee thanks the Attorney-General for his response.**

1.195 The committee considers, based on the information provided, that the 'reasonably necessary' test rather than the 'necessary' test under Australian domestic law may be sufficiently precise for human rights purposes. However, the committee notes that part of the test of 'necessary' under international human rights law requires that there be no other less rights restrictive means available to achieve the same result. That is, a measure which limits human rights must be the least rights restrictive alternative. Use of the 'reasonably necessary' test for access to telecommunications data under Australian domestic law may not therefore, in and of itself, address this particular requirement under international human rights law. However, the committee notes that other recommendations made by the committee, including a warrant regime (discussed below) and that access be restricted to investigation of serious crimes, would assist to address the least restrictive alternative requirement.

1.196 As noted previously, the committee's major concern was that there appear to be no significant limits on the type of investigation to which a valid disclosure authorisation for existing data may apply. The committee notes that the government has not accepted the committee's recommendation that, to ensure a proportionate limitation on the right to privacy, an appropriate threshold should be established to restrict access to retained data to investigations of specified threatened or actual crimes that are serious, or to categories of serious crimes such as major indictable offences.

1.197 In this respect, the committee's recommendation that retained data be accessed only for the purposes of investigating complex or serious offences is not reasonably characterised as imposing an 'arbitrary' threshold on access to retained data. Rather, such a requirement would ensure the scheme did not in fact represent an arbitrary and disproportionate limitation on the right to privacy.

1.198 As noted above, metadata can reveal very significant information about a person's life, associations, habits and preferences and therefore significantly limits the right to privacy. The proposed scheme would allow access to metadata for two years for the investigation of minor offences, including offences attracting only monetary penalties. For example, the scheme could allow access to a person's metadata up to two years after that data was collected for the investigation of a minor traffic offence or copyright infringement. The committee considers that the Attorney-General's response has not established that these kinds of minor crimes warrant the extent and degree of interference with the right to privacy that the scheme imposes. That is, they do not appear to be sufficiently serious to justify such an interference as being proportionate to the stated legitimate objective of the scheme. Indeed, while the response focuses on the need for mandatory data retention in relation to complex investigations, serious crime and national security,

access to retained data under the scheme will not be restricted to such investigations.

1.199 The committee notes the Attorney-General's view that, rather than apply an access threshold relating to the nature of the offence being investigated, it is preferable to restrict access to retained data by specifying the agencies that may access the retained data. The committee considers that this proposal to limit the number of agencies that may access telecommunications data is a relevant safeguard in the assessment of the proportionality of the scheme's limitation on the right to privacy.

1.200 However, the committee notes there will remain a significant number of agencies that will be empowered to access metadata without a warrant. Further, limiting which agencies may access telecommunications data, where the mandates of many of those agencies are relatively broad, does not address the concern that the scheme may operate to disproportionately interfere with a person's right to privacy—namely, that access to a person's metadata may occur even in relation to minor crimes, including those attracting only monetary penalties.

1.201 Given this, notwithstanding the proposed restriction on the number of agencies that may access retained data, the committee considers that the scheme does not appear to be sufficiently circumscribed to ensure that the limit it imposes on the right to privacy is proportionate. That is, the scheme does not appear to be only as extensive as is strictly necessary.

1.202 The committee notes the Attorney-General's remarks on Australia's obligations as a party to the Convention on Cybercrime as a justification for not limiting access to metadata to particular categories of crimes.

1.203 However, the committee notes that any such obligations must be considered against Australia's obligations under the ICCPR in relation to the right to privacy, and in particular that any limitations on the right to privacy are required to be proportionate.

1.204 The committee considers that it would be unusual if precedence were to be given to a Council of Europe Convention on Cybercrime above Australia's obligations under international human rights law.

1.205 Indeed, the committee notes that a number of the other parties to the Convention on Cybercrime were also subject to the European Union (EU) Data Retention Directive scheme, which was struck down by the European Court of Justice as being a disproportionate interference with the right to privacy. One of the reasons that scheme was held to be disproportionate was that it did not include any objective criteria to ensure that only competent national authorities could access retained data, and could then only use it for the prevention, detection or criminal prosecution of offences that, given the extent and seriousness of the scheme's interference with the fundamental human rights in question, may be considered to be sufficiently serious to justify such interference. The committee notes that EU

members are required to take necessary measures to comply with the framework set out by this judgement. The committee therefore considers that any obligations upon parties to the Convention on Cybercrime are not been determinative of the compatibility of the proposed data retention scheme with the right to privacy.

