



Parliamentary Joint Committee on Human Rights

Human rights scrutiny report

Report 3 of 2021

17 March 2021

© Commonwealth of Australia 2021

ISSN 2204-6356 (Print)

ISSN 2204-6364 (Online)

PO Box 6100
Parliament House
Canberra ACT 2600

Phone: 02 6277 3823

Fax: 02 6277 5767

Email: human.rights@aph.gov.au

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

This report can be cited as: Parliamentary Joint Committee on Human Rights, *Report 3 of 2021*; [2021] AUPJCHR 26.

This document was prepared by the Parliamentary Joint Committee on Human Rights and printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

Membership of the committee

Members

Dr Anne Webster MP, Chair	Mallee, Victoria, Nats
Mr Graham Perrett MP, Deputy Chair	Moreton, Queensland, ALP
Senator Patrick Dodson	Western Australia, ALP
Mr Steve Georganas MP	Adelaide, South Australia, ALP
Mr Ian Goodenough MP	Moore, Western Australia, LP
Senator Nita Green	Queensland, ALP
Ms Celia Hammond MP	Curtin, Western Australia, LP
Senator the Hon Sarah Henderson	Victoria, LP
Senator Andrew McLachlan CSC	South Australia, LP
Senator Lidia Thorpe	Victoria, AG

Secretariat

Anita Coles, Committee Secretary
Charlotte Fletcher, Principal Research Officer
Rebecca Preston, Principal Research Officer
Ingrid Zappe, Legislative Research Officer

External legal adviser

Associate Professor Jacqueline Mowbray

Table of contents

Membership of the committee	iii
Committee information	vii
Chapter 1—New and continuing matters	1
Bills	
Online Safety Bill 2021 and Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021	2
Social Services Legislation Amendment (Strengthening Income Support) Bill 2021	30
Bills and instruments with no committee comment	35
Chapter 2—Concluded matters	
Bills	
Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill 2020.....	37
Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020	63

Committee information

Under the *Human Rights (Parliamentary Scrutiny) Act 2011* (the Act), the committee is required to examine bills, Acts and legislative instruments for compatibility with human rights, and report its findings to both Houses of the Parliament. The committee may also inquire into and report on any human rights matters referred to it by the Attorney-General.

The committee assesses legislation against the human rights contained in the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR); as well as five other treaties relating to particular groups and subject matter.¹ A description of the rights most commonly arising in legislation examined by the committee is available on the committee's website.²

The establishment of the committee builds on Parliament's established tradition of legislative scrutiny. The committee's scrutiny of legislation is undertaken as an assessment against Australia's international human rights obligations, to enhance understanding of and respect for human rights in Australia and ensure attention is given to human rights issues in legislative and policy development.

Some human rights obligations are absolute under international law. However, in relation to most human rights, prescribed limitations on the enjoyment of a right may be permissible under international law if certain requirements are met. Accordingly, a focus of the committee's reports is to determine whether any limitation of a human right identified in proposed legislation is permissible. A measure that limits a right must be **prescribed by law**; be in pursuit of a **legitimate objective**; be **rationaly connected** to its stated objective; and be a **proportionate** way to achieve that objective (the **limitation criteria**). These four criteria provide the analytical framework for the committee.

A statement of compatibility for a measure limiting a right must provide a detailed and evidence-based assessment of the measure against the limitation criteria.

-
- 1 These are the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD); the Convention on the Elimination of Discrimination against Women (CEDAW); the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT); the Convention on the Rights of the Child (CRC); and the Convention on the Rights of Persons with Disabilities (CRPD).
 - 2 See the committee's *Short Guide to Human Rights* and *Guide to Human Rights*, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Guidance_Notes_and_Resources.

Where legislation raises human rights concerns, the committee's usual approach is to seek a response from the legislation proponent, or draw the matter to the attention of the proponent and the Parliament on an advice-only basis.

More information on the committee's analytical framework and approach to human rights scrutiny of legislation is contained in *Guidance Note 1*, a copy of which is available on the committee's website.³

3 See *Guidance Note 1 – Drafting Statements of Compatibility*, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Guidance_Notes_and_Resources.

Chapter 1¹

New and continuing matters

1.1 In this chapter the committee has examined the following bills and legislative instruments for compatibility with human rights:

- bills introduced into the Parliament between 22 to 25 February 2021;
- legislative instruments registered on the Federal Register of Legislation between 28 January 2021 to 18 February 2021;² and

1.2 Bills and legislative instruments from this period that the committee has determined not to comment on are set out at the end of the chapter.

1.3 The committee comments on the following bills and seeks a response or further information from the relevant minister.

1 This section can be cited as Parliamentary Joint Committee on Human Rights, *New and continuing matters, Report 3 of 2021*; [2021] AUPJCHR 27.

2 The committee examines all legislative instruments registered in the relevant period, as listed on the Federal Register of Legislation. To identify all of the legislative instruments scrutinised by the committee during this period, select 'legislative instruments' as the relevant type of legislation, select the event as 'assent/making', and input the relevant registration date range in the Federal Register of Legislation's advanced search function, available at: <https://www.legislation.gov.au/AdvancedSearch>.

Bills

Online Safety Bill 2021¹

Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021

Purpose	<p>The Online Safety Bill 2021 seeks to create a new framework for online safety in Australia, and establish an eSafety Commissioner with the powers to investigate complaints and objections</p> <p>The Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021 seeks to repeal the <i>Enhancing Online Safety Act 2015</i>, make consequential amendments to various Acts and provide for transitional provisions relating to the eSafety Commissioner</p>
Portfolio	Communications, Urban Infrastructure, Cities and the Arts
Introduced	House of Representatives, 24 February 2021
Rights	Rights of women; rights of the child; privacy; freedom of expression; life; prohibition against torture and other cruel, inhuman or degrading treatment or punishment; and criminal process rights

Removal of, and disabling of access to, online content

1.4 This bill seeks to establish a new framework for online safety for people in Australia, enabling the minister to determine basic online safety expectations for social media services, electronic services (for example, SMS, chat or other communication services), or internet services (including those which allow individuals to access material online).²

1.5 The bill would also establish the office of the eSafety Commissioner (the Commissioner) to administer: a complaints system for cyber-bullying material targeting an Australian child and cyber-abuse material targeting an Australian adult; and a complaints and objection system for non-consensual sharing of intimate

1 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Online Safety Bill 2021 and Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021, *Report 3 of 2021*; [2021] AUPJCHR 28.

2 Part 4. These terms are defined in clauses 13–14.

images (including images depicting nudity).³ The Commissioner would also be empowered to enforce online safety by issuing blocking notices, link deletion notices, or app removal notices, to require the removal of online materials depicting abhorrent violent conduct, and certain pornographic and other materials depicting sexual or violent content. Non-compliance would be punishable by a range of civil penalty provisions and enforced through the adoption of enforcement powers contained in the *Regulatory Powers (Standard Provisions) Act 2014*. The bill would also empower the Commissioner to develop industry standards requiring compliance, and enable bodies and associations representing sections of the online industry to also develop their own self-regulatory industry codes.⁴

Preliminary international human rights legal advice

Rights of the child, rights of women, rights to privacy and freedom of expression

1.6 The bill seeks to enhance the safety of Australian children and adults on the internet by establishing a legislative framework for receiving and investigating individual complaints about online bullying and abuse, and the posting of intimate images without a person's consent. In particular, it seeks to facilitate the timely resolution of complaints about cyber-bullying of children. The bill also seeks to enhance online safety for Australians more generally by establishing mechanisms by which the Commissioner may require the speedy removal of violent and offensive material, and ensure that individuals do not view them. It also seeks to build-in flexibility to adapt the scheme to address emerging online harms, including by providing for the development of legislative instruments at a later time.

1.7 As such, the proposed scheme is likely to promote numerous human rights, including the right of women to be free from sexual exploitation, the rights of the child and the right to privacy and reputation. The United Nations (UN) Human Rights Council has stated that the human rights which people have offline must also be protected online.⁵ International human rights law recognises that women are vulnerable to sexual exploitation, particularly online, and that States Parties have particular obligations with respect to combatting sources of such exploitation.⁶ The UN Special Rapporteur on violence against women, has noted that:

When women and girls do have access to and use the Internet, they face online forms and manifestations of violence that are part of the continuum

3 The office of the eSafety Commissioner already exists under the *Enhancing Online Safety Act 2015*. That legislation would be repealed with the intention of replacing the scheme with this bill and the associated Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021.

4 Part 9, Division 7.

5 See, UN Human Rights Council, *Resolution 32/13 on the promotion, protection and enjoyment of human rights on the internet*, A/HRC/RES/32/13 (2016).

6 Convention on the Elimination of All Forms of Discrimination Against Women, article 6.

multiple, recurring and interrelated forms of gender-based violence against women. Despite the benefits and empowering potential of the Internet and ICT [Information and Communication Technologies], women and girls across the world have increasingly voiced their concern at harmful, sexist, misogynistic and violent content and behaviour online. It is therefore important to acknowledge that the Internet is being used in a broader environment of widespread and systemic structural discrimination and gender-based violence against women and girls, which frame their access to and use of the Internet and other ICT.⁷

1.8 Children also have special rights under human rights law taking into account their particular vulnerabilities,⁸ including the right to protection from all forms of violence, maltreatment or sexual exploitation.⁹ The international community has recognised the importance of creating a safer online environment for children,¹⁰ and noted the need to establish regulation frameworks which enable users to report concerns about content.¹¹ Indeed, in 2016 the UN Special Representative of the Secretary-General on Violence against Children observed that information and communication technologies can:

be associated with serious risks of violence, including online sexual abuse and exploitation. Children can be exposed to cyberbullying, harmful information or abusive material, groomed by potential predators and subjected to abuse and exploitation, including through sexting, the production and distribution of images depicting child abuse and live web streaming. ICTs have significantly facilitated the production, distribution and possession of child abuse images and with rapidly developing technology, the number of perpetrators is growing.¹²

7 See, for example, Human Rights Council, *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*, A/HRC/38/47 (2018) [14].

8 Convention on the Rights of the Child. See also, UN Human Rights Committee, *General Comment No. 17: Article 24* (1989) [1].

9 See, Convention on the Rights of the Child, articles 19, 34, and 36.

10 UNICEF and International Telecommunications Union, *Guidelines for industry on child protection* (2015) p. 8;

11 See, for example, International Telecommunications Union, *Guidelines for policy-makers on Child Protection Online* (2020).

12 UN Human Rights Council, *Annual report of the Special Representative of the Secretary-General on Violence against Children*, A/HRC/31/20 (2016) [44].

1.9 The Special Representative further stated that responses to violence against children must effectively detect and address online abuse, so that children can explore the online world with confidence and in safety.¹³

1.10 In addition, international human rights law recognises that the right to privacy must also be protected online. The right to privacy is multi-faceted. It protects against arbitrary and unlawful interferences with an individual's privacy and attacks on reputation.¹⁴ It can also be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from excessive unsolicited intervention by other uninvited individuals.¹⁵

1.11 While the proposed measure appears to promote these rights, in order to achieve its important objectives, it also necessarily engages and limits the right to freedom of expression. The right to freedom of expression includes the freedom to seek, receive and impart information and ideas of all kinds, either orally, in writing or print, in the form of art, or through any other media of an individual's choice.¹⁶ It is not an absolute right. While the right to *hold* an opinion may never be permissibly limited under law,¹⁷ the right to freedom of expression (that is, the freedom to *manifest* one's beliefs or opinions) can be limited.¹⁸ For example, the International Covenant on Civil and Political Rights expressly provides that the advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.¹⁹ The International Covenant on the Elimination of Racial Discrimination also requires States to make it an offence to disseminate 'ideas based on racial superiority or hatred, incitement to racial

13 UN Human Rights Council, *Annual report of the Special Representative of the Secretary-General on Violence against Children*, A/HRC/31/20 (2016) [51].

14 There is international case law to indicate that this protection only extends to attacks which are unlawful. See *RLM v Trinidad and Tobago*, UN Human Rights Committee Communication No. 380/89 (1993); and *IP v Finland*, UN Human Rights Committee Communication No. 450/91 (1993).

15 UN Human Rights Council, *Report of the High Commissioner for Human Rights: the right to privacy in the digital age*, A/HRC/39/29 (2018) [5]; *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Martin Scheinin, A/HRC/13/37 (2009) [11].

16 International Covenant on Civil and Political Rights, article 19(2).

17 International Covenant on Civil and Political Rights, article 19(1).

18 Article 19(3) of the International Covenant on Civil and Political Rights states that the exercise of the right to freedom of expression carries with it special duties and responsibilities, and may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: for respect of the rights or reputations of others; for the protection of national security or of public order; or of public health or morals.

19 International Covenant on Civil and Political Rights, article 20(2).

discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin'.²⁰ These provisions are understood as constituting compulsory limitations on the right to freedom of expression.²¹

1.12 The right to freedom of expression may be permissibly limited where a measure seeks to achieve a legitimate objective, is rationally connected to (that is, effective to achieve) that objective, and is a proportionate means by which to achieve it.

1.13 As discussed at paragraph [1.6], this bill seeks to achieve a number of important objectives, with the overarching goal of enhancing the online safety of Australians. The statement of compatibility notes that children; young women; Indigenous Australians; and lesbian, gay, bisexual, transgender, queer or intersex (LGBTQI) people are particularly vulnerable to online harms.²² It highlights that Indigenous and LGBTQI Australians experience online hate speech at more than double the national average.²³ It also notes that the sharing of intimate images without consent can be a component of domestic and family violence, noting that one in four women who reported the posting of such an image of themselves had also experienced other threatening behaviour from the perpetrator.²⁴ The explanatory memorandum also notes the ongoing issue of online child abuse material, noting that in September 2018, the Commissioner reported having undertaken more than 8,000 investigations dealing with 35,000 images and videos relating to this material.²⁵

1.14 Several key components of the proposed scheme—relating to the removal of intimate images posted without consent, and material constituting cyber-bullying of an Australian child—would appear to be clearly effective to achieve that objective and, considering the nature of the content being targeted, would likely constitute a

20 International Covenant on the Elimination of Racial Discrimination, article 4(a). Where each of the treaty provisions above refer to prohibition by law, and offence punishable by law, they refer to criminal prohibition. Although Australia has ratified these treaties, Australia has made reservations in relation to both the International Covenant on Civil and Political Rights and International Covenant on the Elimination of Racial Discrimination in relation to its inability to legislate for criminal prohibitions on race hate speech.

21 See, also, UN Special Rapporteur, F La Rue, *Annual Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion*, Human Rights Council, UN Doc A/HRC/14/23 (20 April 2010) [79(h)] available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/14/23 (accessed 4 November 2020).

22 Statement of compatibility, p. 56.

23 Statement of compatibility, p. 56.

24 Statement of compatibility, p. 53.

25 Explanatory memorandum, p. 16.

proportionate means by which to achieve it. The bill expressly provides that it does not apply to the extent that it would infringe any constitutional doctrine of implied freedom of political expression,²⁶ which is a useful safeguard. Further, with respect to public oversight of the Commissioner's functions, the bill requires the tabling of an annual report in Parliament.²⁷

1.15 However, the bill also seeks to deal with further distinct types of online content, which necessitates an analysis of whether the proposed regulation of access to that content would constitute a proportionate means by which to achieve the important objectives of this bill in each case. This requires consideration of: the extent of the interference with the right to freedom of expression; whether the proposed limitation is sufficiently circumscribed; the presence of sufficient safeguards; and whether any less rights restrictive alternatives could achieve the same stated objective.

Material constituting cyber-abuse of an Australian adult

1.16 Part 7 of the bill would facilitate the removal of online material where the Commissioner is satisfied that the material is or was 'cyber-abuse' material targeted at an Australian adult.²⁸ That is, it is material which: an ordinary reasonable person would conclude is likely intended to have an effect of causing 'serious harm' to a particular Australian adult;²⁹ and which an ordinary reasonable person in the position of the Australian adult would regard as being, in all the circumstances, 'menacing, harassing, or offensive'.³⁰ The term 'offensive' is not defined in the bill. However, clause 8 provides that in determining whether an ordinary reasonable person in the position of the particular Australian adult would regard particular material to be 'offensive' in all the circumstances, matters to be taken into account include: the standards of morality, decency and propriety generally accepted by reasonable adults; the literary, artistic or educational merit (if any) of the material; and the general character of the material (including whether it has a medical, legal or scientific character).³¹ The explanatory memorandum states that in assessing this, the Commissioner may consider the context in which the conduct occurs, including whether the person has been targeted because of a personal characteristic (such as their race, gender, mental health condition, or family violence situation).³² The

26 Part 16, clause 233.

27 Part 11, clause 183.

28 The term 'cyber-abuse material targeted at an Australian adult' is defined in Part 1, clause 7.

29 The term 'serious harm' is defined in clause 5 to mean serious physical harm or serious harm to a person's mental health (being serious psychological harm and serious distress), whether temporary or permanent.

30 Part 1, subclause 7(1).

31 Part 1, clause 8.

32 Explanatory memorandum, p. 70.

statement of compatibility further provides that this higher threshold for cyber-abuse materials (when compared with cyber-bullying material against children) recognises the higher level of resilience to be expected of an adult:

For adults, it is only when the material crosses a threshold well beyond reasonable commentary or expression of opinion and into the realm of intentional, serious harm, and being menacing, harassing or offensive, that the Bill provides a mechanism for that material to be taken down from a platform.³³

1.17 The term 'offensive' may be employed in relation to conduct with effects that range from slight to severe, which raises some questions as to the potential breath of materials which could be captured by this provision, as a matter of statutory interpretation. The right to freedom of expression, to be meaningful, protects both popular and unpopular expression and ideas, including expression that may be regarded as deeply offensive (so long as it does not constitute hate speech).³⁴ The term 'offensive' has been the subject of extensive consideration in existing areas of Australian law. The High Court of Australia has noted that, 'offensiveness is a protean concept which is not readily contained unless limited by a clear statutory purpose and other criteria of liability'.³⁵ It has further stated that the modern approach to interpretation—particularly in the case of general words—requires that the context be considered in the first instance: '[w]hilst the process of construction concerns language, it is not assisted by a focus upon the clarity of expression of a word to the exclusion of its context'.³⁶

1.18 In *Monis v R*, the High Court considered the meaning of the term 'offensive' within the context of the alleged offence of using a postal service in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.³⁷ In that instance, Justices Crennan, Kiefel and Bell guided that the terms 'menacing, harassing or offensive' must be considered together:

It is true that a communication which has the quality of being menacing or harassing can be seen to be personally directed and deliberately so. An offensive communication may have those qualities; it may

33 Statement of compatibility, p. 57.

34 See UN Human Rights Committee, *General Comment 34: Freedom of opinion and expression* (2011) [11].

35 *Monis v R; Droudis v R* [2013] HCR 4 [47] per French CJ. Gleeson CJ (dissenting) in *Coleman v Power* [2004] HCA 39 further commented that concepts of what is offensive will vary within time and place, and may be affected by the circumstances in which the relevant conduct occurs, at [12].

36 *Monis v R; Droudis v R* [2013] HCR 4 [309] (per Crennan, Kiefel and Bell JJ). See also *K & S Lake City Freighters Pty Ltd v Gordon & Gotch Ltd* (1985) 157 CLR 309 [315] per Mason J; and *Project Blue Sky Inc v Australian Broadcasting Authority* (1998) 194 CLR 355 [381].

37 Pursuant to section 471.12 of the *Criminal Code Act 1995*.

not...Importantly, the grouping of the three words and their subjection to the same objective standard of assessment for the purposes of the offences in s 471.12 suggests that what is offensive will have a quality at least as serious in effect upon a person as the other words convey. The words "menacing" and "harassing" imply a serious potential effect upon an addressee, one which causes apprehension, if not a fear, for that person's safety. For consistency, to be "offensive", a communication must be likely to have a serious effect upon the emotional well-being of an addressee.³⁸

1.19 Section 18C of the *Racial Discrimination Act 1975* similarly prohibits an act done on the basis of race or colour that is reasonably likely, in all the circumstances, to offend, insult, humiliate or intimidate. In this context, having had regard to the collective phrase 'offend, insult, humiliate or intimidate', Australian courts have considered that this establishes an objective test of whether the act is reasonably likely to have a 'profound and serious effect', in all the circumstances, and is not to be likened to mere slights.³⁹

1.20 This jurisprudence indicates that the term 'offensive' (which itself may be capable of capturing conduct with effects that range from slight to severe) should, where relevant, and as a matter of modern statutory interpretation, be read in relation to the surrounding terms in the statute. In this instance, the same interpretative approach would appear to also necessitate consideration of the intention to have the effect of causing 'serious harm' to a particular Australian adult. Accordingly, the definition of 'cyber-abuse material targeted at an Australian adult' may well be sufficiently constrained such that any interference on the right to freedom of expression with respect to this particular mechanism may be permissibly limited. Further, clause 7 would permit the development of further legislative rules, which would appear to enable the definition of cyber-abuse to be further narrowed in the future.⁴⁰

1.21 In addition, the Online Safety (Transitional Provision and Consequential Amendments) Bill 2021 seeks to increase the penalty for an offence of using a carriage service to menace, harass or cause offence, from three years imprisonment to five years imprisonment.⁴¹ The explanatory memorandum states that this offence captures conduct including serious cyber-abuse, including in cases where there is family violence, and that the increased penalty will ensure that community

38 *Monis v R; Droudis v R* [2013] HCR 4 [310].

39 *Creek v Cairns Post* [2001] FCA 1007 [16]. See also, *Bropho v Human Rights and Equal Opportunity Commission* (2004) 135 FCR 105 [131]; *Jones v Scully* (2002) 120 FCR 243 [102]; and *Eatock v Bolt* (2011) 197 FCR 261 at [267]-[268].

40 The statement of compatibility identifies that this is the intended purpose of subclause 7(c), relating to the definition of 'cyber-bullying material targeted at an Australian child'. See, p. 57.

41 See Criminal Code Act 1995, section 474.17.

expectations are met and such conduct is adequately deterred.⁴² In light of the judicial guidance as to the correct interpretation of the terms 'menacing, harassing or offensive' as set out at paragraph [1.18], it would appear that increasing the penalty for this offence may constitute a permissible limit on the right to freedom of expression.

Material relating to abhorrent violent conduct

1.22 Part 8 of the bill would enable the Commissioner to either request or require that an internet service provider (ISP) block access to material that promotes, incites, instructs or depicts 'abhorrent violent conduct',⁴³ if the Commissioner is satisfied that the availability of the material online is likely to cause significant harm to the Australian community.⁴⁴ This necessarily limits the right to freedom of expression (while also promoting the rights set out above). The bill provides that a blocking request or requirement may specify that an internet service block domain names, Uniform Resource Locators (URLs) or Internet Protocol (IP) addresses providing access to the material, and may remain in force for up to three months (subject to further renewal).⁴⁵ The term 'significant harm' is not defined in the bill, however in reaching this determination the Commissioner must have regard to the nature of the material, the number of end-users who are likely to access it, and any other matters they consider relevant.⁴⁶ Further, some materials would be exempt, and the Commissioner would have no power to request or require that such material be blocked (including material that must be available in order to monitor compliance with or enforce a law; material necessary for scientific, medical, academic or historical research; material that relates to a news report that is in the public interest and made by a person working in a professional capacity as a journalist; and where the accessibility of the material is for the purpose of lawfully advocating a change to laws or policies).⁴⁷

1.23 The explanatory memorandum states that this scheme is intended to protect the Australian community from the viral online distribution of terrorist and extreme violence material in the case of an 'online crisis event', such as the video created by the perpetrator of the March 2019 terrorist attack in New Zealand.⁴⁸ It states that it

42 Explanatory memorandum, pp. 11–12.

43 A person engages in 'abhorrent violent conduct' if they: engage in a terrorist act; murder (or attempt to murder) another person; or torture, rape or kidnap another person. *Criminal Code Act 1995*, section 474.32.

44 Part 8, clause 95.

45 Part 8, clauses 95 and 99.

46 Part 8, subclauses 95(4) and 99(4).

47 Part 8, clause 104.

48 Statement of compatibility, p. 54; and explanatory memorandum, p. 116.

is not intended for the Commissioner to be able to use this power for material that has limited availability or distribution.⁴⁹ It also states that given the requirement of the Commission to be satisfied that the availability of the material online is likely to cause significant harm to the Australian community, the scheme is not intended to capture certain content, such as footage of violent sporting events or medical procedures.⁵⁰ As noted above, the right to freedom of expression may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective. Part 8 is clearly intended to provide an important mechanism for the speedy removal of material relating to violent conduct with the potential to traumatise or radicalise those who view it. This would clearly constitute a very important and legitimate objective, and the measure would appear effective to achieve this objective.

1.24 However, some questions arise as to whether this scheme would constitute a proportionate means by which to achieve this objective, including questions as to the scope of the materials which would be exempt from this scheme under clause 104. Clause 104 provides that the Commissioner would not, for example, have the power to require that material depicting abhorrent violent conduct be blocked where it relates to a news report that is in the public interest, and was made by a person working in a professional capacity as a journalist. However, the term 'public interest' is undefined, and, noting that it may be subject to an evolving interpretation, it is not clear what matters (if any) the Commissioner would be required to have regard to in making this assessment. Further, this exemption only applies where the content was created by a person working in a professional capacity as a journalist. Given that it may not always be immediately apparent who made the material in question, it is not clear whether, for example, raw video footage of a violent conflict filmed by a non-journalist could be blocked on the basis that it is likely to cause significant harm to the Australian community, even if it may inform journalistic analysis of such conflict. This is a significant consideration with respect to a limitation on the right to freedom of expression, noting the particular importance placed on the role of a free press under human rights law.⁵¹ Further, while the Commissioner would have no power to block access to material where the accessibility is for the purpose of advocating the lawful procurement of a change to any matter established by law, policy or practice in Australia or overseas, it is not clear how this may be applied in practice (including where material could be accessed for a number of purposes). For example, it is not clear whether this

49 Explanatory memorandum, p. 116.

50 Explanatory memorandum, p. 117.

51 UN Human Rights Committee, *General comment no. 34, Article 19, Freedoms of opinion and expression* (2011) [13].

exemption would prevent the Commissioner from blocking video footage of violent police misconduct against a member of the public.

1.25 Questions also arise as to the breadth of what a blocking notice may require under Part 8. Subclauses 95(2) and 99(2) state that the blocking notice may request the provider to take one or more specified steps to disable access to the material. What those steps may be are not specified in the bill. Subclauses 95(2) and 99(2) set out examples of such steps (such as blocking domain names, URLs and IP addresses that provide access to the material), but these are not exhaustive lists. The explanatory memorandum states that it is intended for these powers to work in tandem with any protocol developed by the Commissioner describing how they will provide a blocking request or notice, how affected parties will be notified, and the process of removing blocks,⁵² however there is no such information on the face of the bill. The bill would require only that the Commissioner must have regard to whether their other powers could be used instead of the blocking power.⁵³ If requiring the removal of an individual piece of content (or class of content) would be effective to achieve the aims of the blocking notice, it is not clear if the Commissioner would only be empowered to require this or could still require the blocking of an entire domain or URL (noting that a website could host a wide range of unrelated material). This raises questions as to the scope of potential blocking requests or orders.

