Chapter 1
New and ongoing matters

1.1 The committee comments on the following legislative instruments, and in some instances, seeks a response or further information from the relevant minister.

Legislative instruments

International Organisations (Privileges and Immunities) (Declaration of Organisation for Joint Armament Co-operation) Regulations 2024[7]

FRL No.	F2024L00731
Purpose	The regulation declares the Organisation for Joint Armament Co-operation (OCCAR) to be an international organisation under the *International Organisations (Privileges and Immunities) Act 1963*
Portfolio	Foreign Affairs and Trade
Authorising legislation	*International Organisations (Privileges and Immunities) Act 1963*
Disallowance	15 sitting days after tabling (tabled in the House of Representatives on 24 June 2024 and in the Senate on 25 June 2024. Notice of motion to disallow must be given by 22 August 2024 in the House and by 9 September 2024 in the Senate)[8]
Rights	Fair hearing (access to courts and tribunals); effective remedy; torture and inhuman treatment

Extending privileges and immunities

1.2 The regulation declares the Organisation for Joint Armament Co-operation (OCCAR) to be an international organisation under the *International Organisations (Privileges and Immunities) Act 1963* (the Act). OCCAR is a European inter-governmental organisation that manages arms procurement and support. Australia is a non-member participating in selected OCCAR programmes.[9]

---

7 This entry can be cited as: Parliamentary Joint Committee on Human Rights, International Organisations (Privileges and Immunities) (Declaration of Organisation for Joint Armament Co-operation) Regulations 2024, *Report 7 of 2024*; [2024] AUPJCHR 48.

8 In the event of any change to the Senate or House's sitting days, the last day for the notice would change accordingly.

9 Explanatory statement, p. 1.

1.3 The Act was amended in late 2023 to enable an organisation of which two or more countries other than Australia are members, or that is constituted by two or more persons representing countries other than Australia, to be declared, by way of regulations, to be an international organisation to which the Act applies.[10] This permitted Australia to confer privileges and immunities under the Act on international organisations of which Australia is not a member. The statement of compatibility accompanying the International Organisations (Privileges and Immunities) Amendment Bill 2023 (now Act) noted that the amendments would facilitate Australia giving effect to a Framework Agreement relating to the OCCAR.[11]

1.4 The regulation confers privileges and immunities to specified categories of OCCAR personnel and representatives of countries other than Australia in accordance with section 6 of the Act. The Act allows for the grant of both functional immunity (that is, immunity that attaches to those acts or functions undertaken by an individual in their official capacity as an officer of an international organisation) and personal immunity (that is, an absolute immunity attaching to all acts undertaken in an official or private capacity both before and during office).[12] The Act therefore allows individuals to be conferred with immunity from personal arrest or detention, and from suit and from other legal process.[13]

1.5 The regulations also repeal the International Organisations (Privileges and Immunities) (Declaration of Organisation for Joint Armament Co-operation Related Meetings) Regulations 2022.[14] The explanatory statement states that those regulations were an interim measure to declare OCCAR to be an 'overseas

---

10 International Organisations (Privileges and Immunities) Amendment Bill 2023 (now Act).

11 Framework Agreement between the Government of Australia and the Organisation for Joint Armament Cooperation (Organisation Conjointe de Cooperation en matière d'Armement (OCCAR)) for the participation of Australia in OCCAR-managed programmes [2022] ATS 3. International Organisations (Privileges and Immunities) Amendment Bill 2023, statement of compatibility, p. 2.

12 Personal immunities which may be granted to representatives of international organisations are set out under Part 1 of the Second to Fifth Schedules of the *International Organisations (Privileges and Immunities) Act 1963*. Personal and functional immunities are also granted under other legislation, such as those accorded to a diplomatic agent, under the *Diplomatic Privileges and Immunities Act 1967*, specifically the Schedule – Vienna Convention on Diplomatic Relations. The *Foreign States Immunities Act 1985* also provides functional immunity to foreign states and their representatives in civil proceedings, and personal immunity from both civil and criminal proceedings for foreign heads of state (s 36).

13 See Parts 1 and 2 of the Second to Fifth Schedules of the *International Organisations (Privileges and Immunities) Act 1963.*

14 Schedule 1, item 1.

organisation' and conferred a limited range of privileges and immunities to participants attending OCCAR-related meetings held in Australia.[15]

International human rights legal advice

Right of access to courts and tribunals, right to an effective remedy and obligations under the Convention Against Torture

1.6 By extending a broader set of privileges and immunities to OCCAR (of which Australia is not a member) and to associated persons, these regulations engage and limit the right of access to courts and tribunals—an element of the right to equality before courts and tribunals. The regulations also engage the right to an effective remedy and Australia's obligations to investigate and prosecute (or extradite) persons alleged to have committed torture.[16] The statement of compatibility only identifies that the regulations engage the right to an effective remedy.[17]

Background

1.7 When the committee examined the International Organisations (Privileges and Immunities) Amendment Bill 2023 (now Act) in late 2023, it noted that the amendments engaged several human rights, and concluded that:

- (by allowing regulations to be made to grant such immunities in circumstances where there is no clear international law obligation to do so) the bill did not appear to be compatible with the right to an effective remedy;
- the bill would allow the granting of personal immunities (with the potential to limit the right to an effective remedy and the right to access the courts) in situations where there is no basis in international law for doing so; and
- by providing greater flexibility and efficiency to the process of conferring the existing suite of privileges and immunities in the Act, and making those immunities more widely available, the bill increased the risk that privileges and immunities may be granted in circumstances which are incompatible with Australia's obligations under the Convention Against Torture.[18]

---

15 The 2022 regulations declared OCCAR activities to be an 'international conference' for the purposes of s 7 of the *International Organisations (Privileges and Immunities) Act 1963.*

16 International Covenant on Civil and Political Rights, articles 2(3) and 14.

17 Statement of compatibility, p. 8.

18 Parliamentary Joint Committee on Human Rights, International Organisations (Privileges and Immunities) Amendment Bill 2023, *Report 9 of 2023* (6 September 2023) pp. 135–136. See also *Report 8 of 2023* (2 August 2023) pp. 69–77.

Analysis

1.8 The right to equality before courts and tribunals encompasses the right of access to the courts in cases of determination of criminal charges and rights and obligations in a suit at law.[19] The UN Human Rights Committee has stated that:

> The failure of a State party to establish a competent tribunal to determine such rights and obligations or to allow access to such a tribunal in specific cases would amount to a violation of article 14 if such limitations are not based on domestic legislation, are not necessary to pursue legitimate aims such as the proper administration of justice, or are based on exceptions from jurisdiction deriving from international law such, for example, as immunities, or if the access left to an individual would be limited to an extent that would undermine the very essence of the right.[20]

1.9 The right to an effective remedy requires the availability of a remedy which is effective with respect to any violation of rights and freedoms recognised by the International Covenant on Civil and Political Rights.[21] It includes the right to have such a remedy determined by competent judicial, administrative or legislative authorities or by any other competent authority provided for by the legal system of the state. 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.[22]

1.10 The granting of immunities, including immunity from personal arrest or detention and from suit and other legal processes, to international organisations and other categories of officials, would involve an exclusion of the jurisdiction of Australian

---

19 UN Human Rights Committee, *General Comment No. 32, Article 14: Right to equality before courts and tribunals and to a fair trial* (2007) [9].

20 UN Human Rights Committee, *General Comment No. 32, Article 14: Right to equality before courts and tribunals and to a fair trial* (2007) [18]. See also UN Human Rights Committee, *Concluding observations on Zambia*, CCPR/C/79/Add.92 (1996) [10], where the UN committee found that it was incompatible with article 14 for persons to be vested with total immunity from suit.