1.206 **The committee therefore recommends that the bill, so as to avoid the disproportionate limitation on the right to privacy that would result from disclosing telecommunications data for the investigation of any offence, be amended to limit disclosure authorisation for existing data to instances where it is reasonably necessary for the investigation of specified serious crimes, categories of serious crimes or the investigation of serious matters by the Australian Securities and Investments Commission (ASIC), the Australian Taxation Office (ATO) and the Australian Competition and Consumer Commission (ACCC).**

Use of data after it is accessed—right to privacy

1.207 While there are some safeguards in the TIA Act against misuse of data, the proposed data retention scheme may allow data that is disclosed for an authorised purpose to be used for unrelated purposes. For example, under information sharing provisions in the TIA Act and the *Australian Security Intelligence Organisation Act 1979*, the Australian Secret Intelligence Service (ASIS) may receive information obtained by ASIO under the TIA Act if it is relevant to ASIS's functions.

1.208 The committee recommended that, to avoid the disproportionate limitation on the right to privacy that would result from data that is disclosed for an authorised purpose being used for an unrelated purpose, the bill be amended to restrict access to retained data on defined objective grounds, including:

- where it is 'necessary' for investigations of specific serious crimes such as major indictable offences or specific serious threats; and
- that it be used only by the requesting agency for the purpose for which the request was made and for a defined period of time.

Attorney-General's response

> The Government does not agree with the Committee's recommendation that retained metadata be used only by the requesting agency for the purpose for which the request was made and for a defined period of time. It would unduly and unnecessarily frustrate legitimate law enforcement efforts.
>
> Agencies are often required to conduct joint investigations when a matter spans multiple jurisdictions, when a suspect crosses a border during an investigation. Sometimes the nature and focus of an investigation changes based on new information, requiring information obtained for one purpose to be used for one or more separate purposes. For example, missing person investigations can often become kidnapping, serious sexual assault and/or murder investigations. Security intelligence investigations

can transition into criminal investigations and vice versa, particularly in the case of counter-terrorism and counter-espionage.

In addition, agencies conducting an investigation may identify information pointing to additional criminal conduct. For example, agencies investigating organised criminal activity may identify information pointing to corruption or money laundering. Agencies investigating a particular crime may obtain evidence linking the suspect with other, unsolved crimes. Investigators may often uncover evidence that is directly relevant to another investigation (such as data demonstrating that a suspect in both investigations is using a covert phone).

There is no basis in international law for the proposition that information gathered by a law enforcement or security agency may be used only for the purpose for which it was obtained. Conversely the need to share such information is directly reflected in the *Convention on Cybercrime*, under which agencies may also be required to respond to a request for mutual legal assistance.

Existing safeguards will continue to apply to access to telecommunications data. A limited number of approved management-level officials in Australian enforcement agencies may authorise the disclosure of specified telecommunications data that is reasonably necessary for a prescribed purpose, and only after having regard to whether any interference with the privacy of any person or persons would be justified, having regard to the likely usefulness of the information and the purpose for which it is sought.

Under section 182 of the *Telecommunications (Interception and Access) Act 1979*, a person may only use or disclose telecommunications data lawfully obtained by an enforcement agency if the use or disclosure is 'reasonably necessary' for the performance by ASIO of its functions, for the enforcement of the criminal law, for the enforcement of a law imposing a pecuniary penalty, or for the protection of the public revenue. The interpretation of 'reasonable necessity' in this context will be similar to its interpretation in relation to the authorisation of the disclosure of data- where the use or disclosure of the specified data would have a demonstrable benefit or assist in enforcing the criminal law, without which there would be a likelihood that such enforcement could not occur. The use of metadata for a prurient purpose, or even as part of an investigation where its use or disclosure is not reasonably necessary for a prescribed purpose, would constitute a criminal offence.