1.26 Finally, the bill states explicitly that procedural fairness does not need to be observed in issuing a blocking notice.⁵⁴ The explanatory memorandum explains that procedural fairness is excluded to enable the Commissioner to issue a request as soon as possible to quickly block harmful material.⁵⁵ While it is clear that giving ISPs and owners of a website a chance to make submissions regarding the action would delay the blocking process, it is not clear why Part 8 could not provide for the issue of an interim blocking notice for a short duration—with no requirement for procedural fairness—but which can be followed by a further blocking notice of longer duration. Procedural fairness could then be afforded when making the longer-term blocking notice, without compromising the objective of having the offending material urgently blocked. The exclusion of procedural fairness, and the opportunity to hear from affected parties as to the nature of the material to be blocked, may make it more likely that a broader range of material than is necessary may be blocked. Further, although the Commissioner would be empowered to revoke a blocking request or notice,⁵⁶ the bill provides no criteria on which this decision may be made, and there

52 Explanatory memorandum, p. 116

53 Part 8, subclauses 95(5) and 99(5).

54 Part 8, subclauses 95(3) and 99(3).

55 Explanatory memorandum, p. 117.

56 Part 8, clauses 97 and 101.

is no requirement in the bill that the Commissioner revoke the blocking notice or request should circumstances relevantly change prior to the expiration of the notice. The bill does provide for review of a decision to give a blocking notice by the Administrative Appeals Tribunal,⁵⁷ which is a useful safeguard in terms of providing access to external review. However, it is noted this would only take place after an internet service provider had already been required to comply with the blocking notice, and the right to freedom of expression had been limited.

1.27 In order to assess the proportionality of this measure with the right to freedom of expression, further information is required, in particular:

- (a) what is meant by the term 'significant harm' and what guidance would be provided to the Commissioner in determining what reaches the threshold of 'significant harm' (as opposed to 'harm') in practice;
- (b) whether material which could be used to inform journalistic analysis of violent incidents (for example, raw protest footage filmed by participants, or footage of violent police misconduct) but which was not itself made by a journalist, would be exempt from removal by the Commissioner;
- (c) what guidance would be provided to the Commissioner, and what factors would they take into consideration, in determining whether access to material is in the public interest;
- (d) what range of steps the Commissioner could specify in a blocking notice or request (beyond those examples in subclauses 95(2) and 99(2)), and what limits (if any) are there on the steps which the Commissioner could request or require;
- (e) why the bill does not specify that the Commissioner may require the removal of an individual piece of content (or class of content), rather than requiring the blocking of an entire domain or URL, where satisfied that this would be effective;
- (f) why it would not be as effective to provide for an interim blocking notice of short duration—with no requirement for procedural fairness—together with the power to issue a blocking notice of longer duration, but only where the internet service provider or other relevantly affected person has been provided with the opportunity to make a submission as to the content in question; and
- (g) why the Commissioner would not be required to revoke a blocking notice or request should circumstances relevantly change prior to its original expiration.

57 Part 16, subclause 220(13).

Regulation of online content - class 1 and 2 materials

1.28 Part 9 of the bill would enable the Commissioner to require that a social media service, electronic service, designated internet service, or a hosting service provider remove, or otherwise deny access to, two classes of material on their services:

- 'Class 1 material' refers to a film or publication (or the contents of such), computer game, or other material which has been refused classification (or classified 'RC') under the *Classification (Publications, Films and Computer Games) Act 1995*,⁵⁸ or which would likely be refused classification.⁵⁹
- 'Class 2 material' which refers to:
 - material that has been, or would likely be, classified X 18+ and category 2 restricted material (referred to in the explanatory memorandum as mainstream pornography);⁶⁰ and
 - material depicting violence, implied sexual violence, simulated sexual activity, coarse language, drug use and nudity that is not suitable for

58 A film, publication or computer game will be classified as 'RC' where it: describes, depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that it offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should not be classified; or describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not); or promotes, incites or instructs in matters of crime or violence. National Classification Code (May 2005), sections 2–4. With respect to films see also Guidelines for the Classification of Films 2012, which provides that a film will be classified RC where it contains bestiality; or gratuitous exploitative or offensive depictions of activity accompanied by fetishes or practices which are considered abhorrent.

59 Part 9, clause 106.

60 The catch-all term 'mainstream pornography' is used in the explanatory memorandum, at page 124, to refer to this content. That is, a film (or contents of), or another material, which has been, or would likely be, classified X 18+ (meaning that it contains real depictions of actual sexual activity between consenting adults in which there is no violence, no sexual violence, sexualised violence, coercion, sexually assaultive language, or fetishes or depictions which purposefully demean anyone involved in that activity for the enjoyment of viewers, in a way that is likely to cause offence to a reasonable adult; and which is unsuitable for a minor to see). Alternatively, a publication that is (or would be) classified 'Category 2 restricted' (meaning that it explicitly depicts sexual or sexually related activity between consenting adults in a way that is likely to cause offence to a reasonable adult; or depicts, describes or expresses revolting or abhorrent phenomena in a way that is likely to cause offence to a reasonable adult and is unsuitable for a minor to see or read). See, National Classification Code (May 2005).

persons under 18 years (hereafter referred to as 'less serious Class 2 material').⁶¹

1.29 In the case of Class 1 material (including, for example, child exploitation material), a person would be able to complain to the Commissioner if they had reason to believe that an end-user in Australia could access that content online, including via an instant messaging or SMS service.⁶² The Commissioner would be empowered to require that, within 24 hours of the notice: an online service take all reasonable steps to ensure the removal of that material (or cessation of its hosting);⁶³ an internet search engine service cease providing a link to the material;⁶⁴ or an app distribution service cease enabling Australian end-users from downloading an app that facilitates the posting of Class 1 material.⁶⁵

1.30 In the case of mainstream pornography, a person would be able to complain to the Commissioner if they had reason to believe that an end-user in Australia could access that content online, including via an instant messaging or SMS service,⁶⁶ regardless of whether or not access to that content was restricted in some way. The Commissioner would only be empowered to take action with respect to content that was posted on, or otherwise hosted by, a service from Australia. They could require that such a service must take all reasonable steps to ensure the removal of that material (or cessation of its hosting) within 24 hours.⁶⁷

1.31 As to less serious Class 2 material, a person would be able to complain to the Commissioner if they had reason to believe that an end-user in Australia could access that content online, including via an instant messaging or SMS service,⁶⁸ and that

61 That is, a film (or contents of), a computer game which has been, or would likely be classified R 18+ (meaning that it is unsuitable for viewing or playing by a minor); or a publication (or contents of) which has been (or would likely be) classified 'Category 1 restricted' (meaning that it explicitly depicts nudity, or describes or impliedly depicts sexual or sexually related activity between consenting adults, in a way that is likely to cause offence to a reasonable adult; or describes or expresses in detail violence or sexual activity between consenting adults in a way that is likely to cause offence to a reasonable adult; or is unsuitable for a minor to see or read). See, National Classification Code (May 2005).

62 Part 3, paragraph 38(1)(a).

63 Part 9, clauses 109–110.

64 Part 9, clause 124.

65 Part 9, clause 128.

66 Part 3, paragraph 38(1)(b).

67 Part 9, clause 114 and 120.

68 Part 3, subclause 38(2)

access was not subject to a 'restricted access system'.⁶⁹ The Commissioner would only be empowered to take action with respect to content that was posted on, or otherwise hosted by, a service from Australia. They could issue the service with a remedial notice, requiring that, within 24 hours, they take all reasonable steps to ensure that they either cease hosting the material, or that access to the material be subject to a restricted access system.⁷⁰

1.32 In addition to promoting the rights of women, the child and privacy (as set out above), blocking access to such material necessarily limits the right to freedom of expression. As noted above, the right to freedom of expression may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

1.33 The statement of compatibility states that this scheme deals with seriously harmful content, access to which, if unrestricted, would be harmful to Australians, particularly children.⁷¹ The objective of restricting access to seriously harmful content would likely be legitimate for the purposes of international human rights law.

1.34 It must then be demonstrated that these limitations are rationally connected to the objective sought to be achieved. The key question is whether the relevant measure is likely to be effective in achieving the objective being sought. With respect to the more serious materials within these two classes—including child abuse material, child sexual exploitation material, promotion of paedophile activity, and material advocating a terrorist activity—it is clear that restricting access to these materials would be effective to reduce the risk of harm caused by continued access to them, because those materials are themselves harmful to the viewer, and to persons involved in their production (for example, children being abused). However, it is not clear that other materials, particularly those that fall within Class 2 would necessarily be harmful to adult viewers. In particular, it is not clear that an Australian adult would necessarily experience any harm having viewed material depicting sexual activity between consenting adults,⁷² including materials constituting non-

69 Clause 108 provides that the Commissioner may, by legislative instrument, declare that a specified 'access-control system' is a restricted access system. Clause 5 defines an 'access-control system' as a system under which persons seeking access to the material have a password, or a PIN, or some other means of limiting access by other persons to the material.

70 Part 9, clause 120.

71 Statement of compatibility, p. 58.

72 In addition, clause 114 (removal notices with respect to mainstream pornography removal on a service provided from Australia) would facilitate the removal of pornography on a service provided in Australia. Consequently, it is not clear whether this power would have a disproportionate impact on sex worker and related businesses in Australia, and their capacity to work.

mainstream, yet still consensual, sexual content.⁷³ No information is provided to demonstrate that having access to mainstream pornography online, depicting sex between consenting adults, causes harm to adult Australians. Consequently, further information is required as to whether providing for the removal of content depicting sex between consenting adults from the internet would be effective to protect adults from some kind of harm. Further information is also required to demonstrate that where access to material is restricted, having this material available online could cause harm to Australian children.

1.35 As to whether this scheme would constitute a proportionate means by which to achieve its objective, it is necessary to consider: the extent of the interference with the right to freedom of expression; whether the proposed limitation is sufficiently circumscribed; the presence of sufficient safeguards; and whether any less rights restrictive alternatives could achieve the same stated objective. In this respect, it is significant that this scheme would apply to a broad range of content. Some of the materials would clearly have the capacity to cause harm to a viewer (for example, child exploitation material). However, it is not clear that other materials captured by this scheme (for example, pornography depicting consensual sex between adults) could cause harm to an adult viewer. The Commissioner would be empowered to require the removal of Class 1 and 2 materials, including mainstream pornographic content, material depicting nudity.⁷⁴ In light of the question at paragraph [1.34] as to what evidence there is that access to mainstream adult pornographic content exposes adults to harm, it is unclear why the Commissioner is not solely empowered to only require that mainstream pornographic material must be accessible via a restricted access system, rather than enabling its removal in its entirety, in order to achieve the objective of protecting Australians—and particularly children—from exposure to harmful sexual content.

1.36 Further, some questions arise as to whether the Commissioner's discretion to require the removal of materials could not be further curtailed, without reducing their capacity to achieve the stated objective. The bill could, for example, require that the Commissioner must consider the purpose for which that content was published (for example, an educative, academic, medical, or health-related purpose); whether it would be in the public interest to remove material (on the basis that it

73 Noting that this may necessitate a subjective judgment as to what is mainstream or otherwise harmful sexual activity. In this regard, questions also arise as to whether material which is, or would likely be, classified RC (that is, Class 1 material), could capture non-mainstream sex between consenting adults (that is, material which describes, depicts, expresses or otherwise deals with sex in such a way that it offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should not be classified).

74 Paragraphs 119(2)(f) and 120(1)(g) would, as matter of statutory interpretation, appear to permit the Commissioner to require that a service *either* restricted access to material behind a restricted access system *or* require that that it be removed.

may be unsuitable for a child to view, but may be reasonable for an adult to have access to); and how the interests of affected parties and end users would be affected. In addition, noting that the definition of a 'restricted access system' is potentially broad, it is not clear what kind of system the Commissioner could declare for the purposes of clause 108. This is relevant to the proportionality of this measure because if a system required, for example, the provision of personal information in order to log in, this may deter end-users in practice.

1.37 Lastly, while a decision by the Commissioner could be appealed to the Administrative Appeals Tribunal for review,⁷⁵ it would be less rights restrictive to provide for the issue of an interim removal, link-deletion, app removal, or remedial notice, followed by a further order only once the relevant service had been given the opportunity to make submissions as to the appropriateness of the content remaining accessible. As set out at paragraph [1.26], this would provide a mechanism for procedural fairness in practice.

1.38 In order to assess the proportionality of this measure with the right to freedom of expression, further information is required, and in particular:

- (a) what evidence demonstrates that the full range of materials which would fall within Classes 1 and 2 (in particular, material depicting consensual sex between adults) would be harmful to adult end-users;
- (b) why the Commissioner would be empowered to require the removal of mainstream pornography, rather than requiring that it must be accessible only via a restricted access system;
- (c) why the bill could not require that the Commissioner must consider the purpose for which that content was published (for example, an educative, academic, medical, or health-related purpose); whether it would be in the public interest to remove material (on the basis that it may be unsuitable for a child to view, but may be reasonable for an adult to have access to); and how the interests of affected parties and end users would be affected;
- (d) what types of systems the Commissioner could declare a 'restricted access system', and whether these would require the provision of personal information in order to log in; and
- (e) in order to ensure procedural fairness, why this scheme could not instead provide for the issue of an interim removal, link-deletion, app removal, or remedial notice, followed by a further order only once the relevant service had been given the opportunity to make submissions as to the appropriateness of the content remaining accessible.

75 Part 16, subclauses 220(11) and (14)–(16).

Committee view

1.39 The committee notes the Online Safety Bill 2021 seeks to create a new framework for ensuring online safety in Australia and provide a new legislative authority for the Australian eSafety Commissioner, empowering them to investigate complaints and objections in relation to harmful online content against children and adults, and to require that certain harmful content must be removed, or access to it disabled or restricted. The committee notes that the Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021 would repeal the existing legislative authority for the Commissioner, as well as increasing the criminal penalties associated with two offences for using a carriage service to menace, harass or cause offence.

1.40 The committee notes that, in doing so, the Online Safety Bill 2021 is likely to promote numerous human rights. The committee considers that ensuring the safety of Australians online is a significant and evolving challenge, and notes that some Australians—including women and children—are particularly vulnerable to harms online, including sexual exploitation. The committee notes that the extent of the eSafety Commissioner's work to date demonstrates the vital importance of their role, noting in particular that in September 2018, the eSafety Commissioner reported having undertaken more than 8,000 investigations into child abuse content, representing approximately 35,000 images and videos referred for removal. Consequently, the committee considers that this bill is likely to promote the rights of the child, including by protecting them from exposure to harmful materials online, and from cyber-bullying material. The committee also considers that the bill is likely to promote the right of women to be free from sexual exploitation, and the right to privacy and reputation, including by providing for the removal of cyber-abuse material targeting an Australian adult, and of non-consensual intimate images.

1.41 The committee also notes that, by regulating and disabling access to certain harmful online content, this bill necessarily engages and limits the right to freedom of expression. The committee notes that the right to freedom of expression is not absolute, and may be permissibly limited where a limitation addresses a legitimate objective, is rationally connected to (that is, effective to achieve) that objective, and a proportionate means of doing so. The committee considers that the bill clearly seeks to achieve the important and legitimate objective of enhancing online safety for Australian adults and children in a number of ways, including by providing for the speedy removal of intimate images posted without the subject's consent, or material which constitutes cyber-bullying of an Australian child, and cyber-abuse of an Australian adult. The committee considers that these measures in general appear to permissibly limit the right to freedom of expression.

1.42 However, the committee notes that some clarification is required as to the potential scope of information, and means of regulating access to it, in relation to

abhorrent online content, and some adult sexual content, in order to assess whether the proposed limitations with respect to blocking access to this content is proportionate to the objectives of the bill.

1.43 The committee has not yet formed a concluded view in relation to this matter. It considers further information is required to assess the human rights implications of this bill, and as such seeks the minister's advice as to the matters set out at paragraphs [1.27] and [1.38].

Disclosure of information about a complaint of cyber-bullying against children

1.44 As noted above, the bill would establish a complaints mechanism for material which an ordinary person would conclude is likely intended to have the effect of seriously threatening, intimidating, harassing or humiliating an Australian child.⁷⁶ Information gathered by the Commissioner in investigating this complaint can be disclosed to a number of specified bodies and persons, including to a teacher or school principal, or to a parent or guardian of an Australian child, if the Commissioner is satisfied the information will assist in the resolution of the complaint.⁷⁷

Preliminary international human rights legal advice

Rights of the child

1.45 Enabling the Commissioner to share information about a complaint of cyber-bullying with teachers, principals, parents and guardians, engages the rights of the child. Australia is required to ensure that, in all actions concerning children, the best interests of the child are a primary consideration.⁷⁸ This requires legislative bodies to systematically consider how children's rights and interests are or will be affected directly or indirectly by their decisions and actions.⁷⁹ Children also have the right to privacy.⁸⁰ States Parties are also required to assure to a child capable of forming his or her own views the right to express those views freely in all matters affecting the child.⁸¹ The views of the child must be given due weight in accordance with the age and maturity of the child.

76 Part 1, clause 30.

77 Part 15, clauses 213 and 214.

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

79 UN Committee on the Rights of Children, *General Comment 14 on the right of the child to have his or her best interest taken as primary consideration* (2013).

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

81 Convention on the Rights of the Child, article 12.

1.46 The statement of compatibility states that the bill generally supports the best interests of the child by providing mechanisms so that they are protected from seriously harmful content, and that it is designed to protect persons from exploitation, violence and abuse.⁸² In relation to this specific disclosure provision it recognises that it may limit the right to privacy, but notes:

Resolution of a complaint by teachers or principals, or parents or guardians, has advantages over resolution through the more formal regulatory channels available under the Bill, particularly dealing with instances of cyber-bullying that might be of a less serious nature. These clauses facilitate resolution of complaints in such a manner. By facilitating resolution of complaints outside of the more formal channels, the Bill is also intending to minimise the adverse impacts of its provisions on the right to freedom of expression, discussed above.⁸³

1.47 As such, it appears likely that these measures could have the effect of promoting the rights of the child, insofar as the disclosure may help to quickly resolve the cyberbullying complaint. However, if the personal information relating to the child's complaint is shared with teachers and principals, and parents and guardians (be it the parent or guardian of the complainant or the parent or guardian of the child accused of cyber-bullying), without the child's consent⁸⁴ and against their wishes, this may limit the child's right to privacy, the obligation to take into account the best interests of the child and their right to express their views in matters that affect them. Most of the rights of the child may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

1.48 It is clear that the objective of the measure is to assist in resolving complaints of cyber-bullying which would constitute a legitimate objective for the purposes of international human rights law, and disclosing information to teachers, principals, parents and guardians would appear to be rationally connected to this objective. A key aspect of whether a limitation on a right can be justified is whether the limitation is proportionate to the objective being sought. In this respect, it is necessary to consider a number of matters including whether there are sufficient safeguards and whether any less rights restrictive alternatives could achieve the same stated objective.

82 Statement of compatibility, p. 64.

83 Statement of compatibility, p. 61.

84 It is noted that clause 215 provides a separate ground for disclosure of information that relates to the affairs of a person if that person has consented to the disclosure, which indicates that consent is not a requirement for disclosure to teachers, principals, parents and guardians under clauses 213 and 214.

1.49 The bill provides that the Commissioner must, as appropriate, have regard to the Convention on the Rights of the Child in the performance of their functions.⁸⁵ This may operate to ensure the rights of the child are respected in practice.⁸⁶ However, it is not clear if this broad requirement to 'have regard to' the Convention when performing their functions, would require the Commissioner to consider the rights of the child as a primary consideration when considering whether to disclose information to teachers, principals, parents and guardians. It is also not clear whether it would require the Commissioner to give due weight to the child's wishes in accordance with the age and maturity of the child before authorising disclosure of the information.

1.50 In order to assess the compatibility of this measure with the rights of the child, further information is required as to:

- (a) whether the requirement for the Commissioner to have regard to the Convention on the Rights of the Child in the performance of their functions will require the Commissioner to consider the rights of the child as a primary consideration, and give due weight to the child's wishes in accordance with the age and maturity of the child, when considering whether to disclose information to teachers, principals, parents and guardians; and
- (b) whether the rights of the child would be better protected if clauses 213 and 214 were amended to expressly provide that the Commissioner may disclose information to teachers, principals, parents and guardians where to do so would be in the best interests of the child complainant and, after first giving due weight to the child's wishes in accordance with the age and maturity of the child.

Committee view

1.51 The committee notes that the bill would enable the Commissioner investigating a complaint of cyber-bullying against a child to disclose information gathered in investigating that complaint to teachers, school principals, parents or guardians, if satisfied the information will assist in the resolution of the complaint.

1.52 The committee considers that if the disclosure may help to quickly resolve the cyberbullying complaint, these powers could have the effect of promoting the rights of the child. However, the committee notes that if the personal information relating to the child's complaint is shared against the child's wishes this may limit the child's right to privacy, the obligation to take into account the best interests of the child and their right to express their views in matters that affect them. Many of

85 Part 1, clause 24.

86 Part 1, clause 24.

the rights of the child may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate.

1.53 The committee has not yet formed a concluded view in relation to this matter. It considers further information is required to assess the human rights implications of this measure, and as such seeks the minister's advice as to the matters set out at paragraph [1.50].

Disclosure of information to authorities of foreign countries

1.54 The bill also provides that any information obtained by the Commissioner using these new powers⁸⁷ can be disclosed to a number of listed authorities, including certain authorities of a foreign country where the Commissioner is satisfied that the information will enable or assist the foreign authority to perform or exercise their relevant functions or powers.⁸⁸ The relevant authorities of the foreign countries are those that are responsible for regulating matters or enforcing laws of that country relating to the safe use of certain internet services and material that is accessible to the end-users of certain internet services. The Commissioner may impose conditions to be complied with when disclosing such information.⁸⁹

Preliminary international human rights legal advice

Rights to privacy and life, and prohibition on torture, cruel, inhuman or degrading treatment or punishment

1.55 By authorising the disclosure of information obtained by the Commissioner, including personal information, to the authorities of foreign countries for the purpose of assisting them to perform or exercise any of their functions or powers, the measure engages and limits the right to privacy. 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.⁹⁰ It also includes the right to control the dissemination of information about one's private life.

87 Part 15, clause 207.

88 Part 15, paragraphs 221(1)(h) and (i).

89 Part 15, subclause 212(2).

90 International Covenant on Civil and Political Rights, article 17. Every person should be able to ascertain which public authorities or private individuals or bodies control or may control their files and, if such files contain incorrect personal data or have been collected or processed contrary to legal provisions, every person should be able to request rectification or elimination: UN Human Rights Committee, *General Comment No. 16: Article 17* (1988) [10]. See also, *General Comment No. 34 (Freedom of opinion and expression)* (2011) [18].

1.56 The right to privacy may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective. The statement of compatibility acknowledges that the general disclosure powers in clause 212 engage the right to privacy (without specifically referring to the disclosure to the authorities of foreign countries). It states that this provision is necessary to allow each of the listed authorities to 'function to its maximum extent to protect the best interests of affected children and victims of cyber-abuse'.⁹¹ Enhancing the ability of foreign authorities to protect the interests of children and victims of cyber-abuse would appear to constitute a legitimate objective for the purpose of international human rights law, and authorising the sharing of information obtained by the Commissioner would appear to be rationally connected to that objective. However, questions remain as to whether the measure is proportionate to achieving that objective.

1.57 In order to be proportionate, a limitation on the right to privacy should only be as extensive as is strictly necessary to achieve its legitimate objective and must be accompanied by appropriate safeguards.⁹² The statement of compatibility states that to ensure adequate protection of privacy, clause 212 empowers the Commissioner to impose conditions to be complied with in relation to information disclosed under this clause, which 'may include, for example, conditions that prevent further disclosure to third parties'.⁹³ This may operate to help to safeguard the right to privacy in practice. However, the effectiveness of this as a safeguard will likely depend on the specific conditions (particularly whether they include privacy protections) and their enforceability. In addition, the bill provides only that the Commissioner 'may' impose conditions in relation to the information disclosed – there is no legislative requirement that privacy protections are required before information is disclosed. It is noted that Australian privacy protections would not apply once the information is disclosed to the foreign authority.

1.58 In addition, to the extent that the measure would authorise the disclosure of personal information to foreign authorities responsible for enforcing laws of the foreign country, where this may be used to investigate and convict a person of an offence to which the death penalty applies, the right to life may be engaged and limited. The right to life imposes an obligation on Australia to protect people from being killed by others or identified risks.⁹⁴ While the International Covenant on Civil

91 Statement of compatibility, p. 61.

92 The United Nations (UN) Human Rights Committee has stated that legislation must specify in detail the precise circumstances in which interferences with privacy may be permitted: *NK v Netherlands*, UN Human Rights Committee Communication No.2326/2013 (2018) [9.5].

93 Statement of compatibility, p. 61.

94 International Covenant on Civil and Political Rights, article 6. The right should not be understood in a restrictive manner: UN Human Rights Committee, *General Comment No. 6: article 6 (right to life)* (1982) [5].

and Political Rights does not completely prohibit the imposition of the death penalty, international law prohibits states which have abolished the death penalty (such as Australia) from exposing a person to the death penalty in another state. This includes prohibiting the provision of information to other countries that may use that information to investigate and convict someone of an offence to which the death penalty applies.⁹⁵ Additionally, it is not clear if sharing information with the authorities of certain foreign countries could risk exposing a person to torture or cruel, inhuman or degrading treatment or punishment. Australia has an obligation not to subject any person to torture or to cruel, inhuman or degrading treatment or punishment.⁹⁶ Under international law the prohibition on torture is absolute and can never be subject to permissible limitations.⁹⁷

1.59 The statement of compatibility does not acknowledge that the measure may engage and limit the right to life or have implications for the prohibition against torture or cruel, inhuman or degrading treatment or punishment, and so does not provide an assessment of whether the measure is compatible with these rights. In assessing whether the measure is compatible with these rights, the scope of personal information that may be disclosed is relevant as well as whether there are safeguards in place to ensure that information is not shared with the authority of a foreign country in circumstances that could expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment.

1.60 In order to assess the compatibility of this measure with human rights, further information is required as to:

- (a) what is the nature and scope of personal information that is authorised to be disclosed to the authority of a foreign country;
- (b) what conditions is it expected the Commissioner will impose on the disclosure of information with the authority of a foreign country and what are the consequences, if any, of that authority failing to comply

95 Second Optional Protocol to the International Covenant on Civil and Political Rights. In 2009, the United Nations Human Rights Committee stated its concern that Australia lacks 'a comprehensive prohibition on the providing of international police assistance for the investigation of crimes that may lead to the imposition of the death penalty in another state', and concluded that Australia should take steps to ensure it 'does not provide assistance in the investigation of crimes that may result in the imposition of the death penalty in another State': UN Human Rights Committee, *Concluding observations on the fifth periodic report of Australia*, CCPR/C/AUS/CO/5 (2009) [20].

96 International Covenant on Civil and Political Rights, article 7; and Convention against Torture and other Cruel, Inhuman, Degrading Treatment or Punishment, articles 3–5. See also the prohibitions against torture under Australian domestic law, for example the *Criminal Code Act 1995*, Schedule 1, Division 274.

97 Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment, article 4(2); UN Human Rights Committee, *General Comment 20: Article 7 (1992)* [3].

with those conditions, particularly where an individual's right to privacy is not protected;

- (c) why there is no requirement in the bill requiring that the Commissioner, when disclosing information to a foreign country, must impose conditions in relation to privacy protections around the handling of personal information, and protection of personal information from unauthorised disclosure;
- (d) what is the level of risk that the disclosure of personal information could result in: the investigation and conviction of a person for an offence to which the death penalty applies in a foreign country; and/or a person being exposed to torture or cruel, inhuman or degrading treatment or punishment in a foreign country; and
- (e) what, if any, safeguards are in place to ensure that information is not shared with the authority of a foreign country in circumstances that could expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment, including:
 - (i) the approval process for authorising disclosure;
 - (ii) the availability of any guidelines as to when disclosure would not be appropriate in certain cases and to certain countries; and
 - (iii) whether there will be a requirement to decline to disclose information where there is a risk that it may expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment.

Committee view

1.61 The committee notes that the bill provides that any information obtained by the Commissioner using the powers under the bill can be disclosed to a number of listed authorities, including certain authorities of a foreign country where the Commissioner is satisfied that the information will enable or assist the foreign authority to perform or exercise certain regulatory or enforcement functions or powers.

1.62 The committee notes that authorising the disclosure of this information, which may include personal information, to the authorities of foreign countries engages and limits the right to privacy. The right to privacy may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate. The committee considers that enhancing the ability of foreign authorities to protect the interests of children and victims of cyber-abuse constitutes a legitimate objective, and authorising the sharing of information obtained by the Commissioner may be effective to achieve that important objective. However, the committee notes that some questions remain as to whether the measure is proportionate to achieving that objective.