21 International Covenant on Civil and Political Rights (ICCPR), article 2(3). See, *Kazantzis v Cyprus,* UN Human Rights Committee Communication No. 972/01 (2003) and *Faure v Australia,* UN Human Rights Committee Communication No. 1036/01 (2005), according to which State parties must not only provide remedies for violations of the ICCPR, but must also provide forums in which a person can pursue arguable if unsuccessful claims of violations of the ICCPR. Per *C v Australia* UN Human Rights Committee Communication No. 900/99 (2002), remedies sufficient for the purposes of article 5(2)(b) of the ICCPR must have a binding obligatory effect.

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

courts in criminal, civil and administrative cases. This, in effect, would restrict an individual's access to courts and tribunals, including for the purposes of determining an effective remedy for potential violations of human rights.

1.11 In addition, as a State party to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Australia has an obligation to investigate and prosecute (or extradite) such cases of torture as defined in the Convention if an alleged torturer is found in Australia.[23] This obligation is enlivened even in a case where the alleged torturer may have enjoyed immunity from criminal proceedings in Australia and continues to enjoy immunity in relation to acts carried out in that person's official capacity.[24] Thus, by providing personal immunity to organisations and individuals, including potentially those alleged to have committed torture, the regulation may have implications for Australia's obligation to investigate and prosecute allegations of torture.

---

[23] Convention Against Torture, articles 5–8. The UN Human Rights Committee has stated that: 'States have granted amnesty in respect of acts of torture. Amnesties are generally incompatible with the duty of States to investigate such acts; to guarantee freedom from such acts within their jurisdiction; and to ensure that they do not occur in the future. States may not deprive individuals of the right to an effective remedy, including compensation and such full rehabilitation as may be possible': *General Comment No. 20: Article 7 (Prohibition of torture, or other cruel, inhuman or degrading treatment or punishment)* (1992) [15]. See also *Suleymane Guengueng et al. v Senegal*, UN Committee Against Torture Communication No. 181/2001 (2006), which found the failure by Senegal to prosecute the former head of state of Chad to be a violation of the Torture Convention.

[24] The view that immunity may be limited as a result of the Convention against Torture is supported by jurisprudence, particularly the *Pinochet* case, and the views of the UN Committee against Torture. In the *Pinochet* case the House of Lords considered an extradition request for the surrender of the former President of Chile to face a number of charges of torture. As a former head of state, Pinochet enjoyed immunity for acts undertaken in his capacity as President of Chile. The House of Lords held that, even if the alleged acts of torture had been performed in his capacity as President, the effect of the Convention against Torture was that this immunity was abrogated in relation to alleged acts of torture as defined in that Convention and to which the Convention applied temporally. See *R v Bow Street Metropolitan Stipendiary Magistrate, ex parte Pinochet Ugarte (No 3)* [2000] 1 AC 147. Regarding the UN Human Rights Committee's views, see UN Committee Against Torture, *Consideration of reports submitted by States parties under article 19 of the Convention,* CAT/C/SR.354 (1998) [39]–[40], [46], where the UN Committee stated that article 5, paragraph 2 of the Convention Against Torture 'conferred on States parties universal jurisdiction over torturers present in their territory, whether former heads of State or not, in cases where it was unable or unwilling to extradite them. Whether they decided to prosecute would depend on the evidence available, but they must at least exercise their jurisdiction to consider the possibility'. See also *Conclusions and recommendations on the third periodic report of the United Kingdom of Great Britain and Northern Ireland and Dependent Territories*, CAT/C/SR.360 (1999) [11] and *Report of the Committee against Torture: United Kingdom of Great Britain and Northern Ireland and Dependent Territories*, CAT A/54/44 (1999) para [77(f)].

1.12 Restricting access to courts and tribunals and consequently the availability of a remedy for potential rights violations (other than in relation to torture) may not amount to a violation under international human rights law if such restrictions are based on immunities that are accepted as a matter of international law.[25] The granting of privileges and immunities to international organisations is commonly accepted practice in international law. Australia is bound under several multilateral and bilateral treaties to confer privileges and immunities on various international organisations and their officials, as well as on foreign States and their diplomatic and consular representatives. Australia has an obligation to grant certain immunities to international organisations to which Australia is a member. However, it is not clear that such an obligation exists under international law with respect to organisations (and associated officials) to which Australia is *not* a member. In order for such an obligation to exist, it must be derived from either a treaty commitment or because there is a relevant customary international law rule that applies.

1.13 The extent of the privileges and immunities conferred varies among the different categories of conferee (for example, a diplomatic representative has more extensive accepted immunities than a consular official). Under customary international law Australia is also under additional obligations to afford immunity to certain types of high-level foreign officials, both personal immunity while they are in office and functional immunity after they have left office.[26] In relation to whether granting immunities is compatible with the right to access the courts, this depends on the nature of the immunities granted and whether to do so is necessary and reasonable in all the circumstances.

Australia's OCCAR Convention obligations

1.14 Australia is not a member of OCCAR but has a treaty obligation to grant certain immunities to OCCAR under the Framework Agreement relating to the Organisation

---

25 UN Human Rights Committee, *General Comment No. 32, Article 14: Right to equality before courts and tribunals and to a fair trial* [18]. While the law remains unsettled and continues to evolve at the international level, it has not yet been accepted that there exists a 'human rights exception' to immunity under international law. See, e.g., the rejection of this argument by the House of Lords in *Jones v Ministry of the Interior of the Kingdom of Saudi Arabia and another* [2007] 1 AC 270. For an earlier discussion of this issue, see Parliamentary Joint Committee on Human Rights, *International Organisations (Privileges and Immunities) Amendment Bill 2013,* Fourth Report of 2014 (20 March 2013) pp. 42–47 and Sixth Report of 2013 (15 May 2013) pp. 228–243.

26 *Case Concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v Belgium),* International Court of Justice (ICJ), 14 February 2002 [2002] ICJ Rep 3, especially at [51]-[55].

for Joint Armament Cooperation.[27] These immunities are set out in Annex I to the OCCAR Convention.

1.15 The statement of compatibility states that:

> The privileges and immunities conferred by the Regulations are necessary to facilitate Australia's access to the full benefits of formal participation in OCCAR-managed programmes. The privileges and immunities enable the effective conduct of OCCAR meetings in Australia and ensure the independence of OCCAR representatives and other meeting participants. The privileges and immunities are conferred in the interest of OCCAR and not for the personal benefit of individuals.[28]

1.16 Annex I of the OCCAR Convention requires that OCCAR shall have immunity from jurisdiction subject to certain exceptions.[29] It provides for different immunities and privileges for representatives of Member States, OCCAR staff members, the Director, and experts other than member staff.[30] For example, it provides that:

- representatives of Member States shall, 'while exercising their functions and in the course of their journeys to and from the place of meeting' enjoy specified immunities and privileges, including: immunity from arrest and detention; and immunity from jurisdiction, even after the termination of their mission, in respect of acts, including words spoken and written, done by them in the exercise of their functions (but not in the case of motor traffic offences);[31]
- staff members of OCCAR and experts shall have immunity from jurisdiction in respect of acts done by them in the exercise of their functions (other than in the case of a motor vehicle offence),[32] but are not required to have immunity from arrest and detention; and
- the OCCAR Director shall enjoy the same privileges and immunities as those provided to staff members, and additionally 'shall enjoy the privileges and immunities to which diplomatic agents of comparable rank are entitled' (that is, personal immunity).[33]

---

27 Explanatory statement, p. 1. See, Framework Agreement between the Government of Australia and the Organisation for Joint Armament Cooperation (Organisation Conjointe de Cooperation en matière d'Armement (OCCAR) for the participation of Australia in OCCAR-managed programmes [2022] ATS 3 [33].

28 Statement of compatibility, p. 8.

29 OCCAR Convention (signed at Farnborough on 9 September 1998 and entered into force on 28 January 2001) Annex I, article 3.