In addition:

- section 182 of the TIA Act makes it a criminal offence, punishable by imprisonment for 2 years, to use or disclose metadata that has been lawfully obtained by an enforcement agency under Divisions 4 or 4A of Chapter 4 of the TIA Act

- section 185 of the TIA Act requires enforcement agencies to retain authorisations made under Chapter 4 of the TIA Act for 3 years. The Bill preserves this requirement, and also introduces comprehensive new record-keeping requirements around access to, and the use and disclosure of metadata by enforcement agencies.
- section l 8A of the ASIO Act makes it a criminal offence, punishable by imprisonment for 3 years, to deal in information lawfully obtained by ASIO in connection with its functions, including telecommunications data obtained by ASIO under Division 3 of Chapter 4 of the TIA Act.
- section 18 of the ASIO Act makes it a criminal offence, punishable by imprisonment for 10 years, to communicate such information, subject to a limited number of exceptions to allow for the lawful use and disclosure of lawfully accessed data, and other information in the case of ASIO.

Australian Privacy Principle 11 also requires Commonwealth law enforcement agencies to take such steps as are reasonable in the circumstances to protect personal information in their possession from misuse, interference and loss, and from unauthorised access, modification or disclosure.

The Australian Privacy Principles do not apply to ASIO. However, the *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)* require the Director-General of Security to ensure that all personal information collected or held by ASIO is protected by reasonable security measures against loss and unauthorised access, use or modification. The use and communication of telecommunications data by ASIO is similarly subject to strict controls under the ASIO Act and the Attorney-General's Guidelines.

The Australian Government's Protective Security Policy Framework also requires agencies to appropriately classify, secure and restrict access to information, including metadata and other information lawfully obtained in the course of an investigation. The need-to-know principle is enshrined within the Framework as are the requirements for officials to hold appropriate security clearances and briefings before they are permitted to receive, use and disclose information. The existence of similar appropriate processes and procedures to give effect to such obligations would be a relevant consideration for the Attorney-General when considering an application for an agency to be declared a criminal law-enforcement agency or an enforcement agency, pursuant to paragraphs 110A(4)(d) and 176A(4)(d), respectively.

The Committee has specifically referenced the statutory ability of ASIO to share information with the Australian Secret Intelligence Service. ASIS's functions and activities include supporting Australian soldiers in combat

> operations, enabling the safe rescue of kidnapped civilians, counter-terrorism and counter-proliferation. A limit on ASIO's ability to share that information would frustrate those important objectives. The prevention and suppression of terrorism is of great public importance, and the proliferation of nuclear, chemical and biological weapons, as well as their means of delivery, constitutes a threat to international peace and security within the meaning of Chapter VII of the United Nations Charter. I also note that the Committee has, in a more recent report, contemplated that the sharing of information (not limited to metadata) by ASIS with the Australian Defence Force could be necessary and proportionate.[14]

Committee response

1.209 **The committee thanks the Attorney-General for his response.**

1.210 The committee concurs with the Attorney-General's view that there is no general proposition in international law that information gathered by a law enforcement or security agency may be used only for the purpose for which it was obtained.

1.211 However, in relation to the committee's initial analysis of the proposed data retention scheme, the committee notes that international human rights law requires measures that limit human rights to be sufficiently circumscribed so as to be proportionate to their stated objective. Specifically, measures which permit access to personal information or information sharing between agencies will be a permissible limitation on human rights where they pursue a legitimate objective, are rationally connected to that objective and are a proportionate means of achieving that objective. The committee's initial analysis noted that, for the purposes in international human rights law, the proposed mandatory data retention scheme pursues a legitimate objective, but raises questions regarding the proportionality of the scheme.

1.212 The committee recognises that there are a number of important protections proposed to prevent the unauthorised disclosure of data under the scheme.

1.213 However, while the Australian Privacy Principles provide important protection of the right to privacy, the range of uses to which metadata may be put once accessed remains quite broad. This means that, even if access to metadata is initially proportionate, it may subsequently be used for purposes which would not be proportionate to the right to privacy (this potential may be open-ended, given that there is no express requirement in the bill or the TIA that accessed data be destroyed after a particular period of time). For example, under the proposed scheme a person's metadata may be accessed to investigate a person for a serious offence, which would be a proportionate interference with the right to privacy. However, that

14 See Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 10-11.

data could be kept, shared and used many years later for other ends, such as the investigation of the individual or their associates for a relatively minor crime such as a traffic offence.

1.214 As noted above, metadata is capable of revealing significant personal details about an individual. In this context, ensuring that the use of such data is limited to particular purposes and particular agencies would assist to ensure the interference with the right to privacy is proportionate to the stated legitimate objective of the proposed data retention scheme. The committee's recommendation was therefore aimed at ensuring that any use of retained metadata would be proportionate.