1.63 The committee also notes that to the extent that the measure would authorise the disclosure of personal information to foreign authorities responsible for enforcing laws of the foreign country, where this may be used to investigate and convict a person of an offence to which the death penalty applies, the right to life may be engaged and limited. It is also not clear if sharing information with the authorities of certain foreign countries could risk exposing a person to torture or cruel, inhuman or degrading treatment or punishment.

1.64 The committee has not yet formed a concluded view in relation to this matter. It considers further information is required to assess the human rights implications of this measure, and as such seeks the minister's advice as to the matters set out at paragraph [1.60].

Substantial civil penalties

1.65 In setting out a regulatory framework for online safety, the bill creates several civil penalty provisions for a failure to comply with the Commissioner's orders. Many of these civil penalties are directed to social media and internet search providers, but others would apply to individual members of the public. For example, a person who posted an intimate image of a person without their consent, or refused to comply with a removal notice to remove that image, would be liable to up to 500 penalty units (or \$111,000).⁹⁸ Similarly, a person who posts cyber-abuse material targeted at an Australian adult who does not comply with a removal notice would be liable to up to 500 penalty units.⁹⁹ In addition, a person who refuses or fails to answer a question, give evidence or produce documents when required may be subject to up to 100 penalty units (or \$22,200).

Preliminary international human rights legal advice

Criminal process rights

1.66 By introducing civil penalties for breaches of certain provisions, this measure may engage criminal process rights. This is because certain civil penalties may, depending on the context, be regarded as criminal for the purposes of international human rights law.

1.67 In assessing whether a civil penalty may be considered criminal, it is necessary to consider:

- the domestic classification of the penalty as civil or criminal (although the classification of a penalty as 'civil' is not determinative as the term 'criminal' has an autonomous meaning in human rights law);

98 See Part 6, clauses 75, 79 and 80. The current penalty unit is \$222, see *Crimes Act 1914*, section 4AA.

99 See Part 7, clauses 89 and 91.

- the nature and purpose of the penalty: a civil penalty is more likely to be considered 'criminal' in nature if it applies to the public in general rather than a specific regulatory or disciplinary context, and where there is an intention to punish or deter, irrespective of the severity of the penalty; and
- the severity of the penalty.

1.68 The statement of compatibility notes that the civil penalties are not classified as criminal and do not impose criminal liability, nor do they carry the possibility of imprisonment. The statement of compatibility states that the purpose of the civil penalties is to encourage compliance with a removal notice or remedial direction given to the person. It states that the amount of 500 penalty units reflects the significant harm and distress that can be caused to a person for failing to remove material subject to the removal notice. It also notes that the court, when considering the amount of the penalty to be imposed, has a discretion to not impose the full 500 penalty units in relation to a contravention.¹⁰⁰

1.69 However, while the court retains a discretion as to the amount of the penalty to impose, the legislation itself would allow the imposition of a penalty of up to 500 penalty units. Noting that the provisions could apply to the public at large, and do not apply in a specific regulatory or disciplinary context, a penalty of up to \$111,000 is significant. It is noted that under international human rights law, even if a penalty is not considered 'criminal' separately under steps two or three, it may still be considered 'criminal' where the nature and severity of the penalty are cumulatively considered.

1.70 If the civil penalty provisions were considered to be 'criminal' for the purposes of international human rights law, this does not mean that the relevant conduct must be turned into a criminal offence in domestic law nor does it mean that the civil penalty is illegitimate. Instead, it means that the civil penalty provisions in question must be shown to be consistent with the criminal process guarantees set out in article 14 of the International Covenant on Civil and Political Rights, including the right not to be tried twice for the same offence,¹⁰¹ and the right to be presumed innocent until proven guilty according to law.¹⁰² In this regard, as the statement of compatibility does not recognise that the penalties may be regarded as 'criminal' for the purposes of international human rights law, it provides no information as to whether the penalties would, in all instances, be consistent with these criminal process guarantees.

100 Statement of compatibility, p. 62.

101 International Covenant on Civil and Political Rights, article 14(7).

102 International Covenant on Civil and Political Rights, article 14(2).

Committee view

1.71 The committee notes that the bill seeks to introduce civil penalties for a failure to comply with the Commissioner's orders. While many of the civil penalties are directed to social media and internet search providers, others would apply to individual members of the public and would be up to 500 civil penalty units (or up to \$111,000).

1.72 The committee notes that depending on the context in which they appear, civil penalty provisions can engage criminal process rights if they are considered 'criminal' in nature for the purposes of international human rights law. Significant considerations are whether the penalties apply to the public in general and the severity of the penalty.

1.73 In this case, noting that the penalties apply to the public at large, and a \$111,000 penalty may be significant to many individuals, there is a risk that these penalties may be considered to be 'criminal' penalties under international human rights law. This does not mean that the relevant conduct must be turned into a criminal offence in domestic law nor does it mean that the civil penalty is illegitimate. Instead, it means that the civil penalty provisions in question must be shown to be consistent with criminal process rights, including the right not to be tried twice for the same offence, and the right to be presumed innocent until proven guilty according to law. It is not clear whether these civil penalty provisions would meet these standards.

1.74 The committee draws these human rights concerns to the attention of the minister and the Parliament.

Social Services Legislation Amendment (Strengthening Income Support) Bill 2021¹

Purpose	<p>This bill seeks to amend the <i>Social Security Act 1991</i> to:</p> <ul style="list-style-type: none"> • increase the maximum basic rates of working age social security payments by \$50 per fortnight; • extend until 30 June 2021 the criteria for a person to qualify for youth allowance (other) or jobseeker payment in circumstances where the person is in quarantine or self-isolation or caring for a family member or household member in quarantine or self-isolation due to COVID-19; • extend until 30 June 2021 the waiver of the ordinary waiting period for jobseeker payment and youth allowance (other); • extend until 30 June 2021 the portability period for certain age pensioners and recipients of the disability support pension (for severely disabled persons) unable to return to, or depart from, Australia within 26 weeks due to the impact of COVID-19; and • permanently increase the ordinary income-free area for jobseeker payment, youth allowance (other), parenting payment partnered and related payments to \$150 per fortnight
Portfolio	Social Services
Introduced	House of Representatives, 25 February 2021
Rights	Social security; adequate standard of living

Maximum basic rates of working age social security payments

1.75 This bill seeks to increase the maximum basic rates of working age social security payments by \$50 per fortnight from 1 April 2021, when the current COVID-

1 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Social Services Legislation Amendment (Strengthening Income Support) Bill 2021, *Report 3 of 2021*; [2021] AUPJCHR 29.

19 social security supplement ceases.² The proposed increase would apply to recipients of the jobseeker payment, youth allowance, youth disability support pension, parenting payment, austudy, partner allowance and widow allowance.³ The bill also proposes to extend from 1 April 2021 to 30 June 2021 the temporary COVID-19 altered provisions relating to youth allowance and jobseeker qualification (where the person is in quarantine or self-isolation or caring for a family or household member in quarantine or self-isolation due to COVID-19); waivers of the ordinary waiting period; and the discretion to extend the portability period (where specified recipients have travelled overseas and are unable to return to Australia because of the COVID-19 pandemic).⁴ Additionally, the bill seeks to permanently increase the ordinary

income-free area for jobseeker, youth allowance (other) and parenting payments as well as provide that the jobseeker income free area will no longer be indexed.⁵

Preliminary international human rights legal advice

Rights to social security and adequate standard of living

1.76 By increasing the maximum basic rate of working age social security payments by \$50 per fortnight on an ongoing basis, and extending the temporary COVID-19 altered provisions to 30 June 2021, these measures, taken alone, engage and promote the right to social security and the right to an adequate standard of living. The right to social security 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, in particular the right to an adequate standard of living.⁶ The right to an adequate standard of living requires Australia to take steps to ensure the availability, adequacy and accessibility of food,

2 Schedule 1, items 1–10; explanatory memorandum, p. 2. The COVID-19 supplement was originally introduced at a rate of \$550 per fortnight from 27 April to 24 September 2020. The supplement was subsequently extended for a further three months at \$250 per fortnight, expiring on 31 December 2020. The current COVID-19 supplement, paid at a rate of \$150 per fortnight, is in effect from 1 January to 31 March 2021. See *Coronavirus Economic Response Package Omnibus Act 2020*; Social Security (Coronavirus Economic Response—2020 Measures No. 14) Determination 2020; Social Security (Coronavirus Economic Response—2020 Measures No. 16) Determination 2020.

3 The Explanatory memorandum, p. 2, states that recipients of partner allowance and widow allowance will also receive the same increases to their rate of jobseeker before these payments cease on 1 January 2022. Equivalent changes will also be made to ABSTUDY living allowance.

4 Schedule 1, items 13–20, 34–39

5 Schedule 1, items 21–32.

6 International Covenant on Economic, Social and Cultural Rights, article 9. See also, UN Economic, Social and Cultural Rights Committee, *General Comment No. 19: The Right to Social Security* (2008).

clothing, water and housing for all people in Australia, and also imposes on Australia the obligations listed above in relation to the right to social security.⁷ The statement of compatibility identifies this, and notes that the increased payments have a flow-on effect to the children of recipients by increasing financial support for families, thereby also promoting the rights of the child.⁸

1.77 As a party to the International Covenant on Economic, Social and Cultural Rights, Australia has an obligation to take steps towards achieving the progressive realisation of economic, social and cultural rights. It also has a corresponding duty to refrain from taking unjustified retrogressive measures, or backwards steps with respect to their realisation.⁹ As a matter of law, this bill provides for a \$50 fortnightly increase to the maximum basic rate of working age social security payments. This increase would take effect from 1 April 2021, when the current COVID-19 supplement, paid at a rate of \$150 per fortnight, ceases.¹⁰ As such, the permanent increase to the basic rate may be seen to be a new measure that helps to progressively realise the rights to social security and an adequate standard of living. However, the recipients to whom this \$50 fortnightly increase would apply will, in practice, receive \$100 less per fortnight than they previously received with the COVID-19 supplement. This raises questions as to whether this may constitute a backwards step in the realisation of the rights to social security and an adequate standard of living as a matter of international human rights law.

1.78 The United Nations (UN) High Commissioner for Human Rights has noted that a retrogressive measure may be one that indirectly 'leads to backward movement in the enjoyment of the rights recognized in the Covenant'.¹¹ Accordingly, in assessing whether a measure may be retrogressive, it is relevant to consider the context in which the relevant law is being implemented, the impact it will have on individuals, and the effect it will have on their human rights overall. In this case, while the increase to the maximum basic rate of working age social security payments is, taken alone, a rights-enhancing measure, considering the effect of this measure in context, notably its commencement when the temporary COVID-19

7 International Covenant on Economic, Social and Cultural Rights, article 11.

8 Statement of compatibility, pp. 13–14.

9 International Covenant on Economic, Social and Cultural Rights, article 2. UN Committee on Economic, Social and Cultural Rights, *General Comment No. 3: The nature of States parties obligations (Art. 2, par. 1)* (1990) [9].

10 Explanatory memorandum, p. 2. The Social Security (Coronavirus Economic Response—2020 Measures No. 16) Determination 2020 provided for the payment of the COVID-19 supplement at a rate of \$150 per fortnight from 1 January 2021 to 31 March 2021. The Parliamentary Joint Committee on Human Rights previously commented on this instrument in *Report 2 of 2021*, pp. 54–57.

11 See, UN High Commissioner for Human Rights, *Report on austerity measures and economic and social rights*, E/2013/82 (7 May 2013), p. 11.

supplement ceases, there is a risk that this measure may be retrogressive in relation to the realisation of the rights to social security and an adequate standard of living. This is because in the context of the removal of the COVID-19 supplement – albeit noting that the supplement was always intended to be temporary – the practical effect of the measure will be an overall reduction of \$100 per fortnight in the rate of social security payments received by relevant recipients. If this were to be considered retrogressive, it may be permissible under international human rights law providing that it addresses a legitimate objective, is rationally connected to that objective and is a proportionate way to achieve that objective.

1.79 The UN Committee on Economic, Social and Cultural Rights has advised that if any deliberately retrogressive measures are taken with respect to a right, the State party has the burden of proving that they have been introduced 'after the most careful consideration of all alternatives' and that 'they are duly justifiable by reference to the totality of the rights provided for in the Covenant, in the context of the full use of the maximum available resources of the State party'.¹² It is not entirely clear whether the increase to the working age social security payments in the context of the removal of the COVID-19 supplement would constitute a retrogressive measure as a matter of international human rights law. However, noting that there is a risk that it might, it would be necessary to consider whether the burden of proof referred to by the UN Committee on Economic, Social and Cultural Rights has been met. In light of this, it is difficult to assess the compatibility of this measure, because the statement of compatibility does not address whether the measure was introduced after consideration of all alternatives, nor does it consider the practical impact of the measure on the rights of social security recipients, particularly whether

12 UN Committee on Economic, Social and Cultural Rights, *General Comment 19: the right to social security* (2008) [42]: 'There is a strong presumption that retrogressive measures taken in relation to the right to social security are prohibited under the Covenant. If any deliberately retrogressive measures are taken, the State party has the burden of proving that they have been introduced after the most careful consideration of all alternatives and that they are duly justified by reference to the totality of the rights provided for in the Covenant, in the context of the full use of the maximum available resources of the State party. The Committee will look carefully at whether: (a) there was reasonable justification for the action; (b) alternatives were comprehensively examined; (c) there was genuine participation of affected groups in examining the proposed measures and alternatives; (d) the measures were directly or indirectly discriminatory; (e) the measures will have a sustained impact on the realization of the right to social security, an unreasonable impact on acquired social security rights or whether an individual or group is deprived of access to the minimum essential level of social security; and (f) whether there was an independent review of the measures at the national level'.

the proposed maximum basic rate is adequate, in all circumstances, to meet the basic costs of living for recipients and their dependents.¹³

Committee view

1.80 The committee notes that this bill seeks to increase the maximum basic rates of working age social security payments by \$50 per fortnight as well as extend from 1 April 2021 to 30 June 2021 the temporary COVID-19 altered provisions relating to youth allowance and jobseeker qualifications; ordinary waiting periods; and the portability period. The committee notes that this increase in social security payments will take effect on 1 April 2021, when the current COVID-19 supplement ceases. The committee considers that the \$50 fortnightly increase to the working age payments, which is designed to provide financial assistance to vulnerable groups, taken alone, promotes the rights to social security and an adequate standard of living.

1.81 The committee notes the advice that although the increase is, taken alone, a rights-enhancing measure, considering the effect of this measure in context, notably its commencement when the temporary COVID-19 supplement ceases, there is some risk that this measure in context may constitute a retrogressive measure (that is, a backwards step) in relation to the realisation of the rights to social security and an adequate standard of living. Retrogressive measures, a type of limitation, may be permissible under international human rights law if they are shown to be reasonable, necessary and proportionate. If this were found to constitute a retrogressive measure, the statement of compatibility would need to provide an analysis as to whether this measure would be permissible under international human rights law.

1.82 Noting that it is not entirely clear whether the \$50 fortnightly increase to the working age social security payments in the context of the removal of the \$150 fortnightly COVID-19 supplement would constitute a retrogressive measure as a matter of international human rights law, the committee makes no concluded view in relation to this but draws the above advice to the attention of the minister and the Parliament.

13 The UN Committee on Economic, Social and Cultural Rights has noted that social security benefits must be adequate in amount and duration having regard to the principle of human dignity, so as to avoid any adverse effect on the levels of benefits and the form in which they are provided. It stated that the 'adequacy criteria should be monitored regularly to ensure that beneficiaries are able to afford the goods and services they require to realize their Covenant rights': UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The Right to Social Security* (2008) [22]. It is noted that the Parliamentary Joint Committee on Human Rights has previously questioned the adequacy of (what was then) Newstart (now Jobseeker) in meeting the minimum requirements of the right to an adequate standard of living, see *Social Security Legislation Amendment (Fair Incentives to Work) Act 2012 – Final Report* (March 2013), pp. 28–30.

Bills and instruments with no committee comment¹

1.83 The committee has no comment in relation to the following bills which were introduced into the Parliament between 22 to 25 February 2021. This is on the basis that the bills do not engage, or only marginally engage, human rights; promote human rights; and/or permissibly limit human rights:²

- Australian Local Power Agency Bill 2021;
- Australian Local Power Agency (Consequential Amendment) Bill 2021;
- Ending Indefinite and Arbitrary Immigration Detention Bill 2021;
- Environment Protection and Biodiversity Conservation Amendment (Standards and Assurance) Bill 2021;
- Northern Australia Infrastructure Facility Amendment (Extension and Other Measures) Bill 2021;
- Private Health Insurance Legislation Amendment (Age of Dependents) Bill 2021;
- Special Recreational Vessels Amendment Bill 2021; and
- Work Health and Safety Amendment (Norfolk Island) Bill 2021.

1.84 The committee has examined the legislative instruments registered on the Federal Register of Legislation between 28 January and 18 February 2021.³ The committee has determined not to comment on the instruments from this period on the basis that the instruments do not engage, or only marginally engage, human rights; promote human rights; and/or permissibly limit human rights.

1 This section can be cited as Parliamentary Joint Committee on Human Rights, Bills and instruments with no committee comment, *Report 3 of 2021*; [2021] AUPJCHR 30.

2 Inclusion in the list is based on an assessment of the bill and relevant information provided in the statement of compatibility accompanying the bill. The committee may have determined not to comment on a bill notwithstanding that the statement of compatibility accompanying the bill may be inadequate.

3 The committee examines all legislative instruments registered in the relevant period, as listed on the Federal Register of Legislation. To identify all of the legislative instruments scrutinised by the committee during this period, select 'legislative instruments' as the relevant type of legislation, select the event as 'assent/making', and input the relevant registration date range in the Federal Register of Legislation's advanced search function, available at: <https://www.legislation.gov.au/AdvancedSearch>.

Chapter 2

Concluded matters

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

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

Bills

Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill 2020²

<p>Purpose</p>	<p>This bill seeks to amend various Acts relating to migration and Australian citizenship to:</p> <ul style="list-style-type: none"> • provide a framework to protect disclosure of confidential information provided by gazetted law enforcement and intelligence agencies for consideration in visa decisions or citizenship decisions made on character grounds; • enable the minister to disclose confidential information to a court for the purposes of proceedings before the court; • allow the minister to issue a non-disclosure certificate on public interest grounds in relation to information relating to a decision made under the <i>Australian Citizenship Act 2007</i> where that decision is reviewable by the Administrative Appeals Tribunal; and • make it an offence for Commonwealth officers to disclose unauthorised confidential information relating to visa and citizenship decisions
<p>Portfolio</p>	<p>Home Affairs</p>

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

2 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill, *Report 3 of 2021*; [2021] AUPJCHR 31.

Introduced	House of Representatives, 10 December 2020
Rights	Fair hearing; prohibition against expulsion of aliens without due process

2.3 The committee requested a response from the minister in relation to the bill in [Report 1 of 2020](#).³

Protected information framework

2.4 The bill seeks to amend the *Migration Act 1958* (Migration Act) and the *Australian Citizenship Act 2007* (Citizenship Act), and make consequential amendments to other laws, for the purposes of introducing a 'protected information framework'. The framework would protect disclosure of confidential information⁴ provided by intelligence and law enforcement agencies where the information is used for decisions made to refuse or cancel a visa on character grounds; or revoke or set aside such decisions; or decisions made to refuse, cancel, revoke or cease citizenship.⁵ The bill would prohibit an officer to whom confidential information is communicated from disclosing that information to another person, except in very limited circumstances, or being required to produce or give the information to a court, tribunal, parliament or parliamentary committee.⁶ The bill would make unauthorised disclosure of confidential information an offence, carrying a penalty of 2 years' imprisonment.⁷

2.5 The bill would allow the minister, in specified circumstances, to declare that confidential information be disclosed to a specified minister, Commonwealth officer, court or tribunal.⁸ Where information is disclosed in these circumstances, the receiving officer or member of a tribunal must not onwards disclose the information

3 Parliamentary Joint Committee on Human Rights, *Report 1 of 2020* (3 February 2021), pp. 7-20.

4 Confidential information means information communicated to an authorised Commonwealth officer by a gazetted agency on the condition that it be treated as confidential information and is relevant to the exercise of a specified power, including refusing, cancelling or revoking citizenship or citizenship cessation: Schedule 1, item 3, proposed section 52A. See also Schedule 1, item 9, proposed substituted section 503A (in relation to migration matters).

5 Schedule 1, item 3, proposed section 52A and item 9, proposed section 503A.

6 Schedule 1, item 3, proposed subsections 52A(2) and (3) and item 9, proposed subsections 503A(2) and (3).

7 Schedule 1, item 3, proposed subsection 52A(6) and item 9, proposed subsection 503A(6).

8 Schedule 1, item 3, proposed section 52B and item 9, proposed section 503B.

to any other person. In consideration or exercise of this power by the minister, the bill states that the rules of natural justice would not apply.⁹

2.6 Additionally, the bill would allow the High Court, Federal Court of Australia or Federal Circuit Court to order that confidential information be produced to the court if the information was supplied by law enforcement or intelligence agencies and the information is for the purpose of the substantive proceedings.¹⁰ If information is ordered to be produced, any party to proceedings may make submissions concerning how the court should use the information, including any weight to be given to the information and the impact of disclosing the information on the public interest.¹¹ However, a party can only make submissions or tender evidence with respect to the information if they are lawfully aware of the content of the information.¹² The bill would require the court to order that any party which does not qualify to make submissions relating to the information must be excluded from the hearing of those submissions, including the applicant and their legal representative.¹³ After considering the information and any submissions, the court would be required to make a determination as to whether disclosing the information would create a real risk of damage to the public interest and, if so, the court must not disclose the information to any person, including the applicant and their legal representative.¹⁴ In deciding whether such a risk exists, the court would be required to have regard to the list of matters set out in the bill (and only those matters), which includes the protection and safety of informants; Australia's relations with other countries; Australia's national security; and any other matters specified in regulations.¹⁵ The bill would permit the court to give such weight to the information as it considers appropriate in the circumstances, having regard to any submission made regarding the use of the information.¹⁶

2.7 Schedule 2 of the bill would also establish a new framework for the management of disclosure of certain sensitive and confidential information to, and by, the Administrative Appeals Tribunal (AAT). The secretary of the Department would be prohibited from giving a document or protected information to the AAT in

9 Schedule 1, item 3, proposed subsection 52B(9) and item 9, proposed subsection 50BA(9).

10 Schedule 1, item 3, proposed subsection 52C(1) and item 9, proposed subsection 503C(1).

11 Schedule 1, item 3, proposed subsection 52C(2) and item 9, proposed subsection 503C(2).

12 Schedule 1, item 3, proposed subsection 52C(3) and item 9, proposed subsection 503C(3). A person must not become aware of the content of the information unlawfully or by way of an action for breach of confidence.

13 Schedule 1, item 3, proposed subsection 52C(4) and item 9, proposed subsection 503C(4).

14 Schedule 1, item 3, proposed subsections 52C(5)–(6) and item 9, proposed subsections 503C(5)–(6).

15 Schedule 1, item 3, proposed subsection 52C(5) and item 9, proposed subsection 503C(5).

16 Schedule 1, item 3, proposed subsection 52C(7) and item 9, proposed subsection 503C(7).

relation to the AAT's review of a decision if the minister certifies that disclosing the document or information would be contrary to the public interest because it would prejudice the security, defence or international relations of Australia, or involve the disclosure of cabinet deliberations or decisions.¹⁷ Where a document or information has been given to the AAT and the minister has certified that disclosing that information would be contrary to the public interest, or the information was given to the minister in confidence, the AAT may disclose the information, including to the applicant, if it thinks it appropriate to do so having regard to any advice given to it by the secretary. If the information is disclosed, the AAT would be required to give a direction prohibiting or restricting the publication or other disclosure of that information if it is in the public interest to prohibit or restrict disclosure.¹⁸

Summary of initial assessment

Preliminary international human rights legal advice

Right to a fair hearing and prohibition against expulsion of aliens without due process

2.8 As regards decisions relating to Australian citizens, the measure appears to engage and limit the right to a fair hearing to the extent that it would restrict such persons from accessing confidential information on which the decision was based and exclude such persons from making submissions relating to the use of that information in proceedings.¹⁹ Article 14(1) of the International Covenant on Civil and Political Rights requires that in the determination of a person's rights and obligations in a 'suit at law', everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law.²⁰ The concept of 'suit at law' encompasses judicial procedures aimed at determining rights and obligations, equivalent notions in the area of administrative law and also extends to other procedures assessed on a case-by-case basis in light of the nature of the right

17 Schedule 2, item 5, proposed section 52G; explanatory memorandum, p. 37.

18 Schedule 2, item 5, proposed section 52H; *Administrative Appeals Tribunal Act 1975*, subsections 35(4)–(5).

19 To the extent that the effect of this bill would be to limit a person's ability to challenge a migration or citizenship decision, the consequence of that decision being the person's detention and deportation from Australia or prevention of return to Australia for citizens overseas, the measure may also engage and limit a number of other rights. In particular, the right to liberty (as immigration detention may be a consequence of a decision); right to protection of the family (as family members may be separated); right to non-refoulement (if the consequence of a decision is deportation and removal from Australia); freedom of movement (if cancellation of a visa or cessation of citizenship prevents a person from re-entering and remaining in Australia as their own country); and rights of the child (if the decision relates to a child's nationality). The rights implications of citizenship cessation are discussed in Parliamentary Joint Committee on Human Rights, *Report 8 of 2017* (15 August 2017) pp. 2–31; and *Report 6 of 2019* (5 December 2019), pp. 2–19.

20 International Covenant on Civil and Political Rights, article 14

in question.²¹ A decision involving the removal of an existing right, such as revocation of citizenship, would create a suit at law for the purposes of article 14.²²

2.9 In order to constitute a fair hearing, the hearing must be conducted by an independent and impartial court or tribunal, before which all parties are equal, and have a reasonable opportunity to present their case.²³ The United Kingdom (UK) courts and the European Court of Human Rights have held that the right to a fair hearing is violated where a person is not provided with sufficient information about the allegations against them to enable them to give effective instructions in relation to those allegations, and have an opportunity to challenge the allegations, even in circumstances where full disclosure of information is not possible for reasons of national security.²⁴ There can be no fair hearing if a case against a person is based

21 UN Human Rights Committee, *General Comment 32: Article 14, Right to Equality before Courts and Tribunals and to Fair Trial* (2007) [16]. At [17], the UN Human Rights Committee has indicated that the guarantees in article 14 do not generally apply to expulsion or deportation proceedings, although the procedural guarantees of article 13 are applicable to such proceedings. See, for example, *PK v Canada*, UN Human Rights Committee Communication No.1234/03 (2007), especially at [7.5] where the Committee rejected the applicability of article 14 to a claim relating to the complainant's right to receive protection in the state party's territory. See also, *Zündel v Canada*, UN Human Rights Committee Communication No.1341/2005, (2007) at [6.7–6.8] which recalled that the 'concept of a "suit at law" under article 14, paragraph 1, of the Covenant is based on the nature of the right in question rather than on the status of the parties'. In this case, the author was a permanent resident who sought to continue residing in the State party's territory. The UN Committee concluded that the author's deportation proceedings, as a result of being found to constitute a threat to national security, did not fall within the scope of article 14 because 'proceedings relating to an alien's expulsion, the guarantees of which are governed by article 13 of the Covenant, do not also fall within the ambit of a determination of "rights and obligations in a suit at law", within the meaning of [article 14(1)]'.

22 For previous commentary on the right to a fair hearing in the context of revocation of citizenship see Parliamentary Joint Committee on Human Rights, *Report 8 of 2017* (15 August 2017) pp. 2–31; *Report 6 of 2019* (5 December 2019), pp. 2–19.