30 Articles 13–17.

31 Article 13.

32 Article 15(a) and 16(a).

33 Article 14.

1.17 The OCCAR Convention states that the privileges and immunities are not granted for personal advantage, but are solely to ensure, in all circumstances, the unimpeded functioning of OCCAR and the complete independence of the persons to whom they are accorded.[34] It states that the Director (or the Member State, in the case of a representative) has a duty to waive any relevant immunity wherever retaining it would impede the course of justice and it can be waived without prejudicing the purposes for which it was accorded.[35] These requirements therefore represent the scope of immunities and privileges which Australia is obliged to grant under the OCCAR Framework, and therefore the permissible extent of those immunities and privileges for the purposes of compatibility with international human rights law.

1.18 The privileges and immunities these regulations extend to the Director, staff members, and experts accord broadly with these requirements under the OCCAR Convention. However, the OCCAR Convention establishes a *duty* to waive any relevant immunity where retaining it would impede the course of justice and it can be waived without prejudicing the interests of OCCAR, or the purposes for which it was accorded. Section 17 of the regulation provides that a competent authority 'may' waive the privilege or immunity. This discretion means that privileges and immunities could, as a matter of law, be maintained in circumstances where that would be outside the scope of the OCCAR Convention. As the granting of immunities where there is no clear international law obligation to do so would preclude an individual seeking a remedy against someone who may have violated their rights, this aspect of the regulation may not be compatible with the right to access the courts, and the right to an effective remedy.

1.19 Further, the granting of personal immunity to the OCCAR Director, and immunity from arrest or detention to representatives attending OCCAR conferences, would appear to preclude Australian courts exercising jurisdiction over persons alleged to have committed torture or other serious human rights abuses, even where such persons would not otherwise fall within the general category of individuals covered by personal immunity under general international law (e.g. heads of state).[36] The statement of compatibility states that the instances in which the regulations would limit the right to an effective remedy 'are anticipated to be few given their application to a limited group of individuals'.[37] It states that only those privileges and immunities that are necessary to ensure effective cooperation between OCCAR and Australia are

---

34 Article 13(2) and (20)2).

35 Article 13(2) and 20(2). Article 21 states that OCCAR shall cooperate at all times with the competent authorities of the Member States in order to facilitate the proper administration of justice and to prevent any abuse of the privileges or immunities.

36 Under customary international law, this category of individuals includes heads of state, heads of government, foreign ministers and other high-ranking ministers.

37 Statement of compatibility, p. 9.

conferred, and notes that under the Act these are conferred in the interests of the organisation and not for the personal benefit of individuals.[38] In circumstances where personal immunity has been granted, it would appear that the ability to investigate, prosecute or extradite a person for torture would rely on OCCAR granting a waiver. Leaving this matter to the discretion of OCCAR would not appear to be consistent with Australia's obligations under the Convention Against Torture. As such, there is a risk that privileges and immunities may be granted in circumstances which are incompatible with Australia's obligations under the Convention.

Committee view

1.20 The committee notes that the regulation prescribes the Organisation for Joint Armament Cooperation (OCCAR) as an international organisation under the *International Organisations (Privileges and Immunities) Act 1963* (the Act). The committee notes that, by extending privileges and immunities, including an immunity from personal arrest or detention and from suit and other legal processes to persons associated with OCCAR, the regulation engages and limits the right of access to courts and tribunals, as well as engages the right to an effective remedy and Australia's obligations to investigate and prosecute (or extradite) persons alleged to have committed torture. The committee notes that it recently considered amendments to the Act which relate to this regulation, with respect to these human rights.[39]

1.21 The committee notes that, while Australia is not a member of OCCAR, it has a treaty obligation to grant certain immunities to OCCAR under the *Framework Agreement relating to the Organisation for Joint Armament Cooperation* and, relatedly, the *OCCAR Convention*. The committee notes that while the individual privileges and immunities extended by the regulation broadly accord with those treaty requirements, the Convention provides that, where certain circumstances exist there is a duty to waive an immunity (and thereby facilitate an arrest or other legal process), whereas the regulation only establishes a discretion to waive immunity. The committee considers that privileges and immunities could, as a matter of law, be maintained in circumstances where that would be outside the scope of the OCCAR Convention (Australia's relevant treaty obligation), and therefore in circumstances that may not be compatible with the right to access the courts, and the right to an effective remedy.

1.22 Further, the committee notes that the regulation provides the OCCAR Director with personal immunities and provides immunity from arrest and detention for representatives attending OCCAR conferences. The committee notes that the granting of personal immunity would appear to preclude Australian courts exercising

---

38 Statement of compatibility, p. 9.

39 Parliamentary Joint Committee on Human Rights, International Organisations (Privileges and Immunities) Amendment Bill 2023, *Report 8 of 2023* (2 August 2023) pp. 69–77; and *Report 9 of 2023* (6 September 2023) pp. 122–136.

jurisdiction over persons alleged to have committed torture or other serious human rights abuses, even where such persons would not otherwise fall within the general category of individuals covered by personal immunity under general international law (e.g. heads of state).[40] The committee notes that the ability to investigate, prosecute or extradite a person for torture would rely on OCCAR exercising the discretion to grant a waiver. The committee considers that leaving this matter to the discretion of the organisation would not, as a matter of law, appear to be consistent with Australia's obligations under the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.

Suggested action

1.23 The committee reiterates its previous recommendation that the human rights compatibility of the *International Organisation (Privileges and Immunities) Act 1963* may be assisted were the Act amended to ensure that any immunities do not override Australia's obligations in relation to the prohibition against torture or other cruel, inhuman or degrading treatment or punishment.[41]

1.24 The committee recommends that the statement of compatibility be updated to provide an assessment of the compatibility of the regulation with the right to access the court and Australia's obligations under the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.

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

40 Under customary international law, this category of individuals includes heads of state, heads of government, foreign ministers and other high-ranking ministers.

41 See, Parliamentary Joint Committee on Human Rights, International Organisations (Privileges and Immunities) Amendment Bill 2023, *Report 9 of 2023* (6 September 2023) pp. 122–136.

Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024[42]

Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024

FRL No.	F2024L00711; F2024L00710
Purpose	These instruments establish industry standards for relevant electronic services and designated internet services that require these services to establish and implement systems, processes and technologies to effectively manage risks that Australians will solicit, generate, distribute, access or be exposed to class 1A material or class 1B material through the service
Portfolio	Department of Infrastructure, Transport, Regional Development, Communications and the Arts
Authorising legislation	*Online Safety Act 2021*
Disallowance	15 sitting days after tabling (tabled in the House of Representatives and the Senate on 24 June 2024. Notice of motion to disallow must be given by 22 August 2024 in the House of Representatives or the Senate)[43]
Rights	Freedom of expression; privacy

Regulation of certain online materials

1.26 These legislative instruments establish industry standards for 'relevant electronic services' and 'designated internet services' with respect to certain materials – non-compliance with which attracts a civil penalty of 500 penalty units.[44] A 'relevant electronic service' is defined as an electronic service that enables end-users to communicate with other end-users by way of email, instant messaging, SMS (short message services), MMS (multi-media message services) or chat services (including dating services), as well as an electronic service that enables end-users to play online

---

42 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, *Report 7 of 2024*; [2024] AUPJCHR 49.

43 In the event of any change to the Senate or House's sitting days, the last day for the notice would change accordingly.