1.215 The committee acknowledges the Attorney-General's advice that law enforcement agencies may have legitimate reasons for utilising metadata obtained for one purpose for the purpose of investigating another crime or for sharing data across agencies. The committee therefore considers that, based on the information provided regarding the conduct of investigations, it may not be necessary in this case to restrict use of metadata once accessed solely to the purpose for which the request for access was made.

1.216 However, as noted above, the committee considers that there still needs to be sufficient limitations on the use of retained metadata, once accessed, to ensure that the interference with the right to privacy is proportionate, in the sense of being the alternative that is the least restrictive of rights. In this respect, the committee considers that, where agencies are working together, a less restrictive alternative from the perspective of the right to privacy may be to have a system which expressly authorises the access of each agency to the retained telecommunications data.

1.217 In addition, limiting access to telecommunications data for a defined period (after which the data be destroyed) would be less restrictive of the right to privacy than the proposed scheme.

1.218 **The committee therefore recommends that, to avoid the disproportionate limitation on the right to privacy that could result from data that is disclosed for an authorised purpose being used for an unrelated purpose, the bill be amended to restrict access to retained data on defined objective grounds, including:**

- **where it is reasonably necessary for investigations of specific serious crimes such as major indictable offences, specific serious threats or the investigation of serious matters by the Australian Securities and Investments Commission (ASIC), the Australian Taxation Office (ATO) and the Australian Competition and Consumer Commission (ACCC); and**
- **where it is to be used by the authorised agency for a defined period of time.**

Legal Professional Privilege—right to privacy

1.219 Under the proposed scheme there are no exceptions for the retention of and access to data relating to persons whose communications are subject to obligations

of professional secrecy, such as lawyers. The committee therefore requested the advice of the Attorney General as to whether such data could, in any circumstances, impact on legal professional privilege and, if so, how this is proportionate with the right to privacy.

Attorney-General's response

> At common law, confidential communications between a client and the client's legal adviser are privileged, whether oral or in the form of written or other material, if made for the dominant purpose of submission to the legal adviser for advice (whether connected with litigation or not) or for use in existing or anticipated litigation.
>
> At common law, legal professional privilege attaches to the content of privileged communications, not to the fact of the existence of a communication between a client and their lawyer. This distinction is demonstrated in the routine practice of parties to proceedings filing affidavits of documents listing documents in their possession that are not being produced on the ground of privilege, thereby disclosing the fact of the existence of the document, including legal advice.
>
> The uniform evidence laws contain provisions codifying 'client legal privilege' as it applies to evidence led in court, however these provisions do not apply to pre-trial procedures (such as discovery, subpoenas, search warrants or access to telecommunications data as part of an investigation), where the common law continues to apply.
>
> Proposed new paragraph 187A(4)(a) puts beyond doubt that service providers are not required to keep, or cause to be kept, information that is the content or substance of a communication. Section 172 of the *Telecommunications (Interception and Access) Act 1979* also provides that an authorisation for the disclosure of telecommunications data made under Chapter 4 of that Act does not permit the disclosure of information that is the contents or substance of a communication, or a document to the extent that the document contains the contents or substance of a communication.
>
> The TIA Act also provides that it is a criminal offence, punishable by two years' imprisonment, for a person to access a stored communication without lawful authority (section 108). The TIA Act also makes it an offence to disclose information obtained by unlawfully accessing a stored communication (section 133). As such, the data retention regime, and agencies' powers to access telecommunications data more broadly, do not affect or authorise the disclosure of the content of any communication, including any privileged communication.[15]

15 See Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 12.

Committee response

1.220 **The committee considers that, based on the information provided relating to the current understanding of legal professional privilege under Australian law, the proposed data retention scheme would allow for the protection of legal professional privilege.**

1.221 **However, some committee members considered that the protection of legal professional privilege would be assured only so long as the 'content' or substance of communications that are excluded from mandatory data retention includes all types of communications to which legal professional privilege may attach both now and into the future. These committee members considered that, to ensure that all content of communications that may be subject to legal professional privilege is excluded from the proposed data retention scheme, the bill be amended to include a non-exclusive definition of what type of data would constitute 'content' for the purposes of the scheme.**

Mandatory data retention scheme—oversight and accountability

Prior review—right to privacy

1.222 Under the bill, the Commonwealth Ombudsman would have oversight of the mandatory data retention scheme and the exercise of law enforcement agencies' powers under chapters 3 and 4 of the TIA Act. Additionally, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) would be tasked with reviewing the scheme three years after its commencement. While the proposed oversight mechanisms in the bill are directed at reviewing access powers after they have been exercised, there is no prior review of access to metadata through a warrant system, as is the case for access to other forms of information under the TIA Act.