23 See UN Human Rights Committee, *General Comment 32: Article 14, Right to Equality before Courts and Tribunals and to Fair Trial* (2007) [18].

24 See, *Secretary of State for the Home Department v AF (No. 3)* [2009] UKHL 28, especially at [59] where the court ruled that 'the controlee must be given sufficient information about the allegations against him to enable him to give effective instructions in relation to those allegations. Provided that this requirement is satisfied there can be a fair trial notwithstanding that the controlee is not provided with the detail or the sources of the evidence forming the basis of the allegations'. See also, *A v United Kingdom*, European Court of Human Rights (Grand Chamber), Application no. 3455/05 (2009), especially [218] where the Court stated that 'it was essential that as much information about the allegations and evidence against each applicant was disclosed as was possible without compromising national security or the safety of others. Where full disclosure was not possible, Article 5(4) required that the difficulties this caused were counterbalanced in such a way that each applicant still had the possibility effectively to challenge the allegations against him'.

solely or to a decisive degree on closed materials or where open material consists only of general assertions.²⁵ As regards this bill, a person's right to a fair hearing may be limited by the measure insofar as it would restrict the disclosure of information to the person, including information that was used in character-related decision-making, such as criminal allegations against a person, as well as excluding the person from making submissions about the use of the information in proceedings. The measure appears to have the effect of withholding sufficient information from the person to the extent that they are unable to effectively provide instructions in relation to, and challenge, the information, including possible criminal allegations against them.

2.10 As regards decisions relating to the expulsion or deportation of non-citizens or foreign nationals who are lawfully in Australia, the measure also appears to engage and limit the prohibition against expulsion of aliens without due process. This right is protected by article 13 of the International Covenant on Civil and Political Rights, which provides that:

An alien lawfully in the territory of a State Party...may be expelled therefrom only in pursuance of a decision reached in accordance with law and shall, except where compelling reasons of national security otherwise require, be allowed to submit the reasons against his expulsion and to have his case reviewed by, and be represented for the purpose before, the competent authority or a person or persons especially designated by the competent authority.

2.11 Article 13 incorporates notions of due process also reflected in article 14 of the International Covenant on Civil and Political Rights and should be interpreted in light of that right.²⁶ In particular, the United Nations (UN) Human Rights Committee has stated that article 13 encompasses 'the guarantee of equality of all persons before the courts and tribunals as enshrined in [article 14(1)] and the principles of impartiality, fairness and equality of arms implicit in this guarantee are applicable'.²⁷ The UN Committee has further stated that 'an alien...be given

25 *Secretary of State for the Home Department v AF (No. 3)* [2009] UKHL 28 [59]; *A v United Kingdom*, European Court of Human Rights (Grand Chamber), Application no. 3455/05 (2009) [220].

26 UN Human Rights Committee, *General Comment No. 32: The right to equality before courts and tribunals and to a fair trial* (2007) [17], [63].

27 UN Human Rights Committee, *General Comment No. 32: The right to equality before courts and tribunals and to a fair trial* (2007) [17], [63].

full facilities for pursuing [their] remedy against expulsion so that this right will in all circumstances of [their] case be an effective one'.²⁸

2.12 The measure limits the due process requirements in article 13 to the extent that it restricts a person's access to information that informed the decision leading to their expulsion or deportation, as well as their ability to make submissions on the use of that information or the weight to be attributed to the information by the court. Such restrictions would appear to have the effect of preventing a person in Australia whose visa is refused or cancelled from effectively contesting or correcting potentially erroneous information, thereby hindering their ability to effectively challenge the decision and pursue a remedy against expulsion.²⁹

2.13 The due process guarantees in article 13 may be departed from, but only when 'compelling reasons of national security' so require.³⁰ It is unclear whether this exception would apply to this measure. The bill seeks to depart from due process requirements where there is a real risk of damage to the 'public interest'. While Australia's national security is a factor to be considered by the court in determining whether disclosing the information would create a real risk of damage to the public interest, it is not the only factor. There are other factors to be considered by the court which are broader than national security reasons, such as Australia's relations with other countries and the risk of discouraging informants. Furthermore, the UN Human Rights Committee appears to have interpreted the exception of 'compelling reasons of national security' to be a reasonably high threshold which States parties

28 UN Human Rights Committee, *General Comment No. 15: The position of aliens under the Covenant* (1986) [10]. The Committee has also stated that 'Article 13 directly regulates only the procedure and not the substantive grounds for expulsion. However, by allowing only those carried out "in pursuance of a decision reached in accordance with law", its purpose is clearly to prevent arbitrary expulsions'.

29 See Committee on the Elimination of Racial Discrimination, *General Comment No. 30: discrimination against non-citizens* (2004) at [25], where the Committee on the Elimination of Racial Discrimination stressed the importance of the right to challenge expulsion and access an effective remedy, noting that States should ensure that 'non-citizens have equal access to effective remedies, including the right to challenge expulsion orders, and are allowed effectively to pursue such remedies'.

30 International Covenant on Civil and Political Rights, article 13; UN Human Rights Committee, *General Comment No. 15: The position of aliens under the Covenant* (1986) [10]. Note that if there are compelling reasons of national security not to allow an alien to submit reasons against their expulsion, the right will not be limited. Where there are no such grounds, the right will be limited, and then it will be necessary to engage in an assessment of the limitation using the usual criteria (of necessity and proportionality).

must meet before departing from their due process obligations.³¹ As such, it would appear that article 13 is engaged and limited, yet the statement of compatibility did not identify it as being engaged by the bill, and accordingly no assessment was provided as to whether the limitation was permissible.

2.14 The right to a fair hearing and the prohibition against expulsion of aliens without due process may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

2.15 In order to assess the compatibility of this measure with human rights, particularly the proportionality of the measure, further information is required as to:

- (a) why it is necessary and appropriate to use ‘public interest’ as opposed to ‘national security’ as the threshold concept for determining whether confidential information can be disclosed to another person, and a rationale for the inclusion of each of the grounds in proposed subsections 52C(5) and 503C(5);
- (b) why it is necessary and appropriate for the matters specified in proposed subsections 52C(5) and 503C(5) to be exhaustive;

31 See, for example, *Mansour Leghaei and others v Australia*, United Nations Human Rights Committee Communication No. 1937/2010 (2015): the partially dissenting opinion of Committee members Sarah Cleveland and Víctor Manuel Rodríguez-Rescia (dissenting only because the Committee as a whole did not consider the article 13 arguments) is noteworthy with respect to the national security exception in article 13. The Committee concluded at [10.4] that ‘the author was never formally provided with the reasons for the refusal to grant him the requested visa which resulted in his duty to leave the country, except for the general explanation that he was a threat to national security based on security assessment of which he did not even receive a summary’. In light of this finding, Committee members Cleveland and Rodríguez-Rescia concluded at [5] that the ‘invocation of “compelling reasons of national security” to justify the expulsion of the author...did not exempt the State from the obligation under article 13 to provide the requisite procedural safeguards. The fact that the State failed to provide the author with these procedural safeguards constitutes a breach of the obligation under article 13 to allow the author to submit the reasons against his expulsion...This means that he should have been given the opportunity to comment on the information submitted to them, at least in summary form’. See also, *Mansour Ahani v Canada*, United Nations Human Rights Committee Communication No. 1051/2002 (2004) [10.8]: ‘Given that the domestic procedure allowed the author to provide (limited) reasons against his expulsion and to receive a degree of review of his case, it would be inappropriate for the Committee to accept that, in the proceedings before it, “compelling reasons of national security” existed to exempt the State party from its obligation under that article to provide the procedural protections in question’. Other jurisprudence of the UN Human Rights Committee indicates that States have previously been afforded ‘wide discretion’ as to whether national security reasons exist but that States should at least demonstrate that there are ‘plausible grounds’ for exercising the national security exception: See *Alzery v Sweden*, United Nations Human Rights Committee Communication No. 1416/2005 (2006).

- (c) why it is not possible to allow the court to disclose the relevant information (or a summary of it) to the extent that is necessary to ensure procedural fairness in circumstances where partial disclosure could be achieved without creating a real risk of damage to the public interest;
- (d) why procedural fairness, particularly as relates to the applicant, is not included as a matter that the court must have regard to when determining whether disclosing the information would create a real risk of damage to the public interest;
- (e) what other matters are likely to be specified in the regulations in relation to proposed subsections 52C(5) and 503C(5);
- (f) why is there no process by which a special advocate or equivalent safeguard is able to represent the applicant's interests if it is determined that relevant information be withheld from the applicant; and
- (g) what, if any, other safeguards exist to ensure that the proposed limit on the right to a fair trial and the prohibition against expulsion without due process are proportionate.

Committee's initial view

2.16 The committee noted that the bill engages and limits the right to a fair hearing and the prohibition against expulsion of aliens without due process, to the extent that it restricts a person's access to information that is relevant to the decision which affects them, and excludes the person from hearings where they are not lawfully aware of the contents of the information. The committee noted that these rights may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate.

2.17 The committee considered that the bill pursues the legitimate objective of upholding law enforcement and intelligence capabilities, and insofar as the measure protects disclosure of confidential information where disclosure may jeopardise law enforcement or intelligence activities, the bill is rationally connected to this objective. The committee considered further information was required to assess the proportionality of the measure.

2.18 The committee had not yet formed a concluded view in relation to this matter. It considered further information was required to assess the human rights implications of this bill, and accordingly sought the minister's advice as to the matters set out at paragraph [2.15].

2.19 The full initial analysis is set out in [Report 1 of 2020](#).

Minister's response³²

2.20 The minister advised:

- **why it is necessary and appropriate to use 'public interest' as opposed to 'national security' as the threshold concept for determining whether confidential information can be disclosed to another person, and a rationale for the inclusion of each of the grounds in proposed subsections 52C(5) and 503C(5);**

The measures in the Bill are necessary to strengthen the Government's ability to uphold public safety and the good order of the Australian community through character-related decisions made under both the *Migration Act 1958* (the Migration Act) and the *Australian Citizenship Act 2007* (the Citizenship Act).

The Department relies on confidential information provided by law enforcement and intelligence agencies to assess the character of visa applicants and visa holders. If the person fails the character test, they may be refused a visa, or if they hold a visa, it can be cancelled.

The changes will strengthen the framework for the protection and use of confidential information in the Citizenship Act in substantially the same way as that in the Migration Act, allowing the Department to rely on confidential information provided by law enforcement and intelligence agencies to assess the character of certain citizenship applicants, or persons whose citizenship may be considered for revocation.

Under the proposed amendments, after considering the information and any submissions, the High Court, the Federal Court of Australia, or the Federal Circuit Court (the courts) must determine if disclosure of information would create a real risk of damage to the 'public interest', having regard to any of the following matters (and only those matters) that it considers relevant. As per 52C(5) of the Citizenship Act and 503C(5) of the Migration Act, these are:

- the fact that the information was communicated, or originally communicated, to an authorised Commonwealth officer by a gazetted agency on the condition that it be treated as confidential information;
- the risk that the disclosure of information may discourage gazetted agencies and informants from giving information in the future;
- Australia's relations with other countries;

32 The minister's response to the committee's inquiries was received on 23 February 2021. This is an extract of the response. The response is available in full on the committee's website at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports.

- the need to avoid disruption to national and international efforts relating to law enforcement, criminal intelligence, criminal investigation and security intelligence;
- in a case where the information was derived from an informant - the protection and safety of informants and of persons associated with informants;
- the protection of the technologies and methods used (whether in or out of Australia) to collect, analyse, secure or otherwise deal with, criminal intelligence or security intelligence; and
- such other matters (if any) as are specified in the regulations.

The matters listed above have been included as matters that the court should have regard to as they are relevant to determining whether disclosure of the information would create a real risk of damage to the public interest. In practice, this may include disclosure which would pose an unacceptable risk to the intelligence capabilities, operations and sources of law enforcement and intelligence agencies - including active investigations. This in turn may compromise Australia's national security. The matters listed above are relevant to the court's determination because the disclosure of the information may therefore risk jeopardising the trusted relationship between the Department and law enforcement and intelligence agencies, and may result in information that is relevant to character decisions not being made available to the decision-maker for consideration.

Additionally, while the listed matters include 'Australia's national security' explicitly (as per s52C(5)(g) of the Citizenship Act and s503C(5)(g) of the Migration Act), and will often involve national security issues directly or indirectly, they are broader than this provision alone. This is because the protection of sensitive and confidential information is intended to support the operational activities of law enforcement agencies as well as broader strategies to counter terrorism, transnational crime and related activities, including protection of informants and protection of technologies and methods.

The Bill will provide safeguards for the applicant by allowing the courts to decide how much weight to give to the confidential information that has been submitted in evidence (s52C(7) of the Citizenship Act and s503C(7) of the Migration Act). This allows the courts to weigh up a number of factors, including fairness to the applicant and the public interest when assessing what weight to attribute to the evidence. Practically, this may involve a situation where the court has determined not to disclose the protected information, which would include not disclosing the information to the applicant. Even so, the court is to weigh up a number of factors when assessing what weight to give to evidence, including unfair prejudice to an applicant by not having access to the confidential information as well as the public interest. Information available for the courts to consider in this regard would include any information that the applicant, their authorised

representative or any third party has raised in support of their case, irrespective of whether the protected information has been disclosed to the applicant or their authorised representative.

- **why it is necessary and appropriate for the matters specified in proposed subsections 52C(5) and 503C(5) to be exhaustive;**

The measures in the Bill are necessary to strengthen the Government's ability to uphold public safety and the good order of the Australian community through character-related decisions made under both the Migration Act and the Citizenship Act.

These measures will enhance the ability of decision-makers to use confidential information to manage the risk of certain individuals of character concern, where there may otherwise be insufficient non-confidential information to underpin a decision. The changes help ensure that these individuals who pose a risk to public safety will be prevented from entering or remaining in Australia by providing a framework which protects the confidential information from harmful disclosure.

The potential disclosure of confidential information may pose an unacceptable risk to the intelligence capabilities, operations and sources of law enforcement and intelligence agencies - including active investigations. This risks jeopardising the trusted relationship between the Department and law enforcement and intelligence agencies, and may result in information that is relevant to character decisions not being made available to the decision-maker for consideration.

The framework proposed by the Bill provides a mechanism which allows the court to require disclosure of the relevant information to it and a further mechanism for the court to consider whether it can disclose the protected information to the applicant (amongst others) if doing so does not create a real risk of damage to the public interest.

It is appropriate that the list of matters the court can have regard to (if relevant) in subsections 52C(5) of the Citizenship Act and 503C(5) of the Migration Act is exhaustive, as it provides clarity and certainty for the court in exercising its functions. As noted above, the scope and content of the matters listed in those sections reflects and emphasises the sensitive nature of the information, and the need for the court to give careful consideration to those matters in order to decide whether there would be a real risk of damage to the public interest if the information was disclosed more widely, including to the applicant in judicial review proceedings.

The Bill provides that the court may give such weight in the substantive proceedings to the information as the court considers appropriate in the circumstances. Such circumstances may involve a situation where the court has determined not to disclose the protected information. This allows the courts to weigh up a number of factors, including unfair prejudice to an applicant by not having access to the confidential information and the public interest. This provides clear safeguards for the

applicant's interests in any proceedings, and places these safeguards within the control of the court.

- **why it is not possible to allow the court to disclose the relevant information (or a summary of it) to the extent that is necessary to ensure procedural fairness in circumstances where partial disclosure could be achieved without creating a real risk of damage to the public interest;**

The Bill proposes a number of amendments to the Migration Act and the Citizenship Act to protect confidential information provided by gazetted law enforcement and intelligence agencies on the condition that it is treated as confidential for use in visa and citizenship decision-making, in order to enhance the Government's ability to manage risks to the community posed by certain individuals of character concern .

In practice, law enforcement and intelligence agencies provide confidential information to the Department of Home Affairs on the basis that it can be protected from disclosure. This is because, if such information were disclosed, there would be a real risk that there would be damage to the public interest and jeopardise the capabilities of law enforcement and intelligence agencies – and potentially compromise active investigations. Therefore, it is the agencies themselves who designate the information as confidential because of the intrinsically sensitive nature of its contents and scope.

Criminal intelligence and related information is vital to assessing the criminal background or associations of non-citizen visa and citizenship applicants and visa holders. The measures in this Bill will ensure that information - disclosed in confidence by law enforcement and intelligence agencies - is appropriately protected.

Given the sensitive nature of the information communicated in confidence by the gazetted agencies and the identity of the gazetted agency itself, partial disclosure of the information or of a summary of the information to the applicant could damage the public interest. Further, it is open to gazetted agencies to communicate information which they may indicate is not communicated in confidence. Where this occurs, the information would not be subject to the protected information framework and so may (subject to other relevant laws) be subject to full or partial disclosure, or disclosure of a summary, as appropriate.

The Minister considers that the current approach in the Bill is appropriate and that any consideration of whether to disclose part of the relevant information is duplicative and unnecessary: the same risks of damage to the public interest would arise from partial or full disclosure given the sensitive nature of the information in question.

Nonetheless, the Bill will provide for greater judicial oversight in visa and citizenship decisions that rely on confidential information. The amendments allow the courts to require the disclosure to it of confidential

information provided by gazetted agencies that was relevant to the exercise of power by the Minister (or delegate) which is the subject of the proceedings.

The Bill will provide safeguards for the applicant by allowing the courts to decide how much weight to give to the confidential information. This allows the courts to weigh up a number of factors, including fairness to the applicant and the public interest, in using this information in review of visa and citizenship decisions. Practically, this may involve a situation where the court has determined not to disclose the protected information, which would include not disclosing the information to the applicant.

- **why procedural fairness, particularly as relates to the applicant, is not included as a matter that the court must have regard to when determining whether disclosing the information would create a real risk of damage to the public interest;**

The Bill, together with the existing framework as a whole, aims to strike an appropriate balance between protecting the public interest and providing fairness to the applicant.

- The Bill will allow confidential information provided by law enforcement and intelligence agencies to be considered by the courts while preventing its further disclosure where it would create a real risk of damage to the public interest.
- The Bill will provide safeguards for the applicant by allowing the courts to decide how much weight to give the confidential information in judicial review, and to further disclose this information when there is no real risk of damage to the public interest. Where the court has determined not to disclose the information, which would include not disclosing the information to the applicant, the court may take into account the unfair prejudice for the applicant when deciding what the weight to give to that information.

The matters listed in s52C(5) of the Citizenship Act and s503C(5) of the Migration Act are limited to those which could be broadly characterised as matters going to the public interest, as they reflect and emphasise the highly sensitive nature of the information provided by the gazetted agencies to the Department for use in character-related decision making. Noting this, the Bill also provides that the court may give such weight to protected information as is appropriate in the circumstances, which would include circumstances where the court has determined not to disclose the information to the applicant. This allows the court to consider the impact nondisclosure would have on the applicant when giving weight to evidence.

The Bill does not remove procedural fairness from character-related visa and citizenship decision making processes. Rather, procedural fairness is provided at the various stages of the process in a way that strikes an appropriate balance between protecting the public interest (by protecting

confidential information provided by intelligence and law enforcement agencies) and providing fairness to the affected person.

Where a person seeks judicial review, the court will afford the affected person natural justice and the framework in s52C of the Citizenship Act and s503C of the Migration Act will be enlivened. This framework provides a mechanism which allows the court to require disclosure of the relevant confidential information to it and a further mechanism for the court to consider whether it can disclose the information to the applicant (amongst others) if doing so does not create a real risk of damage to the public interest. In this way, the court can exercise its judicial functions in order to conduct an effective judicial review.

- **what other matters are likely to be specified in the regulations in relation to proposed subsections 52C(5) and 503C(5);**

It is noted that paragraphs 52C(5)(h) of the Citizenship Act and 503C(5)(h) of the Migration Act provide a mechanism for other matters to be included in these subsections if specified in relevant regulations. These paragraphs were included in the Bill in order to provide flexibility going forward.

Given the rapidly evolving and complex security challenges, it is essential that further specifications are able to be made in the regulations to ensure the ongoing protection of confidential information shared between the Department, law enforcement and intelligence agencies in a changeable national security landscape. As such, if Parliament passes the Bill, the Department will monitor the operation of the protected information framework provided for in the Bill and, if deemed desirable or necessary to assist the court in determining whether to disclose the confidential information, to include further matters for the court to have regard to in subsections 52C(5) of the Citizenship Act and 503C(5) of the Migration Act. This can be effected through amendments to the *Australian Citizenship Regulation 2016* or *Migration Regulations 1994*, as appropriate. As amendments to these Regulations are disallowable, they will be accompanied by a Statement of Compatibility with Human Rights and subject to parliamentary scrutiny.

- **why is there no process by which a special advocate or equivalent safeguard is able to represent the applicant's interests if it is determined that relevant information be withheld from the applicant;**

The Bill will allow the courts to admit confidential information into evidence and to decide how much weight to give to that evidence.

This will sufficiently allow the courts to weigh up a number of factors, including prejudice to an applicant by not having access to the confidential information and the public interest.

The gazetted intelligence and law enforcement agencies are defined in the Bill at s503A(9) of the Migration Act (which is identical to the current s503A(9) of the Migration Act). The same definition applies within the

context of the Citizenship Act. Gazetted agencies include Australian and foreign law enforcement or intelligence bodies which are listed in the Gazette. A war crimes tribunal established under international arrangements of law may also be a gazetted agency and is not required to be listed in the Gazette.

As such, the gazetted agencies are publicly identifiable. Effectively, this means that affected persons are on notice as to the identities of intelligence and law enforcement agencies that may communicate confidential information to the Department for use in character-related visa and citizenship decision making. This may help affected persons and their representatives understand where the confidential information may be sourced and to put forward relevant matters for the consideration of the court.

The framework in the Bill provides a mechanism which allows the court to require disclosure of the relevant confidential information to it and a further mechanism for the court to consider whether it can disclose the information to the applicant (amongst others) if doing so does not create a real risk of damage to the public interest. The Bill further provides that the courts may give such weight in the substantive proceedings to the information as the court considers appropriate in the circumstances. In this way, the court can exercise its judicial functions in order to conduct an effective judicial review.

- **what, if any, other safeguards exist to ensure that the proposed limit on the right to a fair trial and the prohibition against expulsion without due process are proportionate.**

The limitations on providing all of the information to the affected person are in place to strengthen the Government's ability to uphold public safety and the good order of the Australian community through character-related visa and citizenship decisions and to protect highly sensitive information communicated in confidence by gazetted agencies when used in making those decisions. The affected person will continue to have the ability to submit reasons against their expulsion in a merits and/or judicial review process. Further, in the judicial review of those decisions, the court will be able to consider the information, whether disclosure would create a real risk of damage to the public interest, and how much weight to accord to information that it knows has not been made available to the affected person.

Specifically, the framework will provide that during judicial review, the courts may order the Minister to disclose confidential information to it that was relevant to the visa or citizenship decision (that is, the Minister will not have a discretion not to comply in this circumstance). The Minister can provide submissions to the courts about the use of the information and the impact that further disclosure would have on the public interest.

As noted elsewhere, the Bill provides that the courts may give such weight in the substantive proceedings to the information as the court considers

appropriate in the circumstances. Such circumstances may involve a situation where the court has determined not to disclose the protected information. This allows the courts to weigh up a number of factors, including unfair prejudice to an applicant by not having access to the confidential information and the public interest. This provides clear safeguards for the applicant's interests in any proceedings and places these safeguards within the control of the court.

Further, existing merits review rights will not be affected by the Bill. The Minister has long had power to disclose or protect information from disclosure during merits review. The Bill will provide the Minister with discretionary powers to disclose the confidential information (having consulted the relevant gazetted agency) to specified persons, bodies, tribunals or courts.

Where the Minister does authorise disclosure of protected information to a Tribunal in accordance with s52B(1) of the Citizenship Act and s503B(1) of the Migration Act, then the Tribunal will have obligations to afford natural justice during any relevant merits review subject to the obligations imposed upon it by s52B of the Citizenship Act and s503B of the Migration Act.

The balance reflected in the Bill will enable law enforcement agencies to continue to provide confidential information to the Department to make fully informed visa and citizenship decisions on character grounds, while providing fairness to applicants seeking merits or judicial review of a departmental decision. This is essential to the Government's core business of regulating, in the national interest, who should enter and remain in Australia, and who should be granted Australian citizenship and the privileges which attach to it.

Concluding comments

International human rights legal advice

Right to a fair hearing and prohibition against expulsion of aliens without due process

2.21 To assess the proportionality of the measure, further information was sought from the minister as to whether the proposed limitation: is sufficiently circumscribed; is accompanied by adequate safeguards; provides sufficient flexibility to treat different cases differently; is the least rights restrictive means of achieving the stated objective; and provides access to effective review.

2.22 In assessing whether the proposed limitation on the rights is sufficiently circumscribed, it is relevant to consider the scope of the matters set out in proposed subsections 52C(5) and 503C(5) and, in particular, whether it is necessary and appropriate to use the wider concept of 'public interest' rather than 'national security' as a basis for non-disclosure of confidential information. The minister noted that while the matters specified in these provisions include 'Australia's national security' (as per subsections 52C(5)(g) and 503C(5)(g)) and will often involve national

security issues directly or indirectly, the specified matters are broader than this provision alone. The minister stated that this is because the measure to protect sensitive and confidential information is intended to support the operational activities of law enforcement agencies as well as broader strategies to counter terrorism, transnational crime and related activities, including protecting informants and technologies and methods. Regarding other matters that may be prescribed in regulations,³³ the minister stated that these provisions were included to provide flexibility going forward. The minister noted that given the rapidly evolving and complex security challenges, it is essential that regulations are able to specify further matters to ensure the ongoing protection of confidential information shared between the department, law enforcement and intelligence agencies in a changeable national security landscape.

2.23 The preliminary analysis noted that the use of the broader concept of 'public interest' rather than the narrower concept of 'national security' would appear to create a lower threshold which must be met in order to prohibit the disclosure of information to any person, including the person to whom the information pertains. It remains unclear whether this broader concept is necessary and whether all specified matters are relevant to achieving the stated objective of protecting national security and associated law enforcement and intelligence capabilities, noting the bill includes things such as 'Australia's relations with other countries'. While it is noted that subsections 52C(5)(h) and 503C(5)(h) are intended to provide flexibility to respond to evolving security challenges, without information as to what other matters may be likely to be specified in the regulations, it remains difficult to ascertain the precise circumstances in which rights may be limited. As such, questions remain as to whether the measure is sufficiently circumscribed.

2.24 With respect to the existence of safeguards, the minister has stated that allowing the courts to decide how much weight to give to the confidential information in any substantive proceedings³⁴ would operate to safeguard the applicant's interests. The minister noted that these provisions would allow the courts to weigh up a number of factors, including fairness to the applicant and the public interest, when assessing what weight to attribute to the evidence. The minister suggested that in practice it may involve a situation where the court has determined not to disclose the information to the applicant and in considering what weight to attribute to that information, the court may consider any unfair prejudice to the applicant by not having access to the confidential information as well as the public interest. In making this assessment, the minister noted that the court could consider any information provided by the applicant or their legal representative in relation to the matter.

33 Schedule 1, item 3, proposed subsection 52C(5)(h) and item 9, proposed subsection 503C(5)(h).

34 Schedule 1, item 3, proposed subsection 52C(7) and item 9, proposed subsection 503C(7).

2.25 However, it is unclear whether this provision would operate as an adequate safeguard in practice, noting the overall effect of the measure is to limit the court's ability to perform its judicial function. The court is only permitted to hear submissions regarding the use of the information and any weight to be attributed to that information from parties who are aware of the contents of the information.³⁵ In practice, the minister is likely to be the only party who is aware of the contents of the information and thus the applicant and their legal representative would inevitably be excluded from these proceedings. While the minister noted that the court could consider information provided by the applicant in support of their case, it is unlikely that the applicant or their legal representative would have an opportunity to make submissions with respect to the use and weight of the information. In such circumstances, it seems likely that any information provided to the court by the applicant would be of a general nature and not directly related to the court's consideration of what weight to attribute to the information. Without the ability to receive submissions from the person to whom the information pertains, it would appear very difficult for the court to properly test the reliability, relevance and accuracy of the information and thus perform its judicial task of determining the appropriate weight to attribute to the information. For these reasons, it appears that allowing the court to decide how much weight to attribute to the information in substantive proceedings would neither safeguard the rights of the applicant nor ensure that any limitation is proportionate.