44 These instruments are made under section 145 of the *Online Safety Act 2021*, which allows the Commissioner to determine a standard that applies to a particular section of an online industry. See also section 146. 500 penalty units currently equates to a penalty of $165,000.

games with other end-users.[45] A 'designated internet service' is defined as a service that allows end-users to access material using an internet carriage service or a service that delivers material by means of an internet carriage service to persons having equipment appropriate for receiving that material, but does not include: a social media service; a relevant electronic service (as defined above); or an on-demand program service.[46] A designated internet service includes, for example, websites, apps and online storage services that allow end-users to upload, store and manage files, including photos and other media.[47] However, relevant electronic services and designated internet services do not include an 'exempt service', that is, a service where none of the material on the service is accessible or delivered to one or more end-users in Australia.[48]

1.27 The object of the industry standards is to improve online safety for Australians in respect of 'class 1A' and 'class 1B' materials, including by ensuring that service providers establish and implement systems, processes and technologies to manage effectively risks that Australians will solicit, generate, distribute, get access to or be exposed to class 1A or class 1B materials through the services.[49] Class 1A material is defined as child sexual exploitation material; pro-terror material; or 'extreme crime and violence material'.[50] Class 1B material is defined as 'crime and violence material' (but not extreme crime and violence material) or 'drug-related material'.[51] Pro-terror, extreme crime and violence, crime and violence and drug-related materials are all defined by reference to 'class 1 material'.[52] Class 1 materials are materials which are

---

45 *Online Safety Act 2021*, subsection 13A(1). Other relevant electronic services may also be specified in legislative rules.

46 *Online Safety Act 2021*, subsection 14. A 'relevant electronic service' is defined in section 13A of the *Online Safety Act 2021*.

47 Explanatory statement, p. 17.

48 *Online Safety Act 2021*, subsections 13A(2) and 14(3).

49 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 4 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 4.

50 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6.

51 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6.

52 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6.

or would likely be classified as RC (Refused Classification) under the *Classification (Publications, Films and Computer Games) Act 1995*.[53]

1.28 'Pro-terror material' means class 1 material that:

- directly or indirectly counsels, promotes, encourages or urges the doing of a terrorist act or provides instruction in the doing of a terrorist act; or
- directly praises the doing of a terrorist act in circumstances where there is a substantial risk that the praise might have the effect of leading a person (regardless of the person's age or any mental impairment that the person might suffer) to engage in a terrorist act; or
- is 'known pro-terror material', meaning that it has been verified as pro-terror material (such as material produced by terrorist entities that are on the United Nations (UN) Security Council Consolidated List).[54]

1.29 However, pro-terror material does not include material that is accessible using a relevant electronic or designated internet service if its availability on the service can reasonably be taken to be part of public discussion, public debate, entertainment or satire.[55]

1.30 The definitions of 'extreme crime and violence material', 'crime and violence material' and 'drug-related material' in the legislative instruments differ slightly

---

53 Class 1 material is defined in section 106 of the *Online Safety Act 2021* as various types of materials, such as films and computer games, that are or would likely be classified as RC (Refused Classification) under the *Classification (Publications, Films and Computer Games) Act 1995*. 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 provide 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.

54 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6.

55 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6.

depending on the type of material or publication in question, for instance, if the material relates to a computer game, publication or neither type of material.[56]

1.31 Drug-related material means class 1 material that, without justification:

- depicts, expresses or otherwise deals with matters of drug misuse or addiction in such a way that the material offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should be classified RC; or
- is or includes detailed instruction in the unlawful use of drugs; or
- depicts the unlawful use of drugs in connection with incentives or rewards, or interactive, detailed and realistic unlawful use of drugs (in relation to computer game materials); or
- is or includes material promoting the unlawful use of drugs (in relation to material that is neither a computer game nor publication).[57]

1.32 Crime and violence material includes material that, without justification:

- promotes, incites or instructs in matters of crime or violence, or is or includes detailed instruction in, or promotion of, matters of crime or violence; or
- is or includes depictions of bestiality or similar practices; or
- depicts, expresses or otherwise deals with matters of crime, cruelty or violence 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 be classified RC; or
- is or includes depictions of violence that have a very high degree of impact and are excessively frequent, prolonged, detailed or repetitive (in relation to computer game materials); or
- is or includes gratuitous, exploitative or offensive descriptions or depictions of violence that have a very high degree of impact and are excessively frequent, emphasised/prolonged or detailed (in relation to publication materials and materials that are neither a computer game nor publication); or
- is or includes gratuitous, exploitative or offensive descriptions or depictions of cruelty or real violence that have a very high degree of impact and are

---

56 Section 6 of each legislative instrument provides that each category of material has a separate definition for material in relation to a 'computer game', 'publication' and 'material that is not a computer game or publication'.

57 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6.

very detailed (in relation to publication materials and materials that are neither a computer game nor publication);

- is or includes depictions of cruelty or realistic violence that have a very high degree of impact and are very detailed (in relation to computer game materials); or
- is or includes depictions of actual sexual violence (in relation to computer game materials); or
- is or includes depictions of implied sexual violence related to incentives or rewards (in relation to computer game materials); or
- is or includes gratuitous, exploitative or offensive descriptions or depictions of sexual violence (in relation to publication materials and materials that are neither a computer game nor publication).[58]

1.33 Extreme crime and violence material is material that is crime and violence material as defined above where, without justification, the impact of the material is extreme for various reasons, such as because the material is more detailed, realistic or highly interactive.[59]

1.34 Part 3 of the standards impose obligations on service providers in relation to risk assessments and risk profiles. Providers are required to carry out a risk assessment as to the risk that classes 1A and 1B materials will be generated or accessed by, or distributed by or to, end-users in Australia and will be stored on the service.[60] The standards set out the methodology, risk factors and indicators to be used for such risk assessments and risk profile determinations.[61] Certain providers are exempt from the risk assessment requirements, such as a gaming service with limited communications functionality or an 'end-user managed hosting service', which is a service primarily

---

58 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6.

59 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6.

60 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 7 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 7.

61 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 8 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 8.

designed or adapted to enable end-users to store or manage material such as an online file or photo storage service.[62]

1.35 Part 4 of the standards impose various requirements on service providers in relation to online safety compliance measures. The standards include an index that sets out the requirements that apply to each type of service, noting that not all requirements apply to all types of services. [63] In general, the higher the risk that a service could be used to solicit, access or distribute classes 1A and 1B materials (based on the risk assessment and consequent risk profile), the more online safety compliance measures apply. Depending on the type of service, providers may be required to:

- include in the terms of use for the service various provisions, such as requiring the account holder of the service to ensure the service is not used to solicit, access, distribute or store classes 1A or 1B material. Non-compliance with such provisions by an account holder could result in the provider suspending the provision of the service or removing or deleting the relevant material;[64]
- have systems and processes for responding to breaches of the terms of use and taking appropriate action to respond to classes 1A or 1B materials, such as by removing material from the service if the provider becomes aware of it;[65]
- notify law enforcement or an appropriate non-governmental organisation of class 1A material;[66]
- ensure the service has certain safety features and settings;[67]

---

62 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, subsection 7(6) and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, subsection 7(6).

63 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 12 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 12.

64 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 13 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 13.

65 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 14, 15, 23 and 24 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 14–17.

66 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 16 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 18.

67 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 18 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 24.

- implement appropriate systems, processes and technologies to detect, identify and remove certain class 1A material that is stored on the service or being distributed using the service. However, a provider is not required to use systems or technologies to do this if it is 'not technically feasible or reasonably practicable'; or it would require the provider to implement or build a systemic weakness or vulnerability into the service, or implement or build a new decryption capability into the service, or render methods of encryption used in the service less effective. If the provider does not implement any systems or technologies for these reasons, they must still take 'appropriate alternative action';[68]
- implement systems, processes and technologies (if appropriate) to effectively deter and disrupt end-users from using the service to create, offer, solicit, access, distribute, or otherwise make available or store certain class 1A material. For example, providers may use hashing technologies, machine learning and artificial intelligence systems that scan for relevant material and detect key words, behavioural signals and patterns;[69]
- respond promptly and take appropriate and timely action to complaints made to the provider, and refer unresolved complaints to the e-safety Commissioner;[70] and
- provide information and compliance reports to the eSafety Commissioner.[71]

Preliminary international human rights legal advice

Multiple rights

1.36 By requiring providers to implement measures to reduce the risk that their services will be used to solicit, generate, access, distribute and store harmful material,

---

68 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 19 and 20 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 20 and 21. Regarding 'appropriate alternative action', section 11 of both standards sets out the matters to be taken into account when determining whether an action is appropriate, including the extent to which the action would achieve the object of the standards; the nature of the material in question; and whether the action would be proportionate to the level of risk to online safety the material poses.