1.223 The committee recommended that, so as to avoid the unnecessary limitation on the right to privacy that would result from a failure to provide for prior review, the bill be amended to provide that access to retained data be granted only on the basis of a warrant approved by a court or independent administrative tribunal, taking into account the necessity of access for the purpose of preventing or detecting serious crime and defined objective grounds as set out above at [1.207].[16]

1.224 The committee further recommended the establishment of a mechanism to provide close prior oversight of the recommended warrant process for access to retained metadata under the scheme.

22 In the case of emergencies application for warrants could occur by telephone as is currently the case under the TIA Act.

Attorney-General's response

The Government does not agree with the Committee's suggestion that agencies should be required to obtain a warrant to access metadata. It follows that the Government believes that it is unnecessary to have an advocate to ensure impartial assessment of the content and sufficiency of warrant applications to access metadata.

To require a warrant to access metadata would be impractical, and result in a significant degradation in agencies' ability to protect public safety. It would considerably delay agencies commencing almost every counter-terrorism, counter-espionage, organised crime, cybersecurity, murder, child exploitation and serious sexual assault investigation, with a considerable risk that critical evidence would be lost. Warrant applications take considerable time to develop, which necessarily delays investigations and creates a risk that perishable physical, electronic and testimonial evidence will be lost.

While metadata is used at all stages of law enforcement and national security investigations, it is predominantly used in the early stages to provide foundational information. By comparison, the other powers contained in the TIA Act, and virtually all other powers that are subject to a warrant, are used in the latter stages of an investigation. Access to metadata commonly provides the basis for more intrusive forms of investigation, including telecommunications interceptions, search warrants and the use of surveillance devices. It ensures that investigators can exclude others from suspicion and in turn from these investigative techniques. There is a clear distinction that can be drawn between the level of privacy impact occasioned by access to metadata and telecommunications interception or the execution of a search warrant.

In reaching its recommendations about warrants, the Committee has referenced the recent decision of the Court of Justice of the European Union in the Digital Rights Ireland case. In finding that the EU Data Directive was not human rights compatible, the Court found that access to data ought to have been dependent upon prior review by a court or independent administrative body.

By contrast, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has expressed a contrary view. The Special Rapporteur has distinguished between the 'surveillance of communications', which 'must only occur... under the supervision of an independent judicial authority' and the 'provision of communications data by the private sector to States' which must be 'sufficiently regulated to ensure that individuals' human rights are prioritized at all times' and 'should be monitored by an independent authority, such as a court or oversight mechanism'.

The requirement to obtain a warrant prior to exercising certain investigative powers is typically reserved for powers that immediately and

irretrievably engage the essence of a particular fundamental right or freedom. Conversely, the exercise of powers that do not engage the essence of fundamental rights and freedoms, or that only create a potential for future engagement of those rights and freedoms should the agency take subsequent, follow up action, are typically not subject to a requirement for independent authorisation by a judicial or quasi-judicial officer. In those circumstances, the preferable approach is to ensure that appropriate controls and safeguards are implemented at relevant points of the information cycle and, in particular, around how agencies may use data.

The use of data under the TIA Act is strictly controlled. Agencies may only access metadata on a case-by-case basis and, in the case of enforcement agencies, only where and to the extent that access is reasonably necessary for a prescribed purpose, such as the enforcement of the criminal law. Access may only be approved by management-level officials, who are required to have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the likely relevance and usefulness of the information or documents, and the reason why the disclosure or use concerned is proposed to be authorised. ASIO may only access metadata in connection with its functions and in accordance with the Attorney-General's Guidelines. The unauthorised use of metadata is a criminal offence punishable by two years' imprisonment, in the case of an enforcement agency, or three years' imprisonment, in the case of ASIO.

In addition, section 276 of the *Telecommunications Act 1997* makes it an offence for a carrier, carriage service provider or their employees to disclose the affairs or personal particulars of any other person that has come in to their knowledge or possession. A contravention of that offence is punishable by a term of imprisonment of up to 2 years.