2.26 The preliminary analysis noted that special advocates have been recognised by the European Court of Human Rights as an important safeguard to 'counterbalance procedural unfairness' in the context of domestic laws that restrict disclosure of information to parties for reasons of national security.³⁶ The minister was asked why the bill provides no process by which a special advocate or equivalent safeguard is able to represent the applicant's interests if it is determined that relevant information be withheld from the applicant. The minister's response did not address this question. Instead, the minister noted that in deciding what weight to attribute to confidential information, the court may weigh up various factors, including any prejudice to the applicant and the public interest. The minister further noted that as gazetted agencies are publicly identifiable, affected persons are effectively on notice as to the agencies that may communicate confidential information to the department for use in character-related visa and citizenship decisions. The minister stated that this may help applicants and their representatives to understand the source of the confidential information and to put forward relevant matters for the court's consideration.

35 See Schedule 1, item 3, proposed subsections 52C(2)–(3) and item 9, proposed subsections 503C(2)–(3).

36 *A v United Kingdom*, European Court of Human Rights (Grand Chamber), Application no. 3455/05 (2009) [209] and [219].

2.27 However, without knowing even the substance of the information, the ability to identify a broad range of agencies that may have communicated the confidential information would seem to be of limited assistance to the applicant in practice.³⁷ As noted in the preliminary analysis, the applicant would need sufficient information about the allegations against them in order to challenge the contents of the information and provide effective instructions to their legal representative.³⁸ At a minimum, to safeguard procedural fairness, it is necessary that the applicant be in a position to understand the substance of the allegations and be afforded the opportunity to respond to those allegations.³⁹ The ability to identify gazetted agencies generally would therefore appear to have no safeguard value.

2.28 The necessity of prescribing an exhaustive list of matters to which the court must have regard in determining whether to disclose the information is a relevant consideration in assessing whether the measure provides sufficient flexibility to treat individual cases differently. The minister stated that it is appropriate that the matters specified in subsections 52C(5) and 503C(5) are exhaustive because it provides clarity and certainty for the court in exercising its functions. The minister noted that the matters prescribed are those which could be broadly characterised as matters going to the public interest and reflect the highly sensitive nature of the information. While

37 The proposed definition of gazetted agency includes a broad range of bodies, including any law enforcement or intelligence body or foreign law enforcement body specified in a notice published by the Minister in the Gazette, as well as a war crimes tribunal established by or under international arrangements or international law: Schedule 1, item 9, proposed subsection 503A(9).

38 See, *Secretary of State for the Home Department v AF (No. 3)* [2009] UKHL 28, especially at [59] where the court ruled that 'the controlee must be given sufficient information about the allegations against him to enable him to give effective instructions in relation to those allegations. Provided that this requirement is satisfied there can be a fair trial notwithstanding that the controlee is not provided with the detail or the sources of the evidence forming the basis of the allegations'. See also, *A v United Kingdom*, European Court of Human Rights (Grand Chamber), Application no. 3455/05 (2009), especially [218] where the Court stated that 'it was essential that as much information about the allegations and evidence against each applicant was disclosed as was possible without compromising national security or the safety of others. Where full disclosure was not possible, Article 5(4) required that the difficulties this caused were counterbalanced in such a way that each applicant still had the possibility effectively to challenge the allegations against him'.

39 See, *Applicant VEAL of 2002 v Minister for Immigration and Multicultural and Indigenous Affairs* [2005] HCA 72, especially at [27] where the High Court found that 'to conduct the review with procedural fairness, the appellant had at least to know the substance of what was said against him in the letter'. It stated at [29] that the public interest and procedural fairness could be accommodated in this case 'by the Tribunal telling the appellant what was the substance of the allegations made in the letter and asking him to respond to those allegations'. Although the court noted at [25] that 'the application of principles of procedural fairness in a particular case must always be moulded to the particular circumstances of that case'.

the court must not consider procedural fairness in determining whether to disclose the information to the applicant and others, the minister stated that the court may consider the impact of non-disclosure on the applicant, including possible unfair prejudice to the applicant, in considering what weight to give the information.

2.29 A measure that provides sufficient flexibility to treat different cases differently, as opposed to imposing a blanket policy without regard to the merits of each individual case, is more likely to be considered proportionate. This measure provides the court with minimal flexibility to treat different cases differently because it prescribes an exhaustive list to which the court must have regard and prohibits the court from considering procedural fairness, particularly as relates to the rights of the applicant, as well as any other matters it considers appropriate and necessary to perform its judicial review task. As noted in the preliminary analysis, the proportionality of the measure would be assisted if the court was able to undertake some form of balancing exercise, whereby it may weigh the risk of damage to the public interest against the right to a fair hearing or other matters that it considers appropriate and necessary.⁴⁰

2.30 The preliminary analysis noted that a less rights restrictive way of achieving the stated objective may be to allow the court to disclose as much information as possible without compromising the public interest. The minister stated that the measure is appropriate, and consideration of partial disclosure is duplicative and unnecessary, noting that the same risk of damage to the public interest would arise from partial or full disclosure given the sensitive nature of the information in question. The minister noted that gazetted agencies designate the information as confidential and it is open to these agencies to communicate information not in confidence, meaning that the information would not be subject to the protected information framework.

2.31 However, the bill requires the court to assess the confidential information and determine whether disclosing the information would create a real risk of damage to the public interest. This assessment is independent from the initial assessment made by the gazetted agency, in which it designates the information as confidential. It is open to the court to determine that disclosure of the information does not create a real risk of damage to the public interest, notwithstanding that the gazetted agency designated that information as confidential. It would appear that there may be circumstances where the court could determine that partial disclosure or a summary of the information could assist the court and safeguard procedural

40 See *A v United Kingdom*, European Court of Human Rights (Grand Chamber), Application no. 3455/05 (2009) at [206] where the Court stated that the right to a fair trial may not be violated in circumstances where, having full knowledge of the issues in the trial, the judge is able to carry out a balancing exercise and take steps to ensure that the defence (whose rights are limited) is kept informed and is permitted to make submissions and participate in the decision-making process so far as is possible without disclosing the confidential material.

fairness for the applicant without creating a real risk of damage to the public interest. However, the bill, as currently drafted, would not permit this. While the gazetted agency may determine that partial or full disclosure would create the same level of risk of damage to the public interest, it does not follow that the court would automatically make the same determination. Indeed, if a court were required to accept the gazetted agency's assessment of the risk of disclosure without independent scrutiny, there would be a substantial risk that the requirement of competence, independence and impartiality with respect to the right to a fair hearing would be impermissibly limited. As noted by the United Nations (UN) Human Rights Committee, this 'requirement of competence, independence and impartiality of a tribunal...is an absolute right that is not subject to any exception'.⁴¹ The requirement of independence demands:

actual independence of the judiciary from political interference by the executive branch and legislature...A situation where the functions and competencies of the judiciary and the executive are not clearly distinguishable or where the latter is able to control or direct the former is incompatible with the notion of independent tribunal.⁴²

2.32 As such, it appears that allowing the court to partially disclose the information or provide the applicant with a summary of the information, following an independent assessment of the information and the risk of disclosure, would be a less rights restrictive way of achieving the objective, and would provide the court with greater flexibility to treat different cases differently.

2.33 Additionally, the preliminary analysis raised concerns that there may not be *effective* access to review. The minister stated that existing merits review rights will not be affected by the bill and that the applicant will continue to have the ability to submit reasons against their expulsion in a merits and/or judicial review process. The minister noted that in judicial review of those decisions, the measure enables the courts to order the disclosure of information that is relevant to the decision, although the court may not be able to onwards disclose that information to the applicant. The minister stated that in this way, the court can exercise its judicial functions in order to conduct an effective judicial review. However, as noted in the preliminary analysis, while review is theoretically available, the measure would appear to render the practical efficacy of review meaningless in many cases. This is because the applicant is unable to access critical information on which the decision was based, making it very difficult for the applicant to understand the reasons for the decision and thus effectively challenge the decision. Furthermore, the measure severely hampers the court's ability to consider all matters appropriate and

41 UN Human Rights Committee, *General Comment 32: Article 14, Right to Equality before Courts and Tribunals and to Fair Trial* (2007) [19].

42 UN Human Rights Committee, *General Comment 32: Article 14, Right to Equality before Courts and Tribunals and to Fair Trial* (2007) [19].

necessary to perform its judicial review task. As such, serious concerns remain that the right of review is not, in all the circumstances, an effective one.

2.34 In conclusion, the measure seeks to achieve the legitimate objective of protecting national security and associated law enforcement and intelligence capabilities, and the measure appears to be rationally connected to that objective. However, there are serious concerns as regards proportionality. The safeguards identified by the minister appear to be inadequate and the court would have minimal flexibility to treat different cases differently. There seem to be less rights restrictive ways of achieving the stated objective and access to review is unlikely to be effective in practice. The measure, therefore, does not appear to be proportionate and there is a significant risk that it impermissibly limits the right to a fair hearing and the prohibition against expulsion of aliens without due process.

2.35 Noting this conclusion, this may have implications for a number of other rights,⁴³ including the requirement under international human rights law for independent, effective and impartial review of non-refoulement decisions, noting that Australia's non-refoulement obligations are absolute and may not be subject to any limitations.⁴⁴ While it is noted that a decision to which this measure applies, including a decision to refuse or cancel a protection visa on character grounds, would not, in itself, result in a person necessarily being sent to a country where they could be at risk of persecution or ill-treatment, it could be the first step in a process by

43 To the extent that the effect of this bill would be to limit a person's ability to challenge a migration or citizenship decision, the consequence of that decision being the person's detention and deportation from Australia or prevention of return to Australia for citizens overseas, the measure may also engage and limit a number of other rights. In particular, the right to liberty (as immigration detention may be a consequence of a decision); right to protection of the family (as family members may be separated); freedom of movement (if cancellation of a visa or cessation of citizenship prevents a person from re-entering and remaining in Australia as their own country); rights of the child (if the decision relates to a child's nationality); and prohibition against non-refoulement (if the consequence of a decision is a person's deportation and removal from Australia and return to a country where there is a real risk that they would face persecution, torture or other serious forms of harm, such as the death penalty; arbitrary deprivation of life; or cruel, inhuman or degrading treatment or punishment). The rights implications of citizenship cessation are discussed in Parliamentary Joint Committee on Human Rights, *Report 8 of 2017* (15 August 2017) pp. 2–31; and *Report 6 of 2019* (5 December 2019), pp. 2–19.

44 Regarding effective remedy with respect to non-refoulement decisions see, *Agiza v Sweden*, UN Committee against Torture Communication No.233/2003 (2005) [13.7]; *Singh v Canada*, UN Committee against Torture Communication No.319/2007 (2011) [8.8]-[8.9]; *Josu Arkauz Arana v France*, UN Committee against Torture Communication No.63/1997 (2000); *Alzery v Sweden*, UN Human Rights Committee Communication No.1416/2005 (2006) [11.8]. See generally UN Committee Against Torture, *General Comment No. 4 on the implementation of article 3 of the Convention in the context of article 22* (2017) [13]. For an analysis of this jurisprudence, see Parliamentary Joint Committee on Human Rights, *Thirty-sixth report of the 44th Parliament* (16 March 2016) pp. 182-183.

which a person may be subject to refoulement. To the extent that the effect of this measure would be to limit a person's ability to effectively challenge a decision which may lead to their expulsion or deportation, possibly to a country where they would face persecution, torture or other serious forms of harm, such as the death penalty; arbitrary deprivation of life; or cruel, inhuman or degrading treatment or punishment, the measure may not be consistent with Australia's non-refoulement obligations and the right to an effective remedy.⁴⁵

Committee view

2.36 The committee thanks the minister for this response. The committee notes that the bill seeks to amend the *Migration Act 1958* and the *Australian Citizenship Act 2007* for the purposes of introducing a 'protected information framework'. The framework would prohibit the disclosure of confidential information provided by intelligence and law enforcement agencies where the information is used for certain character-based migration or citizenship decisions. The bill would allow the courts to order the production of confidential information in certain circumstances, however, the courts would be prohibited from onward disclosing any of the information to any person, including the applicant and their legal representative, where it is determined that disclosure would create a real risk of damage to the public interest.

2.37 The committee considers that the bill engages and limits the right to a fair hearing and the prohibition against the expulsion of aliens without due process, to the extent that it restricts a person's access to relevant information and excludes the person from hearings. The committee notes that these rights may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate.

2.38 While the committee considers that the measure pursues the legitimate objective of upholding law enforcement and intelligence capabilities, it is concerned that the measure may not be a proportionate way to achieve the stated objectives. The committee notes the minister's advice that the bill safeguards the applicant's interests by allowing the courts to decide how much weight to give to the confidential information and, in making this assessment, the court may consider a number of factors, including possible unfairness to the applicant.

45 The reports of the Parliamentary Joint Committee on Human Rights have previously considered Australia's non-refoulement obligations in the context of citizenship cessation and amendments to the Migration Act, see, eg: *Report 1 of 2020* (5 February 2020), pp. 124–125; *Thirty-sixth report of the 44th Parliament* (16 March 2016) pp. 57-58; pp. 182-183; *Thirty-fourth report of the 44th Parliament* (23 February 2016) pp. 34-37; *Fourth report of the 44th Parliament* (18 March 2014) [3.57]-[3.66]; *Second report of the 44th Parliament* (11 February 2014) [1.189]-[1.197].

2.39 However, the committee considers that while this may safeguard rights in some instances, it may not be adequate in all the circumstances. The committee notes that the bill sets out an exhaustive list to which the court must have regard in considering whether to disclose information to the applicant, and as such, the court is prohibited from considering procedural fairness in making this decision. The court thus has minimal flexibility to treat different cases differently. Additionally, by restricting the applicant's ability to make submissions regarding the confidential information, it appears very difficult for the court to properly test the reliability, relevance and accuracy of the information and thus perform its judicial task of determining the appropriate weight to attribute to the information.

2.40 The bill as currently drafted also prevents the court from making its own assessment of the risk of disclosure, in that the court is prohibited from making a partial disclosure or disclosing a summary of the information to the applicant, even if the court considered that to do so could assist it and safeguard procedural fairness for the applicant without creating a real risk of damage to the public interest. The committee considers that allowing the court to partially disclose the information or provide the applicant with a summary of the information, following an independent assessment of the information and the risk of disclosure, would be a less rights restrictive way of achieving the objective, and would provide the court with greater flexibility to treat different cases differently.

2.41 The committee further notes that access to review may not be effective in practice because the applicant is unable to access critical information on which the decision was based, making it difficult for the applicant to challenge the decision, and the court's ability to consider all matters appropriate and necessary to perform its judicial review task is limited. For these reasons, there is a significant risk that the measure impermissibly limits the right to a fair hearing and the prohibition against expulsion of aliens without due process.

Suggested action

2.42 The committee considers that the proportionality of the measure may be assisted were the bill amended to provide that:

- (a)** the matters specified in proposed subsections 52C(5) and 503C(5) are non-exhaustive so as to enable the court to consider any other matter that it considers appropriate and necessary;
- (b)** proposed subsections 52C(5) and 503C(5) specify that the court must have regard to procedural fairness and the rights of the applicant;
- (c)** the court be afforded the discretion to disclose the relevant information (or a summary of it) to the extent that is necessary to ensure procedural fairness in circumstances where partial disclosure could be achieved without creating a real risk of damage to the

public interest; and

- (d) a process by which a special advocate or equivalent safeguard be created to represent the applicant's interests if it is determined that the relevant information cannot be disclosed to the applicant.**

2.43 The committee recommends that consideration be given to updating the statement of compatibility with human rights to reflect the information which has been provided by the minister.

2.44 The committee draws these human rights concerns to the attention of the minister and the Parliament.

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020¹

Purpose	This bill seeks to amend the <i>Surveillance Devices Act 2004</i> and other Acts to introduce new powers and warrants to enhance the enforcement and intelligence gathering powers of the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC), including: <ul style="list-style-type: none"> • data disruption warrants to enable the AFP and the ACIC to disrupt data by modifying, adding, copying or deleting data in order to frustrate the commission of serious offences online; • network activity warrants to allow agencies to collect intelligence on serious criminal activity being conducted by criminal networks; and • account takeover warrants to provide the AFP and the ACIC with the ability to take control of a person's online account for the purposes of gathering evidence to further a criminal investigation
Portfolio	Home Affairs
Introduced	House of Representatives, 3 December 2020
Rights	Privacy; effective remedy; life; and torture or cruel, inhuman or degrading treatment or punishment

2.45 The committee requested a response from the minister in relation to the bill in [Report 1 of 2020](#).²

Enhanced law enforcement and intelligence gathering powers and warrants

2.46 The bill seeks to introduce new law enforcement and intelligence gathering powers and warrants to enhance the ability of the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to frustrate crime and gather intelligence and evidence of criminal activity.

2.47 Schedule 1 would introduce a data disruption warrant which would allow the AFP and ACIC to access data held in computers to frustrate the commission of

1 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, *Report 3 of 2021*; [2021] AUPJCHR 32.

2 Parliamentary Joint Committee on Human Rights, *Report 1 of 2020* (3 February 2021), pp. 20-43.

relevant offences (being offences generally subject to imprisonment of three years or more).³ The AFP or ACIC may apply to an eligible judge or nominated Administrative Appeals Tribunal (AAT) member for a data disruption warrant if they suspect on reasonable grounds that:

- one or more relevant offences have been, are being, are about to be, or are likely to be committed;⁴
- the offences involve or are likely to involve data held in a computer; and
- disruption of that data is likely to substantially assist in frustrating the commission of one or more relevant offences.⁵

2.48 An eligible judge or nominated AAT member may issue a data disruption warrant if satisfied that there are reasonable grounds for the suspicion founding the application for the warrant; and the disruption of data authorised by the warrant is justifiable and proportionate, having regard to the offences.⁶ In considering issuing the warrant, the judge or AAT member must have regard to various considerations, including the:

- nature and gravity of the offences;
- likelihood the disruption of data will frustrate the commission of the offences; and
- existence of any alternative means of frustrating the commission of the offences.⁷

2.49 A non-exhaustive list of things that may be authorised by a data disruption warrant are set out in proposed subsection 27KE(2), including entering a premises; using computers, telecommunications facilities, electronic equipment or data storage devices to obtain access to and disrupt data, including adding, copying, deleting or altering data; and intercepting a passing communication.⁸ Additionally, the bill would

3 Schedule 1, item 13, proposed section 27KE. See the definition of 'relevant offences' in section 6 of the *Surveillance Devices Act 2004*.

4 A relevant offence is an offence which carries a maximum sentence of imprisonment of 3 years or more: *Surveillance Devices Act 2004*, section 6.

5 Schedule 1, item 13, proposed section 27KA. An AFP or ACIC officer may also apply for an emergency authorisation for disruption of data held in a computer if certain conditions are met: Schedule 1, item 15, proposed new subsection 28(1C).

6 Schedule 1, item 13, proposed subsection 27KC(1).

7 Schedule 1, item 13, proposed subsection 27KC(2).

8 Schedule 1, item 13, proposed subsection 27KE(2). Data would be covered by the warrant if the disruption of data would be likely to substantially assist in frustrating the commission of a relevant offence: Schedule 1, item 13, proposed subsection 27KE(5).

authorise a broad range of things to be done for the purposes of concealing anything done in relation to the data disruption warrant.⁹

2.50 Schedule 2 would introduce a network activity warrant which would authorise the AFP and ACIC to access data held in computers and collect intelligence on criminal networks operating online. An AFP or ACIC officer may apply to an eligible judge or nominated AAT member for a network activity warrant if they suspect on reasonable grounds that:

- a group of individuals is a criminal network of individuals;¹⁰ and
- access to data held in a computer that is, from time to time, used or likely to be used by any of the individuals in the group, will substantially assist in the collection of intelligence that relates to the group or individuals in the group, and is relevant to the prevention, detection or frustration of one or more relevant offences.¹¹

2.51 An eligible judge or AAT member may issue a network activity warrant if satisfied that there are reasonable grounds for the suspicion founding the application for the warrant and having regard to prescribed matters, including the:

- nature and gravity of the alleged offences;
- extent to which access to data will assist in the collection of intelligence;
- likely intelligence value of any information sought to be obtained and whether the things authorised by the warrant are proportionate to that intelligence value; and
- existence of any alternative, or less intrusive, means of obtaining the information sought.¹²

2.52 Similarly to a data disruption warrant, a broad range of things may be authorised by a network activity warrant in relation to the computer that holds the

9 Schedule 1, item 13, proposed subsection 27KE(9).

10 A criminal network of individuals is defined as an electronically linked group of individuals, where one or more of the individuals in the group have engaged, are engaging, or are likely to engage, in conduct that constitutes a relevant offence; or have facilitated, are facilitating, or are likely to facilitate, the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence. It is immaterial whether the identities of the individuals in the groups or the details of the offences can be ascertained; or there are changes in the composition of the group from time to time: Schedule 2, item 8, proposed section 7A.

11 Schedule 2, item 9, proposed section 27KK.

12 Schedule 2, item 9, proposed subsection 27KM(2).

data sought to be obtained, including things to be done for the purposes of concealing anything done in relation to the warrant.¹³

2.53 Schedule 3 would introduce an account takeover warrant which would authorise the AFP or ACIC to take control of a person's online account for the purposes of gathering evidence of criminal activity.¹⁴ A law enforcement officer may apply to a magistrate for an account takeover warrant if they suspect on reasonable grounds that:

- one or more relevant offences have been, are being, are about to be, or are likely to be, committed; and
- an investigation into those offences is being, will be, or is likely to be, conducted; and
- taking control of one or more online accounts is necessary, in the course of the investigation, to enable evidence to be obtained of the offence.¹⁵

2.54 A magistrate may issue an account takeover warrant if satisfied that there are reasonable grounds for the suspicion founding the application for the warrant and having regard to prescribed matters, including the:

- nature and gravity of the alleged offence;
- any alternative means of obtaining the evidence;
- extent to which the privacy of any person is likely to be affected; and
- likely evidentiary value of the evidence sought.¹⁶

2.55 Similarly to the other warrants, a broad range of things may be authorised by an account takeover warrant in relation to the target account, including taking exclusive control of the account; accessing, adding, copying, deleting or altering account-based data and account credentials; and the doing of anything reasonably necessary to conceal anything done in relation to the warrant.¹⁷

13 Schedule 2, item 9, proposed subsections 27KP(1), (2) and (8).

14 Schedule 3, item 4, proposed section 3ZZUJ.

15 Schedule 3, item 4, proposed subsection 3ZZUN(1).

16 Schedule 3, item 4, proposed section 3ZZUP.

17 Schedule 3, item 4, proposed section 3ZZUR.

Summary of initial assessment

Preliminary international human rights legal advice

Multiple rights

2.56 To the extent that the new powers and warrants would facilitate the investigation, disruption and prevention of serious crimes against persons, including protecting children from harm, the measure may promote multiple rights, including the right to life and the rights of the child. The right to life imposes an obligation on the state to protect people from being killed by others or identified risks.¹⁸ The right imposes a duty on States to take positive measures to protect the right to life, including an obligation to take adequate preventative measures in order to protect persons from reasonably foreseen threats, such as terrorist attacks or organised crime, as well as an obligation to take appropriate measures to address the general conditions in society that may threaten the right to life, such as high levels of crime and gun violence.¹⁹ Furthermore, States have an obligation to investigate and, where appropriate, prosecute perpetrators of alleged violations of the right to life, even where the threat to life did not materialise.²⁰ Regarding the rights of the child, children have special rights under human rights law taking into account their particular vulnerabilities.²¹ States have an obligation to protect children from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual exploitation and abuse.²²

Right to privacy

2.57 The measure engages and limits the right to privacy by authorising the AFP and ACIC to take various actions that may interfere with a person's privacy, including taking actions to:

-
- 18 International Covenant on Civil and Political Rights, article 6(1) and Second Optional Protocol to the International Covenant on Civil and Political Rights, article 1. UN Human Rights Committee, *General Comment No. 6: article 36 (right to life)* (2019) [3]: the right 'concerns the entitlement of individuals to be free from acts and omissions that are intended or may be expected to cause their unnatural or premature death, as well as to enjoy a life with dignity'.
- 19 UN Human Rights Committee, *General Comment No. 6: article 36 (right to life)* (2019) [21], [26]. See also UN Human Rights Committee, *General Comment No. 6: article 6 (right to life)* (1982) [5].
- 20 UN Human Rights Committee, *General Comment No. 6: article 36 (right to life)* (2019) [27]. The UN Human Rights Committee has stated that investigations in alleged violations of the right to life 'must always be independent, impartial, prompt, thorough, effective, credible and transparent': [28].
- 21 Convention on the Rights of the Child. See also, UN Human Rights Committee, *General Comment No. 17: Article 24* (1989) [1].
- 22 Convention on the Rights of the Child, articles 19, 34, 35 and 36.

- access, use and modify an individual's personal data, such as altering a person's bank account credentials or monitoring and re-directing a person's funds held in a bank account;
- collect personal information and intelligence about individuals;
- add, copy, delete or alter other data to obtain access to data held in a target computer in order to determine whether the data is covered by a warrant;
- take control of an individual's online account through accessing and modifying data, such as changing a person's password in order to take control of a person's account and assume that person's identity; and
- enter an individual's home or workplace to do a thing specified in the warrant.²³

2.58 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.²⁴ It also includes the right to control the dissemination of information about one's private life. Additionally, the right to privacy prohibits arbitrary and unlawful interferences with an individual's privacy, family, correspondence or home.²⁵ The right to privacy may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

2.59 In order to assess the compatibility of this measure with the right to privacy, in particular the adequacy of existing safeguards, further information is required as to:

- (a) why the power to issue a data disruption warrant and network activity warrant is conferred on a member of the AAT, of any level and with a minimum of five years' experience as an enrolled legal practitioner, and whether this is consistent with the international human rights law requirement that judicial authorities issue surveillance warrants;
- (b) why the bill does not require, in relation to all warrants, that the issuing authority must consider the extent to which the privacy of any person is

23 See eg explanatory memorandum, pp. 32–33, 38, 39, and 152.

24 International Covenant on Civil and Political Rights, article 17. Every person should be able to ascertain which public authorities or private individuals or bodies control or may control their files and, if such files contain incorrect personal data or have been processed contrary to legal provisions, every person should be able to request rectification or elimination: UN Human Rights Committee, *General Comment No. 16: Article 17* (1988) [10]. See also, *General Comment No. 34 (Freedom of opinion and expression)* (2011) [18].

25 UN Human Rights Committee, *General Comment No. 16: Article 17* (1988) [3]–[4].

likely to be affected, noting that as drafted, this consideration only applies to account takeover warrants;

- (c) why the bill does not require, in relation to all warrants, that the issuing authority must consider whether the warrant is proportionate having regard to the nature and gravity of the offence and the likely value of the information or evidence sought to be obtained, as well as the extent of possible interference with the privacy of third parties, noting that as drafted, these considerations only apply to network activity warrants;
- (d) how the qualification that the statutory conditions do not limit the conditions to which a data disruption warrant or an account takeover warrant may be subject would operate in practice. In particular, would this qualification allow an issuing authority to authorise an action that can only be executed in a manner that results in loss or damage to data or causes the permanent loss of money, digital currency or property;
- (e) whether all of the exceptions to the restrictions on the use, recording or disclosure of protected information obtained under the warrants are appropriate and whether any exceptions are drafted in broader terms than is strictly necessary;
- (f) why the bill does not include provision for public interest monitors or a similar safeguard to protect the rights of the affected person in warrant application and review proceedings; and
- (g) why the chief officer is not required to review the continued need for the retention of records or reports comprising protected information on a more regular basis than every five years.