69 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 21 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 22.

70 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 29 and 31 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 28 and 30

71 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 32–37 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 31–36.

including material depicting child sexual exploitation and sexual violence, the standards are 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 be protected against arbitrary and unlawful interferences with an individual's privacy and attacks on reputation.[72] The statements of compatibility state that the various measures protect children from seriously harmful content and minimise the harms associated with classes 1A and 1B materials.[73] They state that by reducing the ease of dissemination of harmful material, the potential audience for this material is reduced and the risk of further exploitation, violence and abuse is also reduced.[74] They note that the continued circulation of material depicting crimes perpetrated against victim-survivors can re-traumatise victim-survivors.[75]

1.37 The UN Human Rights Council has stated that the human rights which people have offline must also be protected online.[76] International human rights law recognises that women are vulnerable to sexual exploitation, particularly online, and that states have particular obligations with respect to combatting sources of such exploitation.[77] Children also have special rights under human rights law taking into account their particular vulnerabilities,[78] including the right to protection from all forms of violence, maltreatment or sexual exploitation.[79] The international community has recognised the importance of creating a safer online environment for children,[80]

---

72 Convention on the Elimination of All Forms of Discrimination Against Women, article 16; Convention on the Rights of the Child, article 34; International Covenant on Civil and Political Rights, article 17.

73 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, pp. 7–8 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, pp. 8–9.

74 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 8 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 9.

75 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 7 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 8.

76 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).

77 Convention on the Elimination of All Forms of Discrimination Against Women, article 6. See, also, UN 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].

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

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

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

and noted the need to establish regulation frameworks which enable users to report concerns about content.[81]

1.38 Additionally, to the extent that the measures relating to pro-terror material may deter and prevent terrorist-related conduct and violence, they could promote the rights to life and security of the person and the prohibition against inciting national, racial or religious hatred.[82] The statements of compatibility state that pro-terror material is often disseminated online amongst individuals and within groups to spark racial and religious divides amongst Australians and such dissemination can be reasonably viewed as incitement to racial discrimination.[83]

1.39 The right to life imposes an obligation on the state to protect people from being killed by others or identified risks.[84] The UN Human Rights Committee has stated that the duty to protect life requires states to 'enact a protective legal framework that includes effective criminal prohibitions on all manifestations of violence or incitement to violence that are likely to result in the deprivation of life'.[85] The right to security of person requires the state to take steps to protect people against interference with personal integrity by others. This includes protecting people who are subject to death threats, assassination attempts, harassment and intimidation.

1.40 Article 20 of the International Covenant on Civil and Political Rights obliges states to prohibit by law any advocacy of national, racial or religious hatred that

---

81 See, for example, International Telecommunications Union, *Guidelines for policy-makers on Child Protection Online* (2020). See also UN Human Rights Council, *Annual report of the Special Representative of the Secretary-General on Violence against Children*, A/HRC/31/20 (2016) [44] and [51].

82 International Covenant on Civil and Political Rights, articles 6 (right to life), 9 (right to security of person), 20 (prohibition against racial and religious discrimination and hatred) and article 26 (equality and non-discrimination); Convention on the Elimination of All Forms of Racial Discrimination, article 4.

83 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 8 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 9.

84 UN Human Rights Committee, *General Comment No. 36: article 6 (right to life)* (2019) [3]: the right should not be interpreted narrowly and it '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'.

UN Human Rights Committee, *General Comment No. 6: article 6 (right to life)* [5]: the right should not be understood in a restrictive manner. It requires States to adopt positive measures, noting that it would be desirable for State parties to take all possible measures, for example, to reduce infant mortality and increase life expectancy.

85 United Nations Human Rights Committee, *General Comment No. 36: article 6 (right to life)* (2019) [20].

constitutes incitement to discrimination, hostility or violence.[86] Article 26, which protects the right to equality and non-discrimination, also requires the state to prohibit by law any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race or religion.[87] The International Convention on the Elimination of All Forms of Racial Discrimination further describes the content of these obligations and the specific elements that States parties are required to take into account to ensure the elimination of discrimination on the basis of race, colour, descent, national or ethnic origin.[88] In particular, article 4 obliges States parties to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, discrimination, including declaring an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination and acts of violence or incitement to such acts against any groups of a particular race. Article 4 also obliges states to declare propaganda activities that promote and incite racial discrimination, and participation in such activities, to be illegal.

Rights to freedom of expression and privacy

1.41 However, by requiring providers to regulate certain online material – including by restricting access to, disrupting the dissemination of and removing the material – the measures engage and limit 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.[89] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stated that 'the right to freedom of expression includes expression of views and opinions that offend, shock or disturb'.[90] The UN Human Rights Committee has also stated that the right to freedom of expression encompasses expression that may be regarded as deeply offensive and insulting, although such expression may be restricted in

---

86 The UN Human Rights Committee has stated that measures taken in respect of article 20, namely laws prohibiting the advocacy of national, racial or religious hatred, 'constitute important safeguards against infringements of the rights of religious minorities and of other religious groups to exercise the rights guaranteed by articles 18 and 27, and against acts of violence or persecution directed toward those groups'. See UN Human Rights Committee, *General Comment No. 22: Article 18 (Freedom of thought, conscience or religion)* (1993) [9].

87 International Covenant on Civil and Political Rights, articles 2 and 26. Article 2(2) of the International Covenant on Economic, Social and Cultural Rights also prohibits discrimination specifically in relation to the human rights contained in the International Covenant on Economic, Social and Cultural Rights.

88 See articles 1, 2, 4 and 5 of the International Convention on the Elimination of All Forms of Racial Discrimination.

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

90 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/17/27 (2011) [37].

accordance with articles 19(3) and 20 of the International Covenant on Civil and Political Rights (which obliges States parties to prohibit by law any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence).[91]

1.42 The right to freedom of expression carries with it special duties and responsibilities and accordingly may be subject to limitations that are necessary to protect the rights or reputations of others,[92] national security, public order, or public health or morals.[93] Such limitations must be prescribed by law, be rationally connected to the objective of the relevant measures and be proportionate.[94] Noting the important status of this right under international human rights law, restrictions on the right to freedom of expression must be construed strictly and any restrictions must be justified in strict conformity with the limitation clause in article 19(3), including restrictions justified on the basis of article 20.[95]

1.43 By requiring providers to detect and identify certain material and disrupt attempts by end-users to use the service to create, offer, solicit, access, distribute, or otherwise make available, or store certain material, the measures also engage and limit the right to privacy.[96] Additionally, a number of measures require providers to take certain actions, such as report matters to law enforcement or terminate the provision of a service if they become aware that an end-user is breaching the terms of use or using the service to solicit, access, distribute or store certain material. Depending on how the provider becomes aware of such matters, these measures may also limit 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.[97]

---

91 UN Human Rights Committee, *General comment No. 34: Article 19: Freedoms of opinion and expression*, CCPR/C/GC/34 (2011) [11] and [38].

92 Restrictions on this ground must be constructed with care. See UN Human Rights Committee, *General Comment No. 34: Article 19: Freedoms of Opinion and Expression* (2011) [28].

93 The concept of 'morals' derives from myriad social, philosophical and religious traditions. This means that limitations for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition. See UN Human Rights Committee, *General Comment No. 34: Article 19: Freedoms of Opinion and Expression* (2011) [32].