Similarly, the *Privacy Act 1988* may apply to some information required to be retained by virtue of the Bill. That Act provides effective civil remedies for persons whose privacy may have been breached. Part V of that Act includes a comprehensive scheme for the making of, and investigation of complaints. The Privacy Commissioner also has the power to make determinations in relation to breaches of the Australian Privacy Principles.

In addition to the accountability mechanisms earlier outlined, the Bill introduces additional safeguards. In particular, the Bill will significantly limit the range of agencies permitted to access metadata, and will introduce comprehensive, independent oversight by the Commonwealth Ombudsman for all Commonwealth, state and territory agencies accessing metadata. This oversight function will support accountability and enable assessment of an agency's overall compliance with their powers to access and use stored communications and telecommunications data.

The Ombudsman will be given powers to enter agency premises at a reasonable time, inspect the records of agencies and obtain relevant

documentation and information to carry out its oversight functions. The Bill will empower the Ombudsman to require an officer of an enforcement agency to provide information to the Ombudsman in writing, and make it an offence to refuse to attend, give information or answer questions when required to do so. The offence will ensure that agency officers do not hinder the Ombudsman inspection functions by unreasonably refusing to attend, give information or answer questions as required.

The Bill also ensures that the Ombudsman obtains access to documents despite other laws, including the law of any State or Territory to ensure the Ombudsman is able to obtain all information and documents required to carry out the Ombudsman's inspection functions and that agency officers are not prevented by other laws from providing necessary information or assistance.

The Bill also creates a new public reporting regime in relation to the Ombudsman's oversight functions. The Ombudsman will be required to report on the results of its oversight functions relating to compliance by agencies generally with the requirements of the TIA Act including access to telecommunications data. The Ombudsman will report to the Attorney-General after the end of each financial year on the results of the Ombudsman's inspections. The Attorney-General must table the report in Parliament within 15 sitting days of receiving it.

The Bill also makes it an offence for an officer of a Commonwealth agency to refuse to comply with the requirement to attend, give information or answer questions in relation to the Ombudsman's oversight of telecommunications interception.[17]

Committee response

1.225 **The committee thanks the Attorney-General for his response.**

1.226 The committee notes that the Attorney-General's response sets out a number of reasons rejecting the committee's recommendation that agencies should be required to obtain a warrant to access metadata under the proposed data retention scheme.

1.227 However, as noted previously, technological developments have meant that metadata now allows very precise conclusions to be drawn about an individual's life, habits, interests, relationships and views even without access to the content of a communication being available. Given this, a prior review mechanism would assist to ensure that a person's metadata is accessed only in circumstances where such access would be proportionate. That is, prior review could assist to prevent unjustifiable interference with a person's privacy before it occurs.

17 See, Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 12-14.

1.228 While the committee considers that the proposal for oversight by the Ombudsman and the PJCIS are extremely important, these forms of oversight are directed at reviewing the exercise of powers only after a potentially unjustifiable interference with a person's privacy has occurred.

1.229 The committee acknowledges the important controls in the TIA for access to and use of telecommunications data. However, the committee notes that these internal agency approval processes provide a lower level of protection than could be provided by external independent review processes.

1.230 The committee notes the Attorney-General's further consideration of the recent judgement of the Court of Justice of the European Union (ECJ) which examined the European Union (EU) mandatory metadata retention regime. This case is accepted as bearing on the proposed data retention scheme, because it found that the EU mandatory data retention law was invalid because its interference with the right to privacy was not precisely circumscribed so as to be limited to what was strictly necessary. One of the relevant factors in reaching that conclusion was the absence of a requirement that access to retained data be subject to prior review by a court or independent administrative body (such as is provided by a warrant scheme).

1.231 The Attorney-General questions the validity or force of this finding by citing the apparently contrary view of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression as to whether access to retained metadata requires a warrant. However, the committee considers that this may be a misreading of the report by the Special Rapporteur, who has recommended that the provision of communications data by the private sector to the State should be:

> …sufficiently regulated to ensure that individuals' human rights are prioritized at all times. Access to communications data held by domestic corporate actors should only be sought in circumstances where other available less invasive techniques have been exhausted.
>
> The provision of communications data to the State should be monitored by an independent authority, such as a court or oversight mechanism. At the international level, States should enact Mutual Legal Assistance Treaties to regulate access to communications data held by foreign corporate actors.[18]

1.232 The committee notes the Attorney-General's advice that he considers that it would be unnecessary to establish a formal advocate to ensure impartial assessment of the content and sufficiency of warrant applications to access metadata.