Right to an effective remedy

2.60 If warrants were to be issued inappropriately, or unauthorised actions carried out under the warrant, a person's right to privacy may be violated. The right to an effective remedy requires access to an effective remedy for violations of human rights.²⁶ This may take a variety of forms, such as prosecutions of suspected perpetrators or compensation to victims of abuse. While limitations may be placed in particular circumstances on the nature of the remedy provided (judicial or otherwise), states parties must comply with the fundamental obligation to provide a remedy that is effective.²⁷

26 International Covenant on Civil and Political Rights, article 2(3).

27 See, UN Human Rights Committee, General Comment 29: States of Emergency (Article 4), (2001) [14].

2.61 In order to assess whether any person whose right to privacy might be violated by the proposed warrants would have access to an effective remedy, further information is required as to:

- (a) whether a person who was the subject of a warrant will be made aware of that after the investigation has been completed; and
- (b) if not, how such a person would effectively access a remedy for any violation of their right to privacy.

Committee's initial view

2.62 The committee considered that to the extent that the new powers and warrants would facilitate the investigation, disruption and prevention of serious crimes against persons, including in particular protecting children from harm and exploitation, the measure may promote multiple rights, including the right to life and the rights of the child.

2.63 However, the committee noted that the measure also engages and limits the right to privacy by authorising the AFP and ACIC to access, use and modify an individual's personal data and information. The committee considered that the measure, in seeking to protect national security and ensure public safety, pursues a legitimate objective and these new law enforcement and intelligence gathering powers and warrants would appear to be rationally connected to that objective. The committee considered further information was required to assess the proportionality of the measure and determine whether the measure limits the right to an effective remedy, and sought the minister's advice as to the matters set out at paragraphs [2.59] and [2.61].

2.64 The full initial analysis is set out in [Report 1 of 2020](#).

Minister's response²⁸

2.65 The minister advised:

Right to privacy

- a. **why the power to issue a data disruption warrant and network activity warrant is conferred on a member of the AAT, of any level and with a minimum five years' experience as an enrolled legal practitioner, and whether this is consistent with the international human rights law requirement that judicial authorities issue surveillance warrants**

In the Bill, the power to issue data disruption warrants and network activity warrants is conferred on an eligible Judge or a nominated

28 The minister's response to the committee's inquiries was received on 23 February 2021. This is an extract of the response. The response is available in full on the committee's website at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports.

Administrative Appeals Tribunal (AAT) member. These issuing authorities may grant the warrant if (amongst other things) they are satisfied that there are reasonable grounds for the suspicion founding the application for the warrant. This independent scrutiny of warrant applications is an important mechanism in ensuring that only warrants that are reasonable and proportionate are issued, and that the power is consistent with Australia's international human rights law obligations.

While it is important to ensure that there is a lawful and independent decision-maker in investigatory powers legislation, there is no requirement under international human rights law for Australia to ensure specifically that it is a judicial authority that authorises investigatory powers. This position is reflected in existing legislation including the *Surveillance Devices Act 2004* (SD Act) and the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

AAT members have the experience and skills necessary to issue data disruption warrants and network activity warrants

Both AAT members and judges play critical roles as independent decision-makers in authorising investigatory powers in the current regimes in the SD Act, as well as in the TIA Act. Nominated AAT members issue surveillance device warrants and computer access warrants under the SD Act, and have played a key role in issuing interception warrants under the TIA Act since 1998. The skills and experience of AAT members make them suitable to assess applications for data disruption warrants and network activity warrants, and whilst doing so, to make independent decisions on the compliance of those applications with the legal requirements in the Bill.

To be nominated as an MT member for the purposes of issuing warrants under the SD Act, a person must have been enrolled as a legal practitioner for at least five years. In accordance with the existing framework, the Bill recognises that the complex decision-making involved in authorising the new powers in the Bill requires the independence offered by the MT members and judges who already issue other warrants under those Acts and have the skills and experience to do so.

AAT members are independent decision-makers

The power to issue warrants is conferred on issuing authorities in their personal capacity (*persona designata*) as a means of ensuring accountability in the course of a sensitive investigation or law enforcement procedure. *Persona designata* functions are not an exercise of the formal judicial or administrative powers of a court or tribunal. Rather these issuing authorities are acting as independent decision-makers.

The AAT is not independent of government in the same way that the judiciary is the subject of a separation of powers (though some members of the AAT are also judges). Rather, the AAT's independence arises from its role in reviewing the merits of administrative decisions made under

Commonwealth laws. The independence of the AAT is also demonstrated in the process for the termination of a member's appointment. AAT members who are not judges can only have their appointment terminated by the Governor-General, and this termination can only be made on specific grounds, such as proven misbehaviour or the inability to perform duties.

The independence of AAT members exercising *persona designata* functions is strongly safeguarded. AAT members are afforded the same protection and immunity as a Justice of the High Court of Australia, and they must provide written consent prior to being authorised to perform *persona designata* functions. Consent also serves to protect an AAT members' independence and autonomy to decide whether or not to exercise *persona designata* powers.

Review of administrative decisions

In the unlikely event of unlawful decision-making, Australian courts will retain their jurisdiction to review administrative decisions, including any decision to issue a warrant, through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia by operation of subsection 398(1) of the *Judiciary Act 1903*, or under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act). There is an error in the human rights compatibility statement in the explanatory memorandum supporting the Bill, which states that the Bill excludes judicial review under the ADJR Act. This is incorrect, and the human rights compatibility statement will be amended accordingly. These judicial review mechanisms ensure that an affected person has an avenue to challenge the decisions to issue warrants made by any issuing authorities, including a nominated AAT member.

As such, the Government maintains that the persons eligible to issue data disruption warrants and network activity warrants should not be limited to only judicial officers, but should include nominated AAT members, in line with the existing legislation.

b. why the bill does not require, in relation to all warrants, that the issuing authority must consider the extent to which the privacy of any person is likely to be affected, noting that as drafted, this consideration only applies to account takeover warrants

c. why the bill does not require, in relation to all warrants, that the issuing authority must consider whether the warrant is proportionate having regard to the nature and gravity of the offence and the likely value of the information or evidence sought to be obtained, as well as the extent of possible interference with the privacy of third parties, noting that as drafted, these considerations only apply to network activity warrants

In deciding whether to issue each of the warrants in the Bill, there are certain matters which the issuing authority must take into account. These

considerations have been specifically designed with regard to the objective and contemplated operation of each of the warrants.

Proportionality test for data disruption warrants

In order to issue a data disruption warrant, the Judge or AAT member must be satisfied that, amongst other things, the disruption of data authorised by the warrant is justifiable and proportionate with regard to the offences targeted. This is to ensure that in considering whether to issue the warrant, the issuing authority weighs up the benefits of targeting the particular offences that the proposed data disruption seeks to frustrate, with the likely effect that data disruption could have beyond frustrating those offences. Satisfaction that the execution of the warrant is justifiable assists in satisfying the requirement under international human rights law that the limitation on the right to privacy is reasonable and not arbitrary.

A specific requirement that the issuing authority consider the privacy of third parties is not appropriate in the context of data disruption warrants, even though it is appropriate in the context of other electronic surveillance warrants the purpose of which is the gathering of evidence. Data disruption warrants are for the purpose of frustrating criminal activity, including preventing further harm to victims, stopping criminal offences occurring, and re-directing activity so that agencies can take appropriate action. It may not always be possible, at the time of applying for the warrant, for an agency to estimate the full extent to which activity required to undertake data disruption is likely to have an impact on third parties. In light of this, rather than providing for an express privacy consideration the Bill contains a mandatory condition that the issue of a data disruption warrant be justified and proportionate having regard to the offences targeted. To further ensure that these warrants are proportionate to the activity they authorise, the issuing authority must consider the existence of any alternative means of frustrating the criminal activity.

There is no requirement that in considering whether to issue a data disruption warrant, the issuing authority take into account the likely evidentiary value (or intelligence value) of the information sought under the warrant. This is because data disruption warrants are not for the purposes of collecting evidence (or intelligence). Data disruption warrants are for the purposes of frustrating criminal offences.

Proportionality test for network activity warrants

In order to issue a network activity warrant, the Judge or MT member must consider whether the activities authorised by the warrant are proportionate to the likely value of intelligence to be collected, as well as the extent to which the warrant is likely to result in access to data of persons lawfully using a computer. The issuing authority must also consider the nature and gravity of the conduct constituting the kinds of offences in relation to which information will be obtained under the

warrant. The purpose of network activity warrants is to allow the AFP and ACIC to target the activities of criminal networks to discover the scope of criminal offending and the identities of the people involved. Due to the complexity of the threats posed by cyber-enabled crime, it is unlikely that agencies will know in advance the identity or location of the offenders involved in the commission of offences to which the network activity warrant is related.

Network activity warrants are an intelligence collection tool and the information collected cannot be used in evidence in criminal proceedings. As such, the considerations for issue of a network activity warrant differ from those in relation to warrants that are issued for the purposes of gathering evidence (for example, computer access warrants in the SD Act). Intelligence collection by its nature is less targeted than evidence-gathering. Using a network activity warrant, the AFP or ACIC may need to collect intelligence on a large number of unknown devices, the users and owners of which are not able to be identified or located, before seeking more targeted warrants that authorise gathering evidence (such as computer access warrants under the SD Act). It will be difficult, if not impossible, for an issuing authority to assess the privacy implications for multiple unknown persons to a sufficient degree to meet the threshold of a specific requirement to consider the privacy of third parties. Instead, the issuing authority must consider the extent to which the execution of a network activity warrant is likely to result in access to data of persons who are lawfully using a computer. The proportionality test requires that the issuing authority weigh up the anticipated value of the intelligence sought with the activities authorised by the warrant. This ensures that the issuing authority must balance the utility of the network activity warrant in obtaining information about the criminal network against the scale, scope and intrusiveness of the activities authorised by that warrant. To further ensure that these warrants are proportionate to the activity they authorise, the issuing authority must consider the existing of any alternative or less intrusive means of obtaining the information sought.

Privacy consideration for account takeover warrants

For account takeover warrants, the magistrate must consider the extent to which the privacy of any person is likely to be affected. An explicit privacy consideration is appropriate for the issue of account takeover warrants as it is a targeted evidence gathering power. This is consistent with the approach for existing electronic surveillance powers, such as those in the SD Act.

When deciding whether to issue the warrant, the magistrate must also have regard to the nature and gravity of the alleged offence that founded the application for the warrant. This may involve consideration of the seriousness of the offence and the scale at which the offence has been, or will be, committed. Consideration of this matter ensures that the magistrate will be able to assess the reasonableness and proportionality of

executing the warrant in the circumstances. If the offence for which the warrant is sought is not sufficiently serious to justify the conduct of an account takeover warrant and its impact on privacy, the magistrate can decide not to issue the warrant.

d. how the qualification that the statutory conditions do not limit the conditions to which a data disruption warrant or account takeover warrant may be subject would operate in practice. In particular, would this qualification allow an issuing authority to authorise an action that can only be executed in a manner that results in loss or damage to data or causes the permanent loss of money, digital currency or property

The Bill provides for statutory conditions to which data disruption warrants and account takeover warrants must be subject. These conditions place limitations on the execution of the warrant. If the warrant is executed in a way that breaches the statutory condition then that conduct would be unlawful, as it is not supported by the warrant. As identified by the Committee, the Bill provides that the statutory conditions do not limit the conditions to which a data disruption warrant or an account takeover warrant may be subject. This refers to the ability of the issuing authority to specify any conditions subject to which things may be done under the warrant (subparagraph 27KD(1)(b)(ix) in the SD Act and subparagraph 3ZZUQ(1)(b)(ix) of the Crimes Act). The statutory conditions do not restrict the issuing authority's ability to prescribe additional conditions under those provisions, to which the execution of the warrant would then also be subject.

As noted by the Committee, the statutory conditions provide that if loss or damage to data occurs during the execution of a warrant, the damage must be justified and proportionate to the offence being targeted by the warrant. Whether loss or damage that may possibly occur during execution of the warrant is justified and proportionate will need to be considered by the issuing authority on a case-by-case basis. Warrants must also not be executed in a manner that causes a person to suffer a permanent loss of money, digital currency or property (other than data). This is intended for an abundance of clarity about the scope of the warrants. Interference with a person's money, digital currency or property that is not data is not the intended purpose of either of these warrants. The issuing authority's ability to prescribe additional conditions does not allow authorisation of an action that can only be executed in a manner that results in loss or damage to data or causes the permanent loss of money, digital currency or property.

e. whether all of the exceptions to the restrictions on the use, recording or disclosure of protected information obtained under the warrants are appropriate and whether any exceptions are drafted in broader terms than is strictly necessary

All information collected under the warrants in this Bill is strictly protected. Information is broadly prohibited from being used or disclosed.

Where there are exceptions to that prohibition, those exceptions are necessary to enable the warrants to be effective, strong oversight and accountability mechanisms, proper and appropriate judicial processes to be carried out, information sharing necessary for agencies to carry out their functions, or in emergency circumstances. The ability to use and disclose information has been designed to be limited to only that which is necessary.

Prohibition and offences

The Bill classifies data disruption warrant information as 'protected information' under the existing provisions in the SD Act, which currently govern information collected under other warrants in that Act, for example, computer access warrants.

Information gathered under an account takeover warrant is also classified as 'protected information'. This is a new concept in the Crimes Act introduced by the Bill, borrowing from the SD Act, so that account takeover warrant information is governed by the same prohibitions and exceptions as most information under the SD Act, including data disruption warrant information.

There is also a prohibition on using and disclosing 'protected network activity warrant information', a new category of protected information introduced by the Bill into the SD Act. Protected network activity warrant information is information obtained under, or relating to, a network activity warrant including information obtained from the use of a surveillance device under a network activity warrant but not including information obtained through interception. This also includes any information that is likely to enable the identification of the criminal network of individuals, individuals in that network, computers used by that network, or premises at which computers used by that network are located. Information that was obtained in contravention of a requirement for a network activity warrant is also captured by this definition.

A person commits an offence if he or she uses, records, communicates or publishes protected information or protected network activity warrant information except in very limited circumstances. The Bill also provides for an aggravated offence if this disclosure endangers the health or safety or any person or prejudices the effective conduct of an investigation.

Exceptions - data disruption warrants and account takeover warrants

The exceptions to the prohibition on using, recording, communicating or publishing information collected under a data disruption warrant and under an account takeover warrant are the same as exceptions in the SD Act that relate to existing warrants, such as computer access warrants.

It is permitted to use, record, communicate, publish, and admit in evidence, protected information where necessary for the investigation of a relevant offence, a relevant proceeding, or the making of a decision as to whether or not to bring a prosecution for a relevant offence (amongst

other limited purposes). It is also permitted to use, record, communicate or publish protected information where that information has already been disclosed in proceedings in open court lawfully, and where the communication of the information is necessary to help prevent or reduce the risk of serious harm.

Information collected under each of these warrants may also be shared with an intelligence agency if the information relates to a matter that is relevant to the agency's functions, and with a foreign country, the International Criminal Court, or a War Crimes Tribunal under international assistance authorisations, and also where authorised by the *Mutual Assistance in Criminal Matters Act 1987* or the *International Criminal Court Act 2002*. It is essential that this information sharing is permitted, in order to facilitate investigations that involve other Australian agencies (for example conducting joint operations) and foreign jurisdictions. Further information is outlined below, as requested by the Committee, on the right to privacy, life and prohibition against torture or cruel, inhuman or degrading treatment or punishment, in the context of the Bill's framework for information sharing with foreign countries.

Information may also be shared with the Ombudsman and the IGIS, and between those agencies to allow them to fulfil their oversight responsibilities in relation to the powers in the Bill.

Exceptions - network activity warrants

The exceptions to the general prohibition on using and disclosing protected network activity warrant information are configured differently to those relating to data disruption warrants and account takeover warrants. This is because, as network activity warrants are for intelligence purposes, they cannot be used to gather evidence in investigations, and the information collected generally cannot be adduced in evidence in a criminal proceeding.

Protected network activity warrant information may be used or disclosed if necessary for collecting, correlating, analysing or disseminating, or the making of reports in relation to, criminal intelligence in the performance of the legislative functions of the AFP or the ACIC. The information can also be the subject of derivative use allowing it to be cited in an affidavit on application for another warrant (which will themselves contain protections on information gathered). This will assist in ensuring that network activity warrants can be useful in furthering investigations into criminal conduct made under subsequent warrants.

Protected network activity warrant information cannot be used in evidence in criminal proceedings, other than for a contravention of the secrecy provisions that apply to this intelligence. This is important for ensuring that where a person has unlawfully used or disclosed this information, he or she may be effectively investigated and prosecuted for the offence. The information may also be disclosed for the purposes of the admission of evidence in a proceeding that is not a criminal proceeding.

This is intended to allow protected network activity warrant information to be used in other proceedings, such as those that question the validity of the warrant. Therefore, if a case is brought to challenge the decision to issue a warrant, there will be evidence which can be validly drawn upon. These exceptions are intended to protect the rights of persons who are the subject of, or whose information has been collected under, a network activity warrant.

The ability to share information obtained under a network activity warrant with ASIO or an intelligence agency is intended to facilitate joint operations between the AFP and the ACIC and other members of the National Intelligence Community. These agencies currently conduct complex and interrelated intelligence operations, and may need to share information to support activities within their respective functions, in particular those in relation to safeguarding national security. For example, information collected under a network activity warrant about a terrorist organisation may be shared with ASIO if related to ASIO's functions. Information held by ASIO and intelligence agencies, including information obtained under a network activity warrant that is then communicated to those agencies, is protected by strict use and disclosure provisions in the *Australian Security Intelligence Organisation Act 1979* and *Intelligence Services Act 2001*.

To ensure compliance with reporting and record-keeping requirements, the Bill provides that protected network activity warrant information may be used or disclosed for the purpose of keeping records and making reports by the AFP and the ACIC in accordance with the obligations imposed by the Bill. Information may also be shared with the Ombudsman and the IGIS, and between those agencies to allow them to fulfil their oversight responsibilities in relation to the powers in the Bill. These exceptions are important to facilitate effective oversight of the AFP and the ACIC and protect the rights of persons who are the subject of, or whose information has been collected under, a network activity warrant. Information held by the Ombudsman and IGIS, including information obtained under a network activity warrant that is then communicated to those bodies, is protected by strict use and disclosure provisions in the *Ombudsman Act 1976* and *Inspector-General of Intelligence and Security Act 1986*.

f. why the bill does not include provision for public interest monitors or a similar safeguard to protect the rights of the affected person in warrant application and review proceedings

Consistent with covert powers available to the AFP and the ACIC under existing legislation, the Bill does not make provision for public interest monitors to assess applications for warrants before they can be issued. In particular, this is in accordance with the approach for surveillance device warrants and computer access warrants in the SD Act. At present, public interest monitors recognised under the TIA Act only exist within Victoria

and Queensland, as a corollary of Victorian and Queensland legislation that established those offices within those jurisdictions, for functions that include but are not limited to considering Victorian and Queensland agency applications for interception warrants. These authorities perform an oversight role of their jurisdiction's law enforcement agencies when applying for interception warrants. The Commonwealth, and other States and Territories, have not legislated for this office within their jurisdictions.

To protect the rights of an affected person, the warrants in the Bill are supported by a range of safeguards, stringent thresholds and oversight arrangements which ensure that they may only be sought where reasonable, proportionate and necessary.

Each of the warrants can only be applied for by the AFP or the ACIC on the basis of a link to serious offending. Specifically, the warrants must be sought in respect of relevant offences, that is, generally offences punishable by a maximum term of imprisonment of three years or more. This threshold limits the availability of data disruption warrants, network activity warrants and account takeover warrants to serious crimes, such as terrorism, child exploitation and drugs and firearms trafficking.

All of the warrants in the Bill must be sought by way of application to a judicial officer or AAT member, who may grant the warrant sought if they are satisfied that there are reasonable grounds for the suspicion founding the application for each warrant. Oversight of decisions to apply for warrants by judicial officers and AAT members provides for independent scrutiny of the warrant application and satisfaction of reasonableness and proportionality.

As described above, a key matter that the issuing authority is required to take into account in deciding whether to issue each of the warrants is consideration of proportionality. The issuing of a data disruption warrant or network activity warrant must meet a proportionality test. This is to ensure that the use of these warrants is proportionate to the alleged or suspected offending in all circumstances. An explicit privacy consideration is included for the issue of account takeover warrants as it is a targeted evidence gathering power.

Central amongst other considerations that issuing authorities must take into account is consideration of the existence of any alternative means of achieving the objective of the warrant. These safeguards are particularly important for ensuring that avenues of investigation, information collection or disruption that are less intrusive on privacy are considered. This ensures that, where there are narrower activities that involve a more targeted approach, this will be taken into account by the issuing authority.

Moreover, decisions made in regard to the issue of warrants in the Bill can be challenged through judicial review. Australian courts will retain their jurisdiction to review administrative decisions, including any decision to issue a warrant, through the original jurisdiction of the High Court of Australia and under the ADJR Act. This will ensure that an affected person

has an avenue to challenge the decisions to issue warrants made by issuing authorities. The availability of judicial review is discussed in further detail below.

As with other evidence-gathering powers in the SD Act and Crimes Act, the Commonwealth Ombudsman will have oversight of the use of data disruption warrants and account takeover warrants by the AFP and the ACIC. The Bill provides for oversight of network activity warrants by the Inspector General of Intelligence and Security. The IGIS will be empowered to review the activities of the AFP and the ACIC in relation to network activity warrants for legality, propriety and consistency with human rights. This is consistent with the IGIS's oversight of other agencies' intelligence collection powers.

g. why the chief officer is not required to review the continued need for the retention of records or reports comprising protected information on a more regular basis than every five years

Records comprising protected information in the Bill must be destroyed as soon as practicable if the material is no longer required, and at most within five years of the material no longer being required (unless a relevant officer certifies certain matters that go to the need to keep the material for ongoing activity). As noted by the Committee, the chief officer of the AFP or the ACIC must ensure that information obtained under each of these warrants is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report. This is consistent with existing recordkeeping and destruction obligations in relation to surveillance device warrants and computer access warrants in the SD Act.

As with information collected under existing warrants in the SD Act, the ability to retain information for five years reflects the fact that some investigations and operations are complex and run over a long period of time. Requiring the security and destruction of records ensures that the private data of individuals accessed under a warrant is only handled by those with a legitimate need for access, and is not kept in perpetuity where there is not a legitimate reason for doing so. The Ombudsman and IGIS are empowered to assess compliance with record-keeping and destruction requirements as part of their oversight of powers in the Bill.

Right to an effective remedy

a. whether a person who was the subject of a warrant will be made aware of that after the investigation has been completed

In accordance with existing practice for covert powers under Commonwealth legislation, persons of interest or those who are subject to the new covert warrants in the Bill do not have to be notified of the use of powers against them unless there is a specific requirement under law to do so. This is consistent practice for covert warrants under the SD Act and other Commonwealth legislation that confers covert powers upon law enforcement and security agencies, such as the TIA Act.

If a person were to become aware of the use of a covert warrant while an investigation or operation is ongoing, this could place law enforcement outcomes at risk by tipping off those engaging in criminal conduct about the investigation or operation and, potentially, the capabilities and methodologies being employed. Notifying a person after the conclusion of an investigation or operation can also have significant ramifications for future law enforcement methodologies and the legitimate need to keep technical capabilities that relate to electronic surveillance confidential.

Public disclosure of the details of a covert warrant or the information collected under it may reveal to criminal entities and organisations that using that particular service is subject to, or could be subject to, electronic surveillance. For example, knowing that a certain website or forum is being monitored under a network activity warrant may mean that many months or years of law enforcement efforts to penetrate criminal networks (such as online child sexual abuse groups) can be lost. This ultimately reduces the effectiveness of the AFP and the ACIC to keep the Australian community safe from serious online crime.

Even where the subject of a warrant has been cleared of any criminal activity, this does not necessarily reduce the risk that the disclosure may impact future law enforcement methodologies and protection of technical capabilities. For example, the person who holds the account subject to an account takeover warrant could inadvertently jeopardise future law enforcement investigations by publicly announcing they were subject to the warrant in relation to an account on a particular electronic service.

While the Government acknowledges that the use of a covert warrant will impact a person's privacy, this limitation is reasonable, necessary and proportionate in order to safeguard the Australian community from serious crime. These measures are balanced with strict safeguards, including restrictions on the use and disclosure of information obtained under a warrant, and robust oversight and reporting requirements. In particular, the Commonwealth Ombudsman and the IGIS will inspect and review agencies' use of the warrants in the Bill.

b. if not, how such a person would effectively access a remedy for any violation of their right to privacy

Although a person would not be notified that data relating to them has been obtained under a warrant in the Bill, measures are in place to protect an individuals' right to privacy and right to an effective remedy. The Bill balances the impact on privacy and the covert nature of powers by ensuring independent authorisation of warrants, as well as effective oversight, record-keeping and reporting. In particular, there is aggregated public annual reporting on the AFP and ACIC's use of powers in the Bill.

Importantly, a person who is the subject of a warrant can challenge decisions made in regard to data disruption warrants, network activity warrants and account takeover warrants through judicial review. As these are covert powers, in practice the challenge to these decisions will likely

only be if and when the particular investigation has become overt. For example, a person who is the subject of a warrant may become aware of this during the preparation for or conduct of criminal proceedings.

To make information available in order to bring about such a challenge, the Bill ensures that, although network activity warrants are not for evidence collection and therefore there are strict prohibitions on adducing that information in evidence in proceedings, information obtained under a network activity warrant may be admitted into evidence in proceedings that are not criminal proceedings. This is an important exception to the general secrecy provisions that apply to covert intelligence gathering activities. The Bill also applies the same exception to information gathered under an account takeover warrant.

Australian courts will retain their jurisdiction to review administrative decisions, including any decision to issue a warrant, through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia by operation of subsection 39B(1) of the *Judiciary Act 1903*. This will ensure that an affected person has an avenue to challenge the decisions to issue warrants made by issuing authorities. The availability of judicial review is discussed in further detail below.

As outlined above, decisions made under the SD Act and the Crimes Act are not exempt from judicial review under the ADJR Act. The Bill does not seek to depart from this precedent for the three new warrant it introduces. The human rights compatibility statement in the explanatory memorandum supporting the Bill will be amended to reflect this.

While judicial review is available, agency decisions to exercise a power and issuing authority decisions to issue warrants are not subject to merits review. This is consistent with longstanding principles and practice relating to national security legislation and powers.²⁹ However, a defendant may seek to challenge evidence obtained under a warrant, should this evidence be used in the course of an eventual prosecution.

The use of powers in the Bill will be independently overseen by the Commonwealth Ombudsman (for data disruption warrants and account takeover warrants) and the IGIS (for network activity warrants). While this is not a merits review process, these oversight bodies play an important role in auditing and inspecting the records of agencies which increases transparency and accountability, and monitors and encourages compliance with the legislative requirements in the Bill.

29 Decisions of a law enforcement and national security nature were identified by the Administrative Review Council in its publication 'What decisions should be subject to merits review as being unsuitable for merits review'.
<https://www.arc.gov.au/Publications/Reports/Pages/Downloads/Whatdecisionsshouldbesubjecttomeritreview1999.aspx>

Concluding comments

International human rights legal advice

Right to privacy

2.66 Noting that the measure pursues the legitimate objectives of protecting national security, ensuring public safety and addressing online crime, the key question is whether the measure is proportionate to achieving these objectives. Of particular relevance in assessing proportionality is whether the measure is: accompanied by sufficient safeguards, only as extensive as is strictly necessary and the least rights restrictive means of achieving the stated objectives.³⁰ European Court of Human Rights case law offers some useful guidance as to 'minimum safeguards that should be set out in law to avoid abuses of power' in the context of secret measures of surveillance.³¹ Such safeguards include:

the nature of offences which may give rise to an interception order; the definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be following for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed.³²

2.67 The European Court of Human Rights has reiterated the 'importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information' and collect masses of data.³³ The preliminary analysis noted that the bill contains a number of important safeguards, including some of the minimum safeguards identified by the European Court of Human Rights, that assist with the proportionality of the measure.³⁴

30 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [73]: the Court held that the test of strict necessity is to be applied in the context of secret surveillance, stating that 'given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity"'. The Court further stated that a secret surveillance measure must be strictly necessary in two aspects: for safeguarding democratic institutions and for obtaining vital intelligence in an individual operation.