94 UN Human Rights Committee, *General Comment No.34: Article 19: Freedoms of Opinion and Expression* (2011) [21]–[36].

95 UN Human Rights Committee, *General comment No. 34: Article 19: Freedoms of opinion and expression*, CCPR/C/GC/34 (2011) [2]–[3], [21]–[22], [52].

96 Further, if the exercise of powers under these measures did constitute an impermissible limit on a person's right to privacy or right to freedom of expression, it is not clear whether that person would have access to an effective remedy.

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

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

Limitation analysis

1.45 With respect to child sexual exploitation material, material depicting sexual violence and pro-terror material that reaches the threshold of incitement to national, racial or religious hatred, to the extent that regulating these types of material limits the rights to freedom of expression and privacy, such limitations are likely permissible under international human rights law. Indeed, regulating such material would assist Australia to meet its obligations under international human rights law. The rights to freedom of expression and privacy do not protect expression that amounts to propaganda for war or advocacy of national, racial or religious hatred, or online violence and sexual exploitation of women and children.[98] Indeed regarding the latter material, States parties have 'a human rights obligation to ensure both State and non-State agents refrain from engaging in any act of discrimination or violence against women' as well as 'due diligence obligations to prevent, investigate and punish acts of violence against women committed by private companies, such as Internet intermediaries'.[99] The Committee on the Elimination of Discrimination against Women has recommended that states:

> Encourage, through the use of incentives and corporate responsibility models and other mechanisms, the engagement of the private sector, including businesses and transnational corporations, in efforts to eradicate all forms of gender-based violence against women and in enhancing its responsibility for such violence in the scope of its action.[100]

1.46 The Special Rapporteur on violence against women stated that it follows from the above recommendation 'that online and social media should be encouraged to

---

98 Article 20 of the International Covenant on Civil and Political Rights places limits on the rights to freedom of expression and freedom to manifest religion, providing that any expression or manifestation of religion or beliefs must not amount to propaganda for war or advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. See also UN 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) [52] and UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/38/35 (2018) [13].

99 UN 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) [62].

100 Committee on the Elimination of Discrimination against Women, *General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19*, CEDAW/C/GC/35 (2017) [30(f)].

create or strengthen mechanisms focusing on the eradication of gender stereotypes, and to end any gender-based violence committed on their platforms'.[101]

1.47 However, the scope of material that the measures apply to is much broader than just child sexual exploitation material, material depicting sexual violence and pro-terror material that reaches the threshold of advocacy of national, racial or religious hatred. With respect to these other types of material, such as crime and violence or drug-related material that offends against the standards of morality, decency and propriety, it is necessary to undertake an analysis of whether the regulation of such material is reasonable, necessary and proportionate.

1.48 The Special Rapporteur on violence against women has acknowledged that '[l]egislation intended to protect women against online violence but not carefully designed in accordance with the international human rights framework may have adverse collateral effects on other human rights'.[102] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has also raised concerns with respect to states imposing 'obligations on companies to restrict content under vague or complex legal criteria without prior judicial review and with the threat of harsh penalties' as well as '[o]bligations to monitor and rapidly remove user-generated content'.[103] The Special Rapporteur noted that such obligations 'involve risks to freedom of expression'.[104]

Legitimate objective

1.49 The stated objectives of the measures are to respect and protect the rights of victim-survivors, to promote and improve transparency and accountability of online services, and to improve online safety for Australians.[105] The statements of compatibility note that detecting and removing harmful material is necessary to address the harms that can be associated with its production, distribution and consumption.[106] These objectives constitute legitimate objectives for the purposes of

---

101 UN 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) [63].

102 UN 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) [63].

103 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/38/35 (2018) [13].

104 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/38/35 (2018) [17].

105 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 8 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 9.

106 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 7 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 8.

international human rights law and, as outlined above, depending on the material regulated, may assist Australia to fulfil its international obligations.

Rational connection

1.50 Under international human rights law, it must also be demonstrated that any limitation on a right has a rational connection to, or is likely to be effective in achieving, the stated objective. A key question is therefore whether regulating classes 1A and 1B materials (excluding those materials noted above that can be permissibly restricted) is likely to be effective in achieving the stated objectives, particularly improving online safety for Australians and reducing the harms associated with the materials.

1.51 Noting the breadth of materials captured by the measures and the sometimes vague descriptions of such materials (such as materials dealing with drug addiction or crime in such a way that offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should be classified as RC) it is unclear whether the full range of materials regulated by the measures would necessarily cause harm to consenting adult end-users (noting that such material may more likely cause harm to children end-users). The mere fact that material depicts matters that may fall outside of generally accepted community standards does not demonstrate that the viewing of such content by a consenting adult will cause harm to them. As such, some questions arise as to whether and how the measures would be rationally connected to the objective of preventing harm.[107]

1.52 Further, questions arise as to whether providers are capable of effectively implementing the measures such that the measures would be, in practice, rationally connected to the stated objectives. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has cautioned that imposing obligations on companies to monitor, restrict and remove content places 'significant pressure on companies such that they may remove lawful content in a broad effort to avoid liability'.[108] The Special Rapporteur noted that such rules:

> …involve the delegation of regulatory functions to private actors that lack basic tools of accountability. Demands for quick, automatic removals risk new forms of prior restraint that already threaten creative endeavours in the context of copyright. Complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards and whose motives are principally economic.[109]

---

107 The Parliamentary Joint Committee on Human Rights raised similar queries with respect to the regulation of class 1 material by the Online Safety Bill 2021 (now Act). See *Report 5 of 2021* (29 April 2021) pp. 45–83.

108 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/38/35 (2018) [17].

109 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/38/35 (2018) [17].

1.53 If providers interpreted the scope of materials captured by the measures too broadly such that they took action with respect to materials that fell outside the categories of classes 1A and 1B materials, the causal nexus between the materials being regulated and the potential harm caused by viewing such material becomes more tenuous.

Proportionality

1.54 In assessing whether the limitation on the rights to freedom of expression and privacy are proportionate to the objectives being sought, it is necessary to consider whether the limitations are sufficiently circumscribed; whether the measures are accompanied by sufficient safeguards; the potential extent of the interference with rights; and whether any less rights restrictive alternatives could achieve the same stated objectives.

1.55 The breadth of the measures, including the type of material that is to be regulated by providers, is relevant in considering whether the limitations are sufficiently circumscribed. The UN Human Rights Committee has noted that restrictions on the right to freedom of expression must not be overly broad and restrictions should be specific and directly connected to the threat posed by the particular expression.[110] In the case of restrictions on online communication, including restrictions on internet service providers, the UN Human Rights Committee has stated that 'restrictions generally should be content-specific' rather than 'generic bans on the operation of certain sites and systems'.[111] Likewise, with respect to the right to privacy, the UN Human Rights Committee has stated that legislation must specify in detail the precise circumstances in which interferences with privacy may be permitted.[112]

1.56 The types of material captured by the measures in these instruments are classes 1A and 1B materials, which are defined in the standards (as set out above). The

---

110 UN Human Rights Committee, *General Comment No.34: Article 19: Freedoms of Opinion and Expression* (2011) [34]. At [35], the Committee observed: 'When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat'. Regarding the related test of necessity see e.g. *Faurisson v France*, UN Human Rights Committee Communication No. 550/1993 (1996) separate opinions of Mrs Evatt, Mr Kretzmer and Mr Klein, [8]: 'The restriction [on freedom of expression] must be necessary to protect the given value [such as the rights of others]. This requirement of necessity implies an element of proportionality. The scope of the restriction imposed on freedom of expression must be proportional to the value which the restriction serves to protect. It must not exceed that needed to protect the value…the restriction must not put the very right itself in jeopardy'. See also *Ross v Canada*, UN Human Rights Committee Communication No. 736/1997 (2000) [116].