---

18 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40 (17 April 2013) http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

1.233 The committee notes the existing requirements in the TIA for internal agency authorisation for disclosure of telecommunications data. The majority of the committee consider that the existing requirements provide a sufficient safeguard to address privacy concerns.

1.234 Some committee members consider one method of ensuring that access to metadata is sufficiently regulated and balanced against human rights priorities is to require prior review of access to telecommunications data. Such committee members consider that requirements for prior review would more effectively ensure that the grant of access to metadata under the scheme would be consistent with the right to privacy.

1.235 Further, such committee members note that independent prior review processes are able to be sufficiently flexible to respond to investigative timeframes, including emergency situations.

1.236 **Some committee members therefore recommend that, so as to avoid the unnecessary limitation on the right to privacy that would result from a failure to provide for prior review, the bill be amended to provide that access to retained data be granted only on the basis of prior independent authorisation, taking into account the necessity of access for the purpose of preventing or detecting serious crime and defined objective grounds as set out above at [1.218].**

1.237 **The majority of the committee notes the existing requirements in the TIA for internal agency authorisation for disclosure of telecommunications data and considers that the existing requirements provide a sufficient safeguard to address privacy concerns.**

1.238 **Some committee members consider that a prior independent authorisation system should be instituted, and that such a mechanism could assist to ensure impartial assessment of the content and sufficiency of application. These members are of the view that this would be an important safeguard where applications occurred ex parte (that is, without the individual whose data is to be accessed being present).**

1.239 **Another committee member considers that in order to provide a sufficient safeguard, and to avoid the unnecessary limitation on the right to privacy, such prior independent review should take the form of a warrant approved by a court or independent administrative tribunal, taking into account the necessity of access for the purpose of preventing or detecting serious crime and defined objective grounds as set out above at [1.218].**

1.240 **Further, such committee member considers that warrant processes are able to be sufficiently flexible to respond to investigative timeframes, including emergency situations. They may be expedited where necessary, including by, for example, having magistrates available to issue warrants out of hours or over the phone, and it is usual for warrant systems to have expedited processes to allow for time critical situations.**

1.241 **That committee member therefore recommends that, so as to avoid the unnecessary limitation on the right to privacy that would result from a failure to provide for prior, independent judicial review, the bill be amended to provide that access to retained data be granted only on the basis of a warrant approved by a court or independent administrative tribunal, taking into account the necessity of access for the purpose of preventing or detecting serious crime and defined objective grounds as set out above at [1.218].**

Mandatory data retention scheme—right to freedom of opinion and expression and the right to an effective remedy

1.242 Under the proposed scheme, data would be retained and could subsequently be used without the user or individual ever being informed. The committee recommended that, to ensure a proportional limitation on the right to freedom of opinion and expression, consideration be given to amending the proposed scheme to provide a mechanism to guarantee that access to data is sufficiently circumscribed. Such a mechanism could require, for example:

- individuals to be notified when their telecommunications data is subject to an application for authorisation for access or once it has been accessed (noting that there may be circumstances where delayed notification would be appropriate, such as in the context of investigating a serious crime); and
- a process to allow individuals to challenge such access (noting that exemptions may need to be available for continuing investigations of, for example, a serious crime).

Attorney-General's response

> The Committee's suggestion that individuals be notified when their telecommunications data is subject to an application for authorisation for access, or once it has been accessed, and be then able to challenge such access, would hamper investigations. The covert investigative powers contained in the *Telecommunications (Interception and Access) Act 1979* and *Surveillance Devices Act 2004* are generally used where the integrity of an investigation would be compromised by revealing its existence. In circumstances where overt access to metadata and other communications-related information is possible, such as where an agency is seeking information from a living victim of a crime, agencies are generally able to obtain that information from a provider with the person's consent.[19]

Committee response

1.243 **The committee thanks the Attorney-General for his response.**

---

19 See, Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 14.

1.244 As noted previously with respect to the right to freedom of opinion and expression, the proposed scheme may have an inhibiting or 'chilling' effect on people's freedom and willingness to communicate via telecommunications services. The committee notes that the proposed provisions may have a particular inhibiting or 'chilling' effect on journalists who may be concerned about the protection of their sources. For example, a journalist's email and mobile phone metadata may reveal contact between a journalist and a source. Journalists may also be concerned that such metadata could be used to charge them with criminal offences where information they have received from a source or whistle-blower is classified, sensitive or subject to legislative protection against disclosure. The scheme may also have a consequential inhibiting effect on the willingness of individuals to come forward as sources or whistle-blowers due to fear of greater risk of detection and prosecution.