31 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [56]–[57].

32 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [56].

33 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [68].

34 See Parliamentary Joint Committee on Human Rights, Report 1 of 2021 (3 February 2021), pp. 20–43.

However, questions were raised as to whether some of these safeguards would be adequate in all circumstances. The adequacy of those safeguards is assessed below in light of the minister's advice.

Issuing authority

2.68 Regarding the conferral of power to members of the AAT to issue a data disruption warrant and a network activity warrant, the minister stated that the issuing authority should not be limited to only judicial authority, but should include nominated AAT members, in line with existing legislation. The minister stated that AAT members issue similar warrants under existing legislation and thus have the skills and experience to assess applications for data disruption and network activity warrants and to make independent decisions about compliance of those applications with the bill. Regarding the independence of the AAT, the minister acknowledged that the AAT is not independent of government in the same way that the judiciary is, but that its independence arises from its role in reviewing the merits of administrative decisions made under Commonwealth laws as well as the fact that members can only be terminated by the Governor-General on specific grounds. The minister further noted that the power to issue warrants is conferred on AAT members in their personal capacity acting as independent decision-makers rather than exercising formal judicial or administrative powers. Finally, the minister stated that there is no requirement under international human rights law for Australia to specify a judicial authority to authorise investigatory powers, as reflected in existing legislation dealing with surveillance warrants.

2.69 While not an absolute requirement, judicial authorisation of surveillance activities is considered 'best practice' in international human rights law jurisprudence.³⁵ Indeed, the European Court of Human Rights has held that 'judicial control [offers] the best guarantees of independence, impartiality and a proper procedure'³⁶ and that 'control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close

35 See *Case of Big Brother Watch and Others v The United Kingdom*, European Court of Human Rights, Application nos. 58170/13, 62322/14 and 24960/15 (2019) [320]. See also *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, Application no. 47143/06 (2015) [233]; *Klass and Others v Germany*, European Court of Human Rights, Application no. 5029/71 (1978) [55]; *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [77].

36 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, Application no. 47143/06 (2015) [233]. See also *Klass and Others v Germany*, European Court of Human Rights, Application no. 5029/71 (1978) [55]: 'The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure'.

scrutiny'.³⁷ The United Nations (UN) Human Rights Committee has also recommended that States parties provide for 'judicial involvement in the authorization or monitoring of surveillance measures' and consider establishing 'strong and independent oversight mandates with a view to preventing abuses'.³⁸ Noting that the proposed issuing authority for data disruption and network activity warrants includes a nominated AAT member, it is necessary to closely scrutinise whether it is appropriate in the circumstances to entrust supervisory control to a non-judicial officer. A key consideration in this regard is whether the issuing 'authority is sufficiently independent from the executive'.³⁹ The fact that AAT members are the issuing authority under existing legislation is not an adequate justification to depart from best practice under international human rights law.

2.70 There remain concerns that AAT members do not have all the necessary attributes of a permanent independent judicial authority.⁴⁰ AAT members do not have security of tenure, with each term of appointment being for a period of at most seven years, although members may be eligible for re-appointment.⁴¹ In another context, the UN Human Rights Committee has recognised security of tenure as an important attribute of judicial independence.⁴² The fact that AAT members are conferred power in their personal capacity and may only be terminated by the Governor-General on specific grounds does not alleviate concerns that AAT members have weaker credentials for independence than judges. Additionally, AAT members generally do not have the same level of expertise as judges, with potentially only five

37 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [77].

38 UN Committee on Human Rights, *Concluding observations on the fourth periodic report of the United States of America*, CCPR/C/USA/CO/4 (2014) [22]. See also UN Special Rapporteur on the right to privacy, *Draft Legal Instrument on Government-led Surveillance and Privacy*, Version 0.6 (2018), p. 16.

39 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [77].

40 See United Nations Special Rapporteur on the right to privacy, *Draft Legal Instrument on Government-led Surveillance and Privacy*, Version 0.6 (2018), p. 16: the UN Special Rapporteur on the right to privacy stated that where domestic law provides for the use of surveillance systems, the law shall 'provide that the individual concerned is likely to have committed a serious crime or is likely to be about to commit a serious crime and in all such cases such domestic law shall establish that an independent authority, having all the attributes of permanent independent judicial standing, and operating from outside the law enforcement agency or security or intelligence agency concerned, shall have the competence to authorise targeted surveillance using specified means for a period of time limited to what may be appropriate to the case'.

41 *Administrative Appeals Tribunal Act 1975*, section 8.

42 United Nations Human Rights Committee, *General Comment No. 32. Article 14: Right to equality before courts and tribunals and to a fair trial* (2007) [19].

years' experience as a legal practitioner.⁴³ Noting the expansive powers that the bill seeks to introduce and the likely significant interference with the right to privacy arising from the exercise of these powers, there are serious concerns that the right to privacy may not be adequately safeguarded by conferring AAT members with the power to issue data disruption and network activity warrants.

Mandatory considerations prior to issuing warrants

2.71 The preliminary analysis noted that a number of the mandatory considerations that issuing authorities would be required to have regard to prior to issuing a warrant would likely serve as important safeguards to mitigate the risk of arbitrary interference with the right to privacy. The requirements to consider the extent to which the privacy of any person would likely be affected, including the privacy of third parties, and whether the warrant is proportionate having regard to the nature and gravity of the offence, were highlighted as having particular safeguard value. As such, further information was sought as to why these considerations were not mandatory with respect to all warrants, noting that certain mandatory considerations would only apply to specific warrants.

2.72 The minister noted that the considerations specified in relation to each warrant were specifically designed with regard to the objective and contemplated operation of each of the warrants. Regarding the data disruption warrant, the minister stated that a requirement to consider privacy, particularly with respect to third parties, is not appropriate, notwithstanding that it is appropriate in the context of other evidence gathering electronic surveillance warrants. The minister explained that the purpose of a data disruption warrant is to frustrate criminal activity and that it may not always be possible, at the time of applying for a warrant, for agencies to estimate the full extent to which the activity authorised by the warrant may impact the privacy of third parties. As such, rather than providing for an express privacy consideration in relation to the data disruption warrant, the bill requires that the issuing authority must be satisfied that, amongst other things, the disruption of data authorised by the warrant is justifiable and proportionate having regard to the offences targeted, as well consideration of any alternative means of frustrating the offences. The minister stated that this proportionality requirement ensures the issuing authority weighs the benefits of targeting the particular offences with the likely effect that the warrant could have beyond frustrating those offences. Additionally, the minister stated that the likely value of the information sought is not relevant with respect to data disruption warrants because the purpose is to frustrate crime, not to collect evidence or intelligence.

43 AAT members must have been enrolled as a legal practitioner for at least 5 years or in the opinion of the Governor-General, have special knowledge and skills relevant to their duties as either a Deputy President, senior member or member: *Administrative Appeals Tribunal Act 1975*, section 7.

2.73 Regarding network activity warrants, the minister stated that the purpose of these warrants is to gather intelligence, and this, by its nature, is less targeted than evidence-gathering. The minister noted that the AFP or ACIC may need to use a network activity warrant to collect intelligence on a large number of unknown devices, the users and owners of which are not able to be identified or located, before seeking more targeted warrants that authorise gathering evidence. As such, the minister stated that it will be difficult, if not impossible, for an issuing authority to assess the privacy implications for multiple unknown persons to a sufficient degree to meet the threshold of a specific requirement to consider the privacy of third parties. Instead, the minister noted that the issuing authority must have regard to the extent to which the execution of the network activity warrant is likely to result in access to data of persons lawfully using a computer; questions of proportionality; and any alternative, or less intrusive, means of obtaining the information.

2.74 The proportionality of the measure is assisted by the requirement to consider the existence of any alternative or less intrusive means of achieving the objective of the warrants, and the requirement that the warrants be justifiable and proportionate having regard to the offences (in the case of data disruption warrants) or the likely intelligence value of information sought to be obtained (in the case of network activity warrants). However, noting the very broad range of activities that may be authorised by the warrants, including adding, copying, deleting or altering personal data, intercepting passing communications and using a surveillance device, and as a consequence, the substantial interference with the right to privacy, it remains unclear why privacy, including with respect to third parties, is not a mandatory consideration in relation to data disruption and network activity warrants. Although it may be difficult to estimate the full extent to which the privacy of all persons is likely to be affected by the warrants, this is not an adequate justification for excluding privacy entirely as a consideration to which the issuing authority must have regard. It is noted that other covert powers and surveillance warrants require privacy to be considered by the issuing authority.⁴⁴

2.75 Additionally, without requiring the issuing authority to consider the extent to which the activities authorised by the warrants would interfere with the right to privacy, it is difficult to assess whether the measure is sufficiently circumscribed and the potential interference with privacy is only as extensive as is strictly necessary. In the context of mass surveillance and other broad measures to collect and retain communications data of large populations, the European Court of Human Rights has emphasised the importance of precisely circumscribing the extent of interference

44 See eg *Surveillance Devices Act 2004*, section 16(2)(c) with respect to a surveillance device warrant and section 27C(2)(c) with respect to a computer access warrant; *Telecommunications (Interception and Access) Act 1979*, section 46(2)(a) with respect to a telecommunications service warrant and section 46A(2)(a) with respect to a named person warrant.

with fundamental rights, notably the right to privacy, to ensure that the interference is limited to what is strictly necessary.⁴⁵ Where a measure applies to a broad range of 'persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime', the European Court of Human Rights has held that the consequent interference with privacy may not be limited to what is strictly necessary.⁴⁶ In the case of network activity warrants in particular, there is a risk that interference with privacy may not be limited to what is strictly necessary in all circumstances. This is because the warrant would apply to a large number of unknown persons for whom there may not be evidence to suggest a direct link to crime. Indeed, the bill provides that it is immaterial whether the identities of the individuals in the group or the details of the relevant offences can be ascertained.⁴⁷

2.76 Regarding account takeover warrants, while the issuing authority must have regard to privacy, they are not required to expressly consider whether the warrant is proportionate. The minister stated that the issuing authority must have regard to the nature and gravity of the alleged offence, and this consideration may involve an assessment of the seriousness and scale of the offence and the reasonableness and proportionality of executing the warrant in the circumstances. The minister noted that if the offence for which the warrant is sought is not sufficiently serious to justify the activities authorised by the warrant and its impact on privacy, the issuing authority may not issue the warrant. While the issuing authority *may* consider proportionality when having regard to the matters specified in proposed subsection 3ZZUP(2), it is not a legislative requirement to do so. An express consideration of whether the warrant is proportionate having regard to the matters set out in proposed subsection 3ZZUP(2) would strengthen this safeguard. Considering the proportionality of the warrant having regard to the nature and

45 *Digital Rights Ireland Ltd v Ireland*, European Court of Human Rights (Grand Chamber), Joined Cases C-293/12 and C-594/12 (2014) [65]. More generally, at [54], the Court stated that 'the EU legislation in question must lay down clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data'.

46 *Digital Rights Ireland Ltd v Ireland*, European Court of Human Rights (Grand Chamber), Joined Cases C-293/12 and C-594/12 (2014) [58]: regarding whether the interference caused by European Union Directive 2006/24, which authorised the collection and retention of communications data of 'practically the entire European population', was limited to what was strictly necessary, the Court stated that the Directive 'affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime'.

47 Schedule 2, item 8, proposed subsection 7A(2).

gravity of the offence is particularly important given that the warrants relate to a broad range of offences, not merely limited to those offences that would be considered serious crime.⁴⁸

Statutory limits on interference with data and property

2.77 As noted in the preliminary analysis, the statutory limits on interference with data and property and the additional statutory conditions with respect to data disruption and account takeover warrants requiring that loss or damage to data in the execution of the warrants be justified and proportionate, would appear to be important safeguards against arbitrary interference with privacy. However, questions were raised as to whether the strength of this safeguard would be weakened by the qualification that the statutory conditions do not limit the conditions to which a warrant may be subject. The minister stated that the statutory conditions place limitations on the execution of the warrant and if the warrant is executed in a way that breaches these conditions, then that conduct would be unlawful. The minister clarified that the statutory conditions do not restrict the issuing authority's ability to prescribe additional conditions under those provisions, to which the execution of the warrant would then also be subject. The minister noted that the issuing authority's ability to prescribe additional conditions does not allow authorisation of an action that can only be executed in a manner that results in loss or damage to data or causes the permanent loss of money, digital currency or property. Based on the minister's advice, it appears that while the statutory conditions do not, by implication, limit the issuing authority's ability to prescribe conditions, the issuing authority is not authorised to prescribe a condition which could only be executed in a manner that results in loss or damage to data or causes the permanent loss of money, digital currency or property. On this basis, it appears that the statutory qualification would not lessen the effectiveness of this safeguard in practice. Noting the complexity of this provision, it would assist with statutory interpretation if the explanatory memorandum were updated to reflect the minister's advice.⁴⁹

Restrictions on the use and disclosure of protected information

2.78 The preliminary analysis noted that restrictions regarding the use and disclosure of protected information and the prohibition of unauthorised use or disclosure of protected information may operate as an important safeguard. However, questions were raised as to whether this safeguard is weakened by the broad range of exceptions to the statutory protections contained in the bill.

2.79 The minister stated that the exceptions are necessary to enable the warrants to be effective, and the ability to use and disclose information is limited to only that

48 A relevant offence is an offence which carries a maximum sentence of imprisonment of 3 years or more: *Surveillance Devices Act 2004*, section 6.

49 *Acts Interpretation Act 1901*, section 15AB(2)(e).

which is necessary. The minister noted that protected information collected under each of the warrants may be shared with an intelligence agency if the information relates to a matter that is relevant to the agency's functions, as well as with a foreign country and international criminal bodies. The minister stated that such exceptions to the restrictions on disclosure of protected information are essential to facilitate joint operations and investigations that involve multiple Australian and/or foreign agencies.

2.80 As noted in the preliminary analysis, some of these exceptions, particularly those which allow protected information to be disclosed to intelligence agencies, including in foreign countries, would appear to be broadly framed, thereby creating a risk that information obtained under a warrant for a specified purpose may be shared for other broader purposes, potentially unrelated to the objectives of the bill. The European Court of Human Rights has highlighted the importance of external supervision and remedial measures in the context of governments 'transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance'.⁵⁰ The Court found 'external, preferably judicial, *a posteriori* control of secret surveillance activities, both in individual cases and as general supervision' to be of particular importance.⁵¹ It observed:

The significance of this control cannot be overestimated in view of the magnitude of the pool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks.⁵²

2.81 The bill does not contain such a control mechanism whereby an independent, preferably judicial, authority has oversight or control over the provisions which authorise the onwards disclosure of protected information. Noting that the exceptions allow for the onwards disclosure of a potentially expansive scope of protected information to a broad range of agencies, there are concerns that some of the exceptions may be drafted in broader terms than is strictly necessary, thus weakening the safeguard value of provisions restricting the use and disclosure of protected information. The potential implications on the right to life and the prohibition against torture or cruel, inhuman or degrading treatment or punishment arising from information sharing provisions are further discussed below at paragraph [2.121] onwards.

50 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [78].

51 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [79].

52 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [79].

Storage and destruction of protected information

2.82 The minister noted that records comprising protected information must be destroyed as soon as practicable if the material is no longer required, and at most within five years of the material no longer being required, unless the material is required to be kept for ongoing activity. The minister stated that the ability to retain information for five years reflects the fact that some investigations and operations are complex and run over a long period of time. The minister also noted that requiring the security and destruction of records ensures that the private data of individuals accessed under a warrant is only handled by authorised persons and is not kept in perpetuity without a legitimate reason.

2.83 As noted in the preliminary analysis, the requirement that protected information be securely stored and destroyed within a specified period of time may operate as a safeguard against arbitrary interference with privacy. However, it remains unclear whether the time limit of five years is an appropriate period of time for the purposes of operating as an effective safeguard.⁵³ While some investigations may be complex and protracted and so require records to be retained for a longer period of time, other investigations may not be and thus regular review of the need to retain records is important to ensure that records are destroyed as soon as practicable and not retained for the maximum period of five years by default. It seems that requiring the chief officer to more regularly review the continued need for the retention of records or reports would be a less rights restrictive approach, noting that the retention of protected information collected under the warrants is in itself an interference with the right to privacy.

Oversight frameworks and access to review

2.84 Regarding oversight frameworks, the minister stated that the Commonwealth Ombudsman will have oversight of the use of data disruption and account takeover warrants and the Inspector-General of Intelligence and Security (IGIS) will have oversight of the use of network activity warrants. In relation to the latter, the minister stated that the IGIS will be empowered to review the AFP or ACIC activities to ensure they are legal, proper and consistent with human rights. Protected information may be disclosed to IGIS for the purposes of the IGIS official exercising powers, or performing functions or duties, as an IGIS official.⁵⁴ The

53 In *Roman Zakharov v Russia*, the European Court of Human Rights held that the 'six-month storage time-limit set out in Russian law for such data reasonable. At the same time, it deplore[d] the lack of a requirement to destroy immediately any data that are not relevant for the purpose for which they have been obtained...the automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8': *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, Application no. 47143/06 (2015) [254].

54 Schedule 1, item 35, proposed subsection 45(6A); Schedule 3, item 4, proposed section 3ZZVH(5).

availability of oversight by the Commonwealth Ombudsman and IGIS may serve as an important safeguard against arbitrary and unlawful interference with privacy. As recommended by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'there must be no secret surveillance system that is not under review of an independent oversight body and all interferences must be authorised through an independent body'.⁵⁵

2.85 However, the strength of these oversight frameworks will depend on the broader legislative context. In the case of this bill, the IGIS has raised concerns that there may be challenges in effectively exercising its oversight functions in practice. The IGIS stated that:

effective oversight is more readily achieved where the scope and content of intelligence or law enforcement powers are articulated clearly and fully on the face of the legislation and where consistency is sought, where possible, across like regimes. This is especially so in respect of coercive or covert powers.⁵⁶

2.86 In the case of this bill, the IGIS has stated that the cascading definitions in relation to network activity warrants are 'complex and potentially unclear in scope'.⁵⁷ For example, there is discrepancy between the definitions of a 'criminal network of individuals' and an 'electronically linked group of individuals'.⁵⁸ There is also no requirement that the identities of the individuals in the group, the details of the relevant offences or the target computer and its location be known and specified for the purpose of applying for a network activity warrant.⁵⁹ The IGIS has noted that these 'complex and potentially unclear' definitions 'could create challenges for IGIS oversight, including in determining the legality and propriety of particular action purportedly taken pursuant to a warrant'.⁶⁰ Additionally, in relation to ensuring the conduct of agencies pursuant to a network activity warrant is consistent with human rights, the IGIS noted that given the absence of privacy as an express consideration in

55 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/HRC/13/37 (2009) [62].

56 Inspector-General of Intelligence and Security, *Submission 18*, p. 8 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*.

57 Inspector-General of Intelligence and Security, *Submission 18*, p. 9 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*.

58 Schedule 2, item 3, amended subsection 6(1) and item 8, proposed section 7A.

59 Schedule 2, item 8, proposed subsection 7A(2) and item 9, proposed subsection 27KK(2).

60 Inspector-General of Intelligence and Security, *Submission 18*, p. 9 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*.

proposed subsection 27KM(2), it is unclear the 'extent to which the right to privacy is intended to guide the use of network activity warrants'.⁶¹ The IGIS further noted the absence of a maximum timeframe within which a report must be provided to the minister.⁶² These comments by the IGIS suggest that while the proposed oversight framework has potential safeguard value, its effectiveness in practice will depend on the clarity, precision and scope of the legislation.

2.87 Regarding availability of review, the minister stated that Australian courts will retain their jurisdiction to review administrative decisions, including any decision to issue a warrant, through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia.⁶³ The minister noted that the bill does not exclude judicial review under the *Administrative Decisions (Judicial Review) Act 1977*, advising that the statement of compatibility was incorrect and will be amended accordingly. The minister stated that judicial review will ensure that an affected person has an avenue to challenge any decision to issue a warrant. The minister also noted that oversight of applications for warrants by either a judge, AAT member or magistrate ensures independent scrutiny of warrant applications.

2.88 While judicial review of a decision to issue a warrant is available, external merits review is not. Judicial review in Australia represents a limited form of review in that it allows a court to consider only whether the decision was lawful (that is, within the power of the relevant decision maker). The court cannot undertake a full review of the facts (that is, the merits), as well as the law and policy aspects of the original decision to determine whether the decision is the correct or preferable decision. While access to review is an important safeguard, its effectiveness may be weakened by the lack of access to merits review.

2.89 Additionally, there are serious concerns that access to judicial review may not be effective in practice. Noting the covert nature and purpose of the measure, persons whose privacy would be interfered with are highly unlikely to be aware that they are the subject of a warrant application and will invariably be excluded from participating in the application proceedings. As there is no requirement to notify the affected person once a warrant has been issued, it appears highly unlikely that the person will be able to effectively access judicial review. As the bill provides no mechanism or avenue through which the affected person can represent their interests or challenge a warrant application, the preliminary analysis raised questions

61 Inspector-General of Intelligence and Security, *Submission 18*, p. 10 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*.

62 Inspector-General of Intelligence and Security, *Submission 18*, p. 11 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*.

63 By operation of subsection 39B(1) of the *Judiciary Act 1903* or under the *Administrative Decisions (judicial Review) Act 1977*.

as to why additional safeguards, such as public interest monitors,⁶⁴ are not available. The minister stated that consistent with existing legislation, the bill does not provide for public interest monitors and that the Commonwealth and states and territories (other than Victoria and Queensland) have not legislated for public interest monitors.

2.90 While it is accepted that there is no public interest monitor office at Commonwealth level, the minister's response does not address the substantive question of why a safeguard along these lines cannot be included in the bill. To counterbalance the fact that the affected person is not able to be personally represented at the application for the warrant, a public interest monitor or other independent expert could appear at the hearing to test the content and sufficiency of the information relied on, to question any person giving information, and to make submissions as to the appropriateness of granting the application. As the European Court of Human Rights has held:

the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his rights.⁶⁵

2.91 Public interest monitors or an equivalent mechanism would be a valuable safeguard to protect the interests of the affected person in any warrant application or review proceedings.

2.92 In conclusion, noting that the measure will have the effect of substantially interfering with the right to privacy, the existence of strong safeguards is critical to ensure that such interference is lawful, not arbitrary and only as extensive as is strictly necessary. The bill contains some important safeguards, such as the requirement that issuing authorities have regard to alternative, less intrusive means of achieving the objective of the warrant, and discontinuance and revocation provisions would apply where the warrant is no longer necessary. However, there remain concerns that these safeguards are not sufficient in all circumstances. Noting that judicial authorisation of surveillance warrants is considered best practice in international human rights law, the proposed conferral of issuing powers to AAT members may not be appropriate as they do not appear to have all the attributes of a permanent independent judicial authority. Regarding the mandatory considerations to which an issuing authority must have regard, an express

64 Such as the Victorian or Queensland Public Interest Monitor. See eg *Telecommunications (Interception and Access) Act 1979* in relation to Public Interest Monitors (for example, see section 44A, 45, 46 and 46A).

65 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, application no. 47143/06 (4 December 2015) [233].

consideration of privacy and proportionality for all warrants would strengthen this safeguard by ensuring that the measure is sufficiently circumscribed and that any interference with privacy is only as extensive as is strictly necessary. There remain concerns that some of the exceptions to the restrictions on the use and disclosure of protected information are broadly framed and not accompanied by independent oversight mechanisms, which may weaken the safeguard value of these provisions. Additionally, while the oversight functions of the Commonwealth Ombudsman and the IGIS are an important safeguard, there is no access to merits review and limited access to effective judicial review because the person whose right to privacy is limited will be unaware of the use of the warrant against them. As such, there is some risk that this measure may constitute an arbitrary limitation on the right to privacy.

Right to an effective remedy

2.93 The minister stated that, consistent with the existing practice for covert powers under Commonwealth legislation, persons of interest or those who are subject to the new warrants do not have to be notified of the use of powers against them. The minister explained that if the person were to become aware of the use of a covert warrant against them, there is a risk they may tip off those engaging in criminal conduct about the investigation and potentially the capabilities and methodologies of surveillance being employed, which could compromise law enforcement outcomes. The minister stated that notifying a person after the conclusion of an investigation could also have significant ramifications for future law enforcement operations, methodologies and technical capabilities. The minister stated that these risks of disclosure are not reduced where a person who was the subject of a warrant has been cleared of any criminal activity. The minister acknowledged that the measure limits a person's privacy but states that there are safeguards in place, particularly the oversight functions of the Commonwealth Ombudsman and IGIS, and access to judicial review. Although regarding the latter, the minister noted that as these are covert powers, in practice the challenge to these decisions will likely only be if and when the particular investigation has become overt, for example, in preparation for, or during, criminal proceedings.

2.94 As discussed above at paragraphs [2.84]–[2.91], the oversight functions of the Commonwealth Ombudsman and IGIS may serve as a useful safeguard to ensure decision-makers are complying with the legislation. However, this oversight framework will not provide a remedy to individuals whose right to privacy may be violated. The only remedy available to individuals would be judicial review. However, given the covert nature of the measure and the broad concealment powers, it would appear that judicial review is not an effective remedy in practice. Indeed, the minister has advised that the person whose right to privacy may be violated will not be notified of the use of a covert warrant against them, even following the conclusion of the investigation or where a person has been cleared of any criminal activity. Where a person is unaware that they are the subject of a warrant and that

their privacy has been interfered with, they will not be able to practically seek judicial review of the decision and thus do not have access to an effective remedy. United Nations bodies and the European Court of Human Rights have provided specific guidance as to what constitutes an effective remedy where personal information is being collected in the context of covert surveillance activities. While effective remedies can take a variety of forms, they must be known and accessible to anyone with an arguable claim that their rights have been violated.⁶⁶ The European Court of Human Rights has held that:

the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively.⁶⁷

2.95 The European Court of Human Rights acknowledged that, in some instances, notification may not be feasible where it would jeopardise long-term surveillance activities.⁶⁸ However, it explained that:

[a]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned.⁶⁹

2.96 Given that the measure does not require the person whose privacy might be violated to be notified of such a violation and, as advised by the minister, there is no intention to notify such persons even after the conclusion of an investigation, it does not appear that such a person could have access to an effective remedy for any potential violation of their right to privacy. The existence of other safeguards and oversight frameworks, none of which offer an individual remedy or access to merits

66 Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age (A/HRC/27/37) [40].

67 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [86]. See also *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, Application no. 47143/06 (2015) [234] and *Klass and Others v Germany*, European Court of Human Rights, Plenary Court, Application no. 5029/71 (1978) [57].

68 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, Application no. 47143/06 (2015) [287].

69 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, Application no. 47143/06 (2015) [287]. See also *Klass and Others v Germany*, European Court of Human Rights, Plenary Court, Application no. 5029/71 (1978) [58] and *Szabó and Vissy v Hungary*, European Court of Human Rights, Application no. 37138/14 (2016) [86].

review, are unlikely to be sufficient to fulfil the international standard required for an effective remedy.

Committee view

2.97 The committee thanks the minister for this response. The committee notes that the bill seeks to introduce new law enforcement and intelligence gathering powers and warrants to enhance the ability of the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to frustrate crime and gather intelligence and evidence of criminal activity. Specifically, the committee notes that the bill would introduce three new warrants, including data disruption warrants, network activity warrants and account takeover warrants.