111 UN Human Rights Committee, *General Comment No. 34, Article 19: Freedoms of opinion and expression* (2011) [43].

112 *NK v Netherlands*, UN Human Rights Committee Communication No.2326/2013 (2018) [9.5].

statements of compatibility state that these materials are class 1 materials, meaning that they have been or would likely be classified as RC, which is material that cannot be sold, hired, advertised, or legally imported into Australia.[113] However, even if the material captured by the measures is unlawful under Australian law, it may still be protected under international human rights law. This is particularly so where the definition of the material is drafted in vague and/or broad terms such that the scope of expression restricted by Australian law may be overly broad.

1.57 For example, pro-terror material means material that: directly or indirectly counsels, promotes, encourages or urges the doing of a terrorist act or provides instruction in the doing of a terrorist act; or directly praises the doing of a terrorist act in circumstances where there is a substantial risk that the praise might have the effect of leading a person to engage in a terrorist act.[114]

1.58 This definition of pro-terror material reflects the definition of 'advocates' in the context of the offence of advocating terrorism in the Criminal Code.[115] A 'terrorist act' is defined in the Criminal Code as an action or threat of action that:

- is intended to advocate a political, religious or ideological cause and coerce or influence by intimidation a foreign government or a section of the public; and
- is a certain type of action, including actions that cause serious physical harm to a person or serious damage to property; cause a person's death or endanger their life; create a serious risk to the health or safety of the public; or seriously interfere with, seriously disrupt, or destroy an electronic system (including a telecommunication, financial or transport system).[116]

1.59 The Parliamentary Joint Committee on Human Rights has previously raised concerns regarding the breadth of the offence of advocating terrorism, both when it

---

113 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 5 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 6.

114 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 6.

115 Under section 80.2C of the Criminal Code, a person commits an offence if they advocate the doing of a terrorist act or the commission of a terrorism offence, and they engage in that conduct reckless as to whether another person will engage in a terrorist act or commit a terrorism offence. A person advocates the doing of a terrorist act or the commission of a terrorism offence if they (a) counsel, promote, encourage or urge the doing of a terrorist act or the commission of a terrorism offence; (b) provide instruction on the doing of a terrorist act or the commission of a terrorist offence; or (c) praise the doing of a terrorist act or the commission of a terrorism offence in circumstances where there is a substantial risk that such praise might lead other persons to commit terrorist acts or offences.

116 Criminal Code, subsections 100.1(1) and (2).

was first introduced in 2014 and when it was amended in 2023.[117] In particular, concerns were raised that the offence is overly broad in its application and may result in the criminalisation of speech and expression that does not genuinely advocate the commission of a terrorist act or terrorism offence. In the absence of clear legislative guidance with respect to key terms in the offence, such as 'instruction', 'praises' and 'advocates', as well as the very broad definition of 'terrorist act' itself, there were concerns that the offence was not sufficiently circumscribed and the scope of expression restricted was overly broad.[118] In the absence of sufficient safeguards, the committee considered that the offence did not appear to be compatible with the right to freedom of expression. Given that the definition of pro-terror material directly draws on the offence of advocating terrorism, these concerns remain relevant to these measures. Accordingly, similar questions arise as to whether the measures are sufficiently circumscribed.

1.60 Likewise, the other types of material captured by the measures, including crime and violence, and drug-related materials, are similarly defined in vague and broad terms. Neither the standards nor the explanatory materials provide clarity as to the meaning of key terms within the definitions. While the definitions draw on the language used in the National Classification Code, which sets out the criteria for classifying material as RC, the Code does not include definitions of key terms or concepts. For example, crime and violence material includes material that, without justification, promotes, incites or instructs in matters of crime or violence. However, the meaning of terms such as 'without justification', 'promotes', 'incites', 'instructs' or 'violence' is unclear on the face of the legislation. Crime and violence material also includes material that depicts, expresses or otherwise deals with matters of crime or violence 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 be classified as RC. It is unclear what key terms in this definition mean and the threshold that must be met in order for material to offend against standards of morality, decency and propriety, noting that these concepts are inherently subjective. The explanatory statements refer to the Classification Guidelines (Guidelines for the Classification of Publications 2005; Guidelines for the Classification of Films 2021 and Guidelines for the Classification of Computer Games 2012), which set out the factors that are

---

117 Parliamentary Joint Committee on Human Rights, *Fourteenth Report of the 44th Parliament*, Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 (28 October 2014) pp. 50–52; *Report 9 of 2023*, Counter-Terrorism Legislation Amendment (Prohibited Hate Symbols and Other Measures) Bill 2023 (6 September 2023) pp. 61–121.

118 The UN Human Rights Committee has stated '[s]uch offences as "encouragement of terrorism" and "extremist activity" as well as offences of "praising", "glorifying", or "justifying" terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression. Excessive restrictions on access to information must also be avoided'. See *General Comment No. 34, Article 19: Freedoms of opinion and expression* (2011) [46].

relevant to determining whether material is crime and violence material.[119] These Guidelines provide limited guidance as to the meaning of certain terms. For instance, the Guidelines for the Classification of Publications 2005 defines 'violence' as 'acts of violence' and 'the obvious threat of violence or its result'.

1.61 Further, the explanatory statements note that crime and violence material and drug-related material each have three different definitions depending on the form of material in question. The explanatory statements note that providers should apply the most relevant definition.[120] However without legislative or other guidance as to the meaning of these definitions, it may be difficult in practice for providers to interpret and apply the appropriate definition to the material they are dealing with and do so consistently. In this regard, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has raised concerns about vague content regulation rules, noting that excessively vague terms, such as 'promotes terrorist acts or incites violence' and 'distasteful or offensive content' are 'subjective and unstable bases for content moderation'.[121] The potential complexity in applying the standards, due to the use of vague terms, multiple definitions and the lack of clear guidance, may result in substantial variation in the way the standards are interpreted and applied in practice by providers. Additionally, as observed by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, vague rules may result in providers excessively restricting material so as to avoid liability.[122] The broader the scope of material that may be restricted, the greater the interference with the right to freedom of expression would be.

1.62 The breadth of the obligations imposed on providers and how providers will comply with these obligations in practice are relevant considerations in assessing proportionality, particularly the extent to which the measures would interfere with the right to privacy. Providers are required to implement appropriate systems, processes and technologies to detect, identify and remove known pro-terror material that is stored on the service or is being distributed using the service.[123] 'Known pro-terror material' is material that has been verified as pro-terror material (as defined

---

119 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 143 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 144.

120 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 143 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 144.

121 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/38/35 (2018) [26].

122 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/38/35 (2018) [17].

123 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 19 and 20 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 20 and 21.

above).[124] However, a provider is not required to implement systems, processes and technologies if it is not technically feasible or reasonably practicable to do so; or it would require the provider to implement or build a systemic weakness or vulnerability into the service, or implement or build a new decryption capability into the service, or render methods of encryption used in the service less effective. The explanatory statements state that the term 'technically feasible' maintains its ordinary meaning under the law.[125] It explains that when considering whether a system or technology is reasonably practicable, providers should consider:

- the risk of pro-terror material being stored by, or distributed to, Australian end-users;
- whether the system or technology is proportionate to that risk;
- the costs and practicality of implementation; and
- whether the system or technology is likely to achieve the intended outcome of the standards.[126]

1.63 The explanatory statements note that any burden in addressing an impediment to implementation of systems or technologies must be balanced against the severity of risks and harms to end-users.[127]

1.64 If the provider does not implement any systems or technologies because it is not technically feasible or reasonably practicable, for example, they must still take

---

124 Section 6 of both standards define pro-terror material as class 1 material that directly or indirectly counsels, promotes, encourages or urges the doing of a terrorist act or provides instruction in the doing of a terrorist act; or directly praises the doing of a terrorist act in circumstances where there is a substantial risk that the praise might have the effect of leading a person (regardless of the person's age or any mental impairment that the person might suffer) to engage in a terrorist act; or material that is known pro-terror material. Note 1 accompanying the definition of 'known pro-terror material' states '[k]nown pro-terror material may include material that can be detected via hashes, text signals, searches of key words terms, URLs or behavioural signals or patterns that signal or are associated with online materials produced by terrorist entities that are on the United Nations Security Council Consolidated List'. Note 2 states that material may be verified as a result of a decision of the Classification Board or verified by independent experts, such as non-government organisations Tech Against Terrorism and the Global Internet Forum to Counter Terrorism.