1.245 Further, under the proposed scheme, data would be retained, and could subsequently be used, without the user or individual ever being informed. The potential for such undisclosed retention and use of metadata could lead people to 'self-censor' the views expressed via telecommunications services, or to restrict their own use of such services. That is, the scheme could engender the feeling that people are under constant surveillance.

1.246 The committee therefore considers that the scheme limits the right to freedom of expression. Measures that limit the right to freedom of expression are justifiable under international human rights law where they pursue a legitimate objective, are rationally connected to that objective and are a proportionate means of achieving that objective.

1.247 As noted above, the committee considers that the scheme pursues a legitimate objective but has concerns regarding the proportionality of the scheme.

1.248 The committee is of the view that the range of recommendations outlined above with respect to the right to privacy would also assist with the proportionality of the scheme with respect to the right to freedom of opinion and expression.

1.249 The committee further recommended additional safeguards, including with respect to the right to freedom of opinion and expression, in order to improve the proportionality of the scheme. Specifically, the committee suggested that a requirement for a notification to an individual that their data had been subject to an application for an authorisation for access would improve the proportionality of the scheme.

1.250 The committee notes the Attorney-General's view that a notification requirement that telecommunications data had been accessed would hamper investigations.

1.251 However, the committee notes that its suggestion clearly acknowledged the potential for such a requirement to impact on investigations, in stating that delayed notification arrangements would be appropriate in a range of circumstances

including where ongoing investigations may be hampered. The committee notes that the Attorney-General's response therefore does not significantly address the issues raised by the committee in relation to the right to freedom of opinion and expression, and ensuring the proportionality of the scheme in this regard.

1.252 The committee reiterates that it is the fundamental and legitimate interest of government to ensure that there are adequate tools for law enforcement agencies to ensure 'public safety and the ability for victims of crime to have recourse to justice'.[20] In this respect, safeguards to protect human rights must be balanced against the need to preserve the integrity of investigations of serious crimes.

1.253 **Some committee members recommend that, to ensure a proportional limitation on the right to freedom of opinion and expression, consideration be given to amending the proposed scheme to provide a mechanism to guarantee that access to data is sufficiently circumscribed, so that individuals are notified when their telecommunications data has been accessed (noting that there may be circumstances where such notification would need to be delayed to avoid jeopardising any ongoing investigation).**

1.254 **In addition, another committee member considered that the following requirements would better ensure the proportionality of the scheme in relation to the right to freedom of expression:**

- **a requirement for individuals to be notified when their telecommunications data is subject to an application for authorisation for access (noting that there may be circumstances where delayed notification would be appropriate, such as in the context of investigating a serious crime); and**
- **a process to allow individuals to challenge such access (noting that exemptions may need to be available for continuing investigations of, for example, a serious crime).**

1.255 The committee's initial analysis also noted that the right to an effective remedy would be supported by a notification requirement. This is because, for example, it would be impossible for an individual to seek redress for breach of their right to privacy if they did not know that data pertaining to them had been subject to an access authorisation.

1.256 The committee notes that the Attorney-General's response provided a range of information regarding remedies that may be available in relation to misuse of telecommunications data. However, the response does not directly address how and whether there are sufficient mechanisms to seek redress for a violation of the right to privacy or the right to freedom of opinion and expression in circumstances where

20 See, Appendix 1, Letter from Senator the Hon. George Brandis, Attorney-General, to Senator Dean Smith (dated 17 February 2015) 1-5.

a person is not aware that their telecommunications data has been accessed. Noting the significant number of issues in relation to which the committee sought further advice or responses from the Attorney-General, this issue may have been overlooked in the preparation of the Attorney-General's response.

1.257 **The committee therefore reiterates its request for the advice of the Attorney-General as to what measures there are to ensure that there are effective remedies available to individuals for any breaches that may occur of the right to privacy or the right to freedom of association as a result of the mandatory data retention regime.**