2.98 The committee considers that to the extent that the new powers and warrants would facilitate the investigation, disruption and prevention of serious crimes against persons, including in particular protecting children from harm and exploitation, the measure may promote multiple rights, including the right to life and the rights of the child.

2.99 However, the committee notes that the measure also engages and limits the right to privacy by authorising the AFP and ACIC to access, use, modify and store an individual's personal data and information. The committee notes that the right to privacy may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate.

2.100 The committee considers that the measure pursues the legitimate objective of seeking to protect national security and ensure public safety, and these law enforcement and intelligence gathering powers and warrants would appear to be rationally connected to that objective. However, the committee notes that questions remain as to whether there are sufficient safeguards to ensure the measure is proportionate. The committee notes that the measure contains some important safeguards such as the requirement that issuing authorities have regard to alternative, less intrusive means of achieving the objective of the warrant; protected information is to be kept in a secure location; records or reports containing protected information are to be destroyed as soon as practicable; and discontinuance and revocation provisions would apply where the warrant is no longer necessary.

2.101 However, the committee is concerned that these safeguards may not be sufficient in all circumstances. Noting that judicial authorisation of surveillance warrants is considered best practice in international human rights law, the committee is concerned that conferring issuing powers to AAT members may not be appropriate as they do not appear to have all the attributes of a permanent independent judicial authority. Further, the committee notes that there is no requirement that privacy and proportionality be considered before all types of warrants are issued.

2.102 The committee also notes that some of the exceptions to the restrictions on the use and disclosure of protected information are broadly framed, which may weaken the safeguard value of these restrictions. While the oversight frameworks are an important safeguard, the committee notes there is limited access to effective review as the person whose right to privacy is limited will be unaware of the use of the warrant against them. Given the covert nature of the measure and the absence of a requirement to notify the person whose privacy is affected of the use of the warrant, the committee considers that where a person's right to privacy is violated, they may not have access to an effective remedy.

Suggested action

2.103 The committee considers that the proportionality of this measure, particularly as regards the right to privacy, may be assisted were the bill amended to provide that:

- (a)** the power to issue data disruption and network activity warrants is only conferred on judges;
- (b)** with respect to data disruption and network activity warrants, the issuing authority must have regard to the extent to which the privacy of any person is likely to be affected by the warrant;
- (c)** with respect to account takeover warrants, the issuing authority must have regard to whether the warrant is proportionate having regard to the matters set out in proposed subsection 3ZZUP(2);
- (d)** some form of control mechanism is introduced whereby an independent, preferably judicial, authority has oversight or control over the provisions which authorise the onwards disclosure of protected information, particularly disclosure to foreign countries;
- (e)** the chief officer reviews the continued need for the retention of records or reports comprising protected information on a more regular basis than every five years; and
- (f)** a public interest monitor office or equivalent safeguard be established to ensure an independent expert can appear at the hearing of an application for a warrant to test the content and sufficiency of the information relied on, question any person giving information, and make submissions as to the appropriateness of granting the application.

2.104 The committee recommends that consideration be given to updating the statement of compatibility with human rights and explanatory memorandum to reflect the information which has been provided by the minister.

2.105 The committee draws these human rights concerns to the attention of the minister and the Parliament.

Assistance orders

2.106 The bill would allow the AFP or ACIC to apply to an eligible judge, nominated AAT member or magistrate for an assistance order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to do a specified thing with respect to data disruption, network activity or account takeover warrants.⁷⁰ A specified person includes a person reasonably suspected of having committed the alleged offence as well as third parties who may have relevant knowledge, such as an employee of the owner of the computer that holds data sought to be obtained.⁷¹ A person would commit an offence if they are subject to an assistance order, are capable of complying with a requirement in the order and they fail to comply with the requirement of the order.⁷² The maximum penalty for contravention of an assistance order is 10 years imprisonment.

Summary of initial assessment

Preliminary international human rights legal advice

Right to privacy

2.107 To the extent that the measure may compel a person to provide personal information to the AFP or ACIC, such as a password to access their computer or other personal device, or information enabling the decryption of personal data, the measure engages and limits the right to privacy. 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.⁷³ It also includes the right to control the dissemination of information about one's private life. The right to privacy may be subject to permissible limitations which are provided by law and are not arbitrary. In order for limitations not to be arbitrary, the measure must pursue a legitimate objective, and be rationally connected to (that is, effective to achieve) and proportionate to achieving that objective. The statement of compatibility does not identify that the right to privacy is engaged and limited by this

70 Schedule 1, item 47, proposed section 64B; Schedule 2, items 30 and 31; Schedule 3, item 4, proposed section 3ZZVG.

71 Schedule 1, item 47, proposed section 64B; Schedule 3, item 4, proposed section 3ZZVG.

72 Schedule 1, item 47, proposed subsection 64B(3); Schedule 2, item 30; Schedule 3, item 4, proposed subsection 3ZZVG(3).

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

measure, and as such does not provide an assessment as to the compatibility of assistance orders with the right to privacy.

2.108 In order to assess the compatibility of this measure with the right to privacy, in particular the adequacy of the safeguards that apply, further information is required as to:

- (a) why the issuing authority is not required to be satisfied that an assistance order is justifiable and proportionate, having regard to the offences to which it would relate, with respect to all warrants, noting that this criterion only applies to an assistance order with respect to data disruption warrants; and
- (b) whether the measure is accompanied by any other safeguards that would ensure that any interference with the right to privacy is not arbitrary and only as extensive as is strictly necessary.

Committee's initial view

2.109 The committee noted that this measure would appear to engage and limit the right to privacy insofar as it may compel a person to provide personal information to the AFP or ACIC. The committee considered that the measure pursues the legitimate objective of combatting serious online crime, and as the assistance order would facilitate the investigation and disruption of crime, the measure is rationally connected to this objective. The committee considered further information was required to assess the proportionality of the measure and sought the minister's advice as to the matters set out at paragraph [2.108].

2.110 The full initial analysis is set out in [Report 1 of 2020](#).

Minister's response

2.111 The minister advised:

Right to privacy

- a. **why the issuing authority is not required to be satisfied that an assistance order is justifiable and proportionate, having regard to the offences to which it would relate, with respect to all warrants, noting that this criterion only applies to an assistance order with respect to data disruption warrants**
- b. **whether the measure is accompanied by any other safeguards that would ensure that any interference with the right to privacy is not arbitrary and only as extensive as is strictly necessary.**

As the committee notes, an eligible Judge or nominated AAT member must be satisfied that disruption of data held in a computer is justifiable and proportionate, having regard to the offences targeted, before granting an assistance order in support of a data disruption warrant. This is because the criterion upon which the granting an assistance order is assessed

reflects the criterion of which the issuing authority must be satisfied when authorising the supporting warrant.

In order to issue a data disruption warrant, an eligible Judge or nominated AAT member must (amongst other things) be satisfied that there are reasonable grounds for the suspicion of the law enforcement officer who made the warrant application that the disruption of data is likely to substantially assist in frustrating the commission of relevant offences. The eligible Judge or nominated AAT member must also be satisfied that the disruption of data authorised by the warrant is justifiable and proportionate, having regard to the offences targeted (subsection 27KC(1) of the SD Act).

These are similar conditions for which an eligible Judge or nominated AAT member must be satisfied of when granting an assistance order in support of a data disruption warrant (subsection 64B(2) of the SD Act). Satisfaction of the similar matters at the time of issuing the warrant and the granting of the assistance order ensures that any activity required by an assistance order does not extend beyond the scope of the underpinning warrant.

The same principles apply in relation to the granting of assistance orders supporting network activity warrants and account takeover warrants. Similar matters that must be satisfied at the time of issuing these warrants must again be satisfied at the granting of an assistance order.

In recognition of the impact on privacy of third parties, the issuing authority is required to have regard to certain specified matters when deciding whether to issue the warrant. For network activity warrants, this includes consideration of whether the activities authorised by the warrant are proportionate to the likely value of intelligence to be collected, as well as the extent to which the warrant is likely to result in access to data of persons lawfully using a computer. For account takeover warrants, this includes taking into account the extent to which the privacy of any person is likely to be affected. Consideration of these matters will inform the issuing authority's decisions to issue warrants, including his or her satisfaction of the matter particular to that warrant and, in turn, inform decisions about whether to grant an assistance order. Ensuring that the issuing authority is required to be satisfied of justifiability and proportionality before a warrant can be issued or assistance order granted is intended to safeguard against any undue impact on privacy.

Concluding comments

International human rights legal advice

Right to privacy

2.112 Regarding the criteria to which the issuing authority must be satisfied prior to granting an assistance order, the minister stated that these reflect the criteria to which the issuing authority must be satisfied when authorising the supporting warrant. The minister noted that satisfaction of similar matters at the time of issuing

the warrant and the granting of the assistance order will ensure that any activity required by an assistance order does not extend beyond the scope of the underpinning warrant. The minister did not address whether the measure is accompanied by any other safeguards.

2.113 As noted in the preliminary analysis, with respect to assistance orders relating to data disruption warrants, the criterion that disruption of data held in the computer is justifiable and proportionate, having regard to the offences, may assist with the proportionality of the measure by ensuring that any interference with privacy is only as extensive as is strictly necessary. Noting the safeguard value of this criterion, it remains unclear why this criterion, as well as an express consideration of the extent to which the privacy of any person is likely to be affected, should not apply to assistance orders with respect to all warrants. Such criteria are particularly important given that the penalty for non-compliance with an assistance order is imprisonment for 10 years and the measure has the potential to substantially interfere with the right to privacy of third parties, including persons who have no direct link to serious crime and potentially a remote link to the person suspected of having committed the offence (such as a person who is a system administrator for the computer system).

Committee view

2.114 The committee thanks the minister for this response. The committee notes that the bill would allow the AFP or ACIC to apply to an eligible judge, nominated AAT member or magistrate for an assistance order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to do a specified thing with respect to the warrants.

2.115 The committee notes that this measure would appear to engage and limit the right to privacy insofar as it may compel a person to provide personal information to the AFP or ACIC. The committee notes that the right to privacy may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate. The committee considers that the measure pursues the legitimate objective of combatting serious online crime, and as the assistance order would facilitate the investigation and disruption of crime, the measure is rationally connected to this objective.

2.116 Regarding proportionality, the committee notes that the criteria to which the issuing authority must be satisfied prior to granting an assistance order may operate to help safeguard the right to privacy. However, the committee considers that these criteria could be strengthened.

Suggested Action

2.117 The committee considers that the proportionality of this measure may be assisted were the bill amended to provide that in relation to assistance orders in support of all warrants, the issuing authority must be satisfied that an assistance order is justifiable and proportionate, having regard to the relevant offences and the extent to which the privacy of any person is likely to be affected.

2.118 The committee recommends that consideration be given to updating the statement of compatibility with human rights to reflect the information which has been provided by the minister.

2.119 The committee draws these human rights concerns to the attention of the minister and the Parliament.

Information sharing with foreign governments

2.120 The bill would allow protected information obtained under the warrants to be disclosed to foreign countries in certain circumstances. For example, protected information obtained under an account takeover warrant and a network activity warrant (other than through the use of a surveillance device), may be used or disclosed in connection with the functions of the AFP under section 8 of the *Australian Federal Police Act 1979*.⁷⁴ The AFP's functions include providing police services to assist or cooperate with a foreign law enforcement or intelligence or security agency.⁷⁵

Summary of initial assessment

Preliminary international human rights legal advice

Right to privacy, life, and prohibition against torture or cruel, inhuman or degrading treatment or punishment

2.121 By authorising the sharing of protected information to foreign governments the measure engages and limits the right to privacy. 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.⁷⁶ It also includes the right to control the dissemination of information about one's private life.

74 Schedule 2, item 19, proposed subsection 45B(5)(a); Schedule 3, item 4, proposed subsection 3ZZVH(3)(b).

75 *Australian Federal Police Act 1979*, subsection 8(1)(bf).

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

2.122 To the extent that the measure authorises protected information to be shared with foreign police, intelligence or security agencies and results in the investigation and prosecution of an offence that is punishable by the death penalty in that foreign country, the measure may also engage and limit the right to life.⁷⁷ The right to life imposes an obligation on Australia to protect people from being killed by others or from identified risks. While the International Covenant on Civil and Political Rights does not completely prohibit the imposition of the death penalty, international law prohibits states which have abolished the death penalty (such as Australia) from exposing a person to the death penalty in another state.⁷⁸ The provision of information to other countries that may be used to investigate and convict someone of an offence to which the death penalty applies is also prohibited.⁷⁹ In 2009, the UN Human Rights Committee stated its concern that Australia lacks 'a comprehensive prohibition on the providing of international police assistance for the investigation of crimes that may lead to the imposition of the death penalty in another state', and concluded that Australia should take steps to ensure it 'does not provide assistance in the investigation of crimes that may result in the imposition of the death penalty in another State'.⁸⁰

2.123 Additionally, the sharing of protected information, including personal information, with foreign countries, may, in some circumstances, expose individuals to a risk of torture or other cruel, inhuman or degrading treatment or punishment. International law absolutely prohibits torture and cruel, inhuman or degrading treatment or punishment.⁸¹ There are no circumstances in which it will be permissible to subject this right to any limitations.

2.124 In order to fully assess the compatibility of the measure with the rights to privacy and life as well as the prohibition against torture or cruel, inhuman or other degrading treatment or punishment, further information is required as to

- (a) what is the objective being pursued by the measure and how is the measure rationally connected to that objective;
- (b) what safeguards are in place to ensure that protected information obtained under the warrants is not shared with a foreign country in circumstances that could expose a person to the death penalty or to

77 International Covenant on Civil and Political Rights, article 6(1) and Second Optional Protocol to the International Covenant on Civil and Political Rights, article 1.

78 Second Optional Protocol to the International Covenant on Civil and Political Rights.

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

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

81 International Covenant on Civil and Political Rights, article 7; Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.

torture or cruel, inhuman or degrading treatment or punishment. In particular, why is there no legislative requirement that where there are substantial grounds for believing there is a real risk that disclosure of information to a foreign government may expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment, protected information must not be shared with that government.

Committee's initial view

2.125 The committee noted that the disclosure of protected information with foreign police, intelligence or security agencies engages and limits the right to privacy. To the extent that there may be a risk that disclosure of protected information to a foreign country could expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment, the measure may also engage and limit the right to life and have implications for the prohibition against torture or cruel, inhuman or degrading treatment or punishment. The committee considered further information was required to assess the human rights implications of this bill, and accordingly sought the minister's advice as to the matters set out at paragraph [2.124].

2.126 The full initial analysis is set out in [Report 1 of 2020](#).

Minister's response

2.127 The minister advised:

Information sharing with foreign governments - right to privacy, life and prohibition against torture or cruel, inhuman or degrading treatment or punishment

- a. **what is the objective being pursued by the measure and how is the measure rationally connected to that objective**
- b. **what safeguards are in place to ensure that protected information obtained under the warrants is not shared with a foreign country in circumstances that could expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment. In particular, why is there no legislative requirement that where there are substantial grounds for believing there is a real risk that disclosure of information to a foreign government may expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment, protected information must not be shared with that government**

As noted by the Committee, the Bill provides that information obtained under these warrants may be shared with foreign governments in certain limited circumstances. The AFP's primary aim is to enforce Commonwealth criminal law and contribute to combatting complex, transnational and organised crime which impacts on the Australian community and Australia's national interests. The AFP collaborates with national and

international partners to enhance the safety of the Australian community and provide a more secure regional and global environment. The ACIC works to identify new and emerging serious and organised crime threats and criminal trends, to create a national strategic intelligence picture across the spectrum of crime, fill intelligence and knowledge gaps and share information and intelligence holdings to inform national and international responses to crime. This necessarily requires cooperation between the AFP and the ACIC and foreign police and law enforcement agencies. The ACIC has a specific power in the *Australian Crime Commission Act 2002 (Cth)* (ACC Act), its underpinning legislation, in support of this collaboration.⁸²

The criminal activity targeted by the Bill - serious crime occurring on the dark web or facilitated by anonymising technology - is an increasing global problem. Cooperation with foreign law enforcement partners can be crucial to identifying and targeting criminal activity which harms the Australian community, as well as building a high-risk, hostile environment for cyber criminals both onshore and offshore. That is why the Bill ensures that the AFP and the ACIC will be able to share information obtained under the warrants with foreign governments in accordance with their existing functions.

Importantly, in cooperating with foreign law enforcement agencies, the AFP and the ACIC operate in accordance with Australia's longstanding bipartisan opposition to the death penalty and the existing death penalty safeguards across the full spectrum of Australia's international crime cooperation frameworks.

For example, there are a number of safeguards that apply when cooperating with foreign countries through the mutual assistance framework. Provision of any evidentiary material, including protected information, to a foreign country is subject to the requirements of the *Mutual Assistance in Criminal Matters Act 1987*. A request for assistance must be refused where (i) a person has been arrested, detained, charged or convicted in relation to an offence where the death penalty may be imposed in the foreign country, and (ii) where there are substantial grounds for believing that, if the request were granted, a person would be in danger of being subjected to torture.

In addition to the protections which apply under the Bill in relation to the disclosure of information to foreign agencies, section 59AA of the ACC Act contains additional safeguards. Under section 59AA, the authorising officer must be satisfied that the disclosure is appropriate and the information is relevant to a permissible purpose as defined in section 4 of the ACC Act. In considering whether a disclosure will be appropriate, amongst other factors, the authorising officer must take into account the ACIC Death

82 See s17(2) *Australian Crime Commission Act 2002 (Cth)* (ACC Act)

Penalty and Foreign Disclosure Policy (which aligns to the AFP's *Practical Guide on international police-to-police assistance in potential death penalty situations*) where:

- A member of the staff of the ACIC proposes that information be disseminated to a foreign agency or international body or otherwise disclosed to a foreign official;
- The information relates to an offence that may have been committed and that could be prosecuted in the home country of the agency or official, or in a country to which the international body might be expected to disclose the information (the foreign country);
- Under the law of the foreign country, the offence is a death penalty offence; unless:
 - No person has been arrested, detained, charged or convicted for the offence in the foreign country; and
 - Providing the information is not reasonably likely to result in a person being arrested, detained, charged or convicted for the offence in the foreign country.

On a police-to-police basis, the AFP has strict national guidelines which govern the provision of information in situations which could expose a person to the death penalty. The AFP's *Practical Guide on international police-to-police assistance in potential death penalty situations* requires Ministerial approval of assistance in any case in which a person has been arrested, detained, charged with, or convicted of, an offence that carries the death penalty. Where a person is yet to be arrested, detained, charged or convicted of a death penalty offence, the Guide requires senior AFP management to consider a set of prescribed factors before providing police assistance to foreign countries. Examples of these factors include the age and personal circumstances of the person and the seriousness of the suspected criminal activity. In particular, these guidelines were updated in 2016 to response to recommendations made by the Joint Standing Committee on Foreign Affairs, Defence and Trade in its report 'A world without the death penalty: Australia 's advocacy for the abolition of the death penalty.'

Information sharing with foreign governments

International human rights legal advice

Right to privacy, life, and prohibition against torture or cruel, inhuman or degrading treatment or punishment

2.128 Regarding the objective of the measure, the minister stated that allowing the AFP and the ACIC to share information obtained under the warrants with foreign governments is necessary to ensure that these agencies can effectively perform their functions. The minister stated that the AFP's functions include enforcing Commonwealth criminal law and combatting complex, transnational and organised

crime. The ACIC's functions include identifying new and emerging serious and organised crime threats and criminal trends, creating a national strategic intelligence picture, and sharing information and intelligence holdings to inform national and international responses to crime. The minister stated that these functions necessarily require cooperation between the AFP and ACIC and foreign police and law enforcement agencies. Such cooperation, the minister explained, is crucial to identifying and targeting criminal activity which harms the Australian community and to building a high-risk, hostile environment for cyber criminals.

2.129 Regarding the possibility that the measure engages and limits the right to life or engages the prohibition against torture or cruel, inhuman or degrading treatment or punishment, the minister noted that in cooperating with foreign law enforcement agencies, the AFP and ACIC operate in accordance with Australia's longstanding bipartisan opposition to the death penalty and the death penalty safeguards that exist in Australia's international crime cooperation frameworks. In particular, the minister identified the requirements under the Mutual Assistance Act as a primary safeguard. A further safeguard identified by the minister is the *Australian Crime Commission Act 2002*, which requires an authorising officer to be satisfied that the disclosure of information to foreign agencies is appropriate and the information is relevant to a permissible purpose.⁸³ A permissible purpose is defined broadly and includes preventing, detecting, investigating, prosecuting or punishing criminal offences, contraventions of law or seriously improper conduct, enforcing laws (including foreign laws) relating to proceeds of crime and unexplained wealth, protecting public revenue, developing government policy and researching criminology.⁸⁴ The minister stated that in considering whether it is appropriate to disclose the information, the authorising officer must take into account internal policies and guidance which requires ministerial approval of assistance in any case where a person is arrested, detained, charged with, or convicted of an offence that carries the death penalty. Where a person has not yet been arrested, detained, charged or convicted of a death penalty offence, the minister stated that the AFP must have regard to prescribed factors before providing assistance to foreign countries, such as the age and personal circumstances of the person and the seriousness of the offence.

2.130 In relation to the right to privacy, the objective of combatting transnational crime and identifying and responding to organised crime threats and trends would appear to be a legitimate objective for the purposes of international human rights law. Sharing protected information, including evidence and intelligence obtained under the warrants, with foreign intelligence and law enforcement agencies would appear to be rationally connected to this objective insofar as it would facilitate

83 *Australian Crime Commission Act 2002*, section 59AA.

84 *Australian Crime Commission Act 2002*, section 4.

cooperation between agencies and joint police investigations and enforcement operations.

2.131 As regards the existence of safeguards with respect to the right to privacy, the minister referred to the protections which generally apply under the bill in relation to the disclosure of information to foreign agencies. As discussed above at paragraphs [2.78]–[2.81], the bill does not contain any type of control mechanism whereby an independent, preferably judicial, authority has oversight or control over the provisions which authorise the onwards disclosure of protected information, including to foreign countries. While there are provisions that restrict the use and disclosure of protected information, there are concerns that some of the exceptions may be drafted in broader terms than is strictly necessary, thereby creating a risk that information obtained under a warrant for a specified purpose may be shared for other broader purposes. Questions remain as to what other safeguards are in place to ensure that the limit on the right to privacy is proportionate. For example, it is not clear that there are measures to ensure that any information shared is only used for the specified purpose and that adequate privacy protections are in place, such as protections around the handling of personal information both before and after it is disclosed, and protection of personal information from unauthorised disclosure by a foreign country.

2.132 As regards the strength of the identified protections with respect to the right to life and the prohibition against torture or cruel, inhuman or degrading treatment or punishment, the Mutual Assistance Act provides that a request by a foreign country for assistance under the Act must be refused if the offence is one in respect of which the death penalty may be imposed.⁸⁵ However, the Act qualifies this by stating that this prohibition will not apply if ‘the Attorney-General is of the opinion, having regard to the special circumstances of the case, that the assistance requested should be granted’.⁸⁶ Consequently, it appears that the Mutual Assistance Act creates a risk of facilitating the exposure of individuals to the death penalty.⁸⁷ The Mutual Assistance Act provides stronger protections with respect to the prohibition against torture. It provides that a request by a foreign country for assistance under the Act shall be refused if, in the opinion of the Attorney-General, there are substantial grounds for believing that, if the request was granted, the person would be in danger of being subjected to torture.⁸⁸ However, this protection does not extend to cruel, inhuman or degrading treatment or punishment. As such, while the

85 *Mutual Assistance in Criminal Matters Act 1987*, subsection 8(1A).

86 *Mutual Assistance in Criminal Matters Act 1987*, subsection 8(1A).

87 This was previously observed by the Parliamentary Joint Committee on Human Rights in 2013. See, Parliamentary Joint Committee on Human Rights, *Report 6 of 2013*, Mutual Assistance in Criminal Matters (Cybercrime) Regulation 2013, pp. 167-169.

88 *Mutual Assistance in Criminal Matters Act 1987*, subsection 8(1)(ca).

Mutual Assistance Act would operate as a safeguard to protect persons from exposure to torture, it may not provide full protection against the sharing of information that could lead to the death penalty and to cruel, inhuman or degrading treatment or punishment.

2.133 Furthermore, while the government may intend to act consistently with its policy to oppose the death penalty and in accordance with policies and practical guidelines regarding international police assistance, it is not a legal requirement in the bill to do so. The UN Human Rights Committee has previously raised concerns that Australia lacks 'a comprehensive prohibition on the providing of international police assistance for the investigation of crimes that may lead to the imposition of the death penalty in another state', and concluded that Australia should take steps to ensure it 'does not provide assistance in the investigation of crimes that may result in the imposition of the death penalty in another State'.⁸⁹ The measure also does not prohibit the sharing of information with a foreign country in circumstances that could expose a person to torture or cruel, inhuman or degrading treatment or punishment. Without a comprehensive prohibition, the relevant policies and guidelines may be insufficient for the purpose of meeting Australia's obligations with respect to the right to life and the prohibition on torture or cruel, inhuman or degrading treatment or punishment.

Committee view

2.134 The committee thanks the minister for this response. The committee notes that the bill would allow protected information obtained under the warrants to be shared with foreign countries in certain circumstances. The committee notes that the disclosure of protected information with foreign police, intelligence or security agencies engages and limits the right to privacy. The committee notes that this right may be subject to permissible limitations if it is shown to be reasonable, necessary and proportionate. The committee considers that the measure pursues the legitimate objective of combatting transnational crime and identifying and responding to organised crime threats and trends. However, the committee notes that questions remain as to whether the proposed limitation on the right to privacy is proportionate, noting that few safeguards have been identified by the minister.

2.135 In addition, to the extent that there may be a risk that disclosure of protected information to a foreign country could expose a person to the death penalty or to ill treatment, the committee notes that the measure may also engage and limit the right to life and have implications for the prohibition against torture or cruel, inhuman or degrading treatment or punishment. The committee notes the minister's advice that there are a number of safeguards that apply when the AFP and ACIC cooperates with foreign countries through the mutual assistance

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

framework, including in the existing *Mutual Assistance in Criminal Matters Act 1987* and guidelines relating to international police assistance. The committee also notes and welcomes the advice that the government intends to act consistently with its opposition to the death penalty.

2.136 While the Mutual Assistance Act would operate as a safeguard to protect persons from exposure to torture it may not provide full protection against the sharing of information that could lead to the death penalty and to cruel, inhuman or degrading treatment or punishment. The committee notes that the other safeguards identified by the minister may, to some extent, mitigate the risk. However, noting that there is no legislative requirement to prohibit the sharing of protected information in circumstances that may expose a person to a real risk of the death penalty being applied or to ill treatment, the committee considers that discretionary considerations and the limited protections afforded under the Mutual Assistance Act may be insufficient for the purpose of meeting Australia's obligations with respect to the right to life and the prohibition on cruel, inhuman or degrading treatment or punishment.

Suggested action

2.137 The committee considers that the proportionality of this measure with the right to privacy may be assisted were the bill amended to provide that:

- (a) when considering disclosure of protected information to a foreign country, an individual's right to privacy is considered, including the likely extent of interference with the privacy of any person or persons so as to ensure that any limitation on the right to privacy is only as extensive as is strictly necessary; and
- (b) prior to sharing information with a foreign country, the authorised officer must be satisfied that adequate privacy protections are in place around the handling of personal information and protection of personal information from unauthorised disclosure by a foreign country.

2.138 The committee considers that the compatibility of this measure with the right to life and the prohibition against torture or cruel, inhuman or degrading treatment or punishment may be assisted were the bill amended to provide that where there are substantial grounds for believing there is a real risk that disclosure of information to a foreign country may expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment, protected information must not be shared with that country.

2.139 The committee recommends that consideration be given to updating the statement of compatibility with human rights to reflect the information which has been provided by the minister.

2.140 The committee draws these human rights concerns to the attention of the minister and the Parliament.

Dr Anne Webster MP

Chair