125 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, explanatory statement, p. 153 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, explanatory statement, p. 158.

126 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, explanatory statement, p. 153 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, explanatory statement, p. 158.

127 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, explanatory statement, p. 152 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, explanatory statement, p. 158.

'appropriate alternative action'.[128] The matters that are to be taken into account when determining whether an action is appropriate include the extent to which the action would achieve the object of the standards; the nature of the material in question; and whether the action would be proportionate to the level of risk to online safety the material poses.[129]

1.65 In relation to pro-terror material more broadly (which includes material that has not necessarily been verified as such), providers are required to implement systems, processes and technologies (if appropriate) to effectively deter and disrupt end-users from using the service to create, offer, solicit, access, distribute, or otherwise make available, or store such material.[130]

1.66 As to the extent to which the obligations to detect, identify and remove known pro-terror material, and deter and disrupt pro-terror material will interfere with the right to privacy, the statements of compatibility state that compliance with these obligations will not, given the range of tools available to providers, necessitate interference with privacy.[131] They note that providers can implement effective and privacy preserving systems and processes while also meeting their obligations and achieving the objects of the standards.[132] The statements of compatibility further state that the obligation to identify, detect and remove material does not require providers to do something that is not technically feasible or reasonably practicable, nor does the obligation require a provider to proactively scan texts, emails or messages for content other than material that has been verified as pro-terror material (that is, known pro-terror material).[133] However, to detect known pro-terror material, providers may still need to scan vast amounts of private communications in order to identify and remove such material and, noting the broad definition of known pro-terror material, this is likely to result in a significant interference with privacy. While not requiring providers

---

128 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 19 and 20 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 20 and 21.

129 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 11 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 11.

130 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 21 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 22.

131 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 7 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 8.

132 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 7.

133 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 7.

to take action that is not technically feasible or reasonably practicable could operate as safeguards with respect to the obligation to identify, detect and remove material, the potential value of these safeguards appears likely to decrease over time as technology evolves and circumstances change. The explanatory statements note that providers may use hashing technologies, machine learning and artificial intelligence systems that scan for relevant material and detect key words, behavioural signals and patterns.[134] Noting the continuing advancements in artificial intelligence and machine learning, it appears likely that, at some stage, providers will have access to mechanisms making it technically feasible to scan all communications and material to identify and remove known pro-terror material. The potential interference with privacy may therefore increase over time as advances in technology allow for greater interference.

1.67 The safeguards of not being required to do something that is not technically feasible or reasonably practicable do not, however, apply to the obligation to implement systems, processes and technologies (if appropriate) to disrupt and deter pro-terror material.[135] The matters that are to be taken into account in determining whether it is appropriate to implement technologies include the extent to which doing so would achieve the objective of the standards and whether it would be proportionate to the level of risk to online safety that the material poses. Whether it would be technically feasible or reasonably practicable are not listed as relevant matters.[136] The explanatory statements state that the obligation to disrupt and deter is intended to be broader than the obligation to detect and remove material. This is intended to ensure that service providers who are limited in their ability to identify, detect and remove known material, still implement systems, processes and technologies (if appropriate) that effectively disrupt and deter new and known pro-terror material on their services. However, in practical terms, it is not clear how these two obligations differ. The standards list hashing, machine learning and artificial intelligence that scans and detects material as examples of systems, processes and technologies that providers could use to disrupt and deter pro-terror material.[137] These are the same technologies that providers could use to detect and identify known

---

134 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, explanatory statement, p. 154 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, explanatory statement, p. 160.

135 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 21 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 22.

136 Section 11 of both standards sets out the matters to be taken into account when determining whether an action is appropriate, including the extent to which the action would achieve the object of the standards; the nature of the material in question; and whether the action would be proportionate to the level of risk to online safety the material poses.

137 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, section 21 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, section 22.

pro-terror material. It is also not clear how a provider would disrupt pro-terror material without first identifying it.

1.68 For end-to-end encrypted services, the statements of compatibility emphasise that providers are not required to implement or build new decryption capability into the service or render encryption less effective in order to comply with the obligation to detect and remove known pro-terror material. However, if end-to-end encrypted service providers have existing decryption capability (and so would not need to implement or build new decryption capability), it is not clear whether they would be required to scan encrypted communications to identify and remove known pro-terror material as to do so would arguably render encryption less effective.

1.69 Further, the statements of compatibility note that the standards do not require or expect providers to undertake actions that are inconsistent with their obligations under the *Privacy Act 1988* (Privacy Act), the *Telecommunications Act 1997* or *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.[138] However, it is unclear what specific privacy safeguards would be applicable in the context of these measures. Further, the Parliamentary Joint Committee on Human Rights has stated on a number of occasions that compliance with the Privacy Act is not a complete answer to concerns about interference with the right to privacy for the purposes of international human rights law, noting that the Act contains numerous exceptions to the prohibition on use or disclosure of personal information for a secondary purpose.

1.70 In addition to the above obligations with respect to pro-terror material, providers also have obligations to implement systems and processes to take appropriate action in relation to a breach of the terms of use and respond to classes 1A and 1B materials, including by removing the material and ensuring the material can no longer be accessed or distributed via the service.[139] These obligations apply when the provider becomes aware that there is, or has been, a breach of the terms of use or that the service is being used or has been used to solicit, access, distribute or store classes 1A and 1B materials. Relevant electronic service providers do not need to remove the material if it is not technically feasible or reasonably practicable for the provider to do so.[140] The explanatory statement states that this recognises that some providers, for example telephony relevant electronic services, may have limited or no

---

138 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 7.

139 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 14, 15, 23 and 24 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 14–17.

140 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, sections 15 and 24.

ability to exercise control over materials.[141] It is not clear why this exception to the requirement to remove material does not also apply to designated internet service providers. The extent to which these obligations will interfere with privacy depends on how providers become aware of the breach of the terms of use or the material in question. Reports by end-users of the service appears to be one way in which the provider may become aware of these matters.[142] However, it is not clear whether more intrusive methods may be used by providers to become aware of these matters, such as proactively scanning private communications and materials. If this were to occur, it would constitute a more significant interference with privacy given the breadth of materials captured by these obligations.

1.71 Finally, the statements of compatibility state that the standards adopt an outcomes and risk-based approach so that services with a higher risk profile have more obligations they must meet. They indicate that this ensures that the measures are proportionate to the risk a service presents in respect of classes 1A and 1B materials.[143] The statements of compatibility state that this approach minimises the potential for illegitimate restriction of personal expression.[144] For example, with respect to designated internet services, the statement of compatibility states that:

> Providers of low risk designated internet services, including a general-purpose designated internet service (e.g. review websites, business or informational websites), have minimal obligations under the Standard and will therefore be negligibly affected. The Standard will have a greater impact on designated internet services that are higher risk, as well as individuals generating, accessing or attempting to distribute these harmful forms of material.[145]

1.72 This risk-based approach may assist with proportionality. However, generally services which are considered to be high risk under the standards and are therefore subject to more compliance measures, are those services which contain more personal information. For example, the obligation to identify, detect and remove pro-terror

---

141 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, explanatory statement, p. 149 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024.

142 See e.g. Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, subsection 15(3), which provides that the systems and processes to respond to breaches of the terms of use must include ones which the provider reviews reports by end-users of the service in Australia that class 1A material is accessible using the service.

143 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 4 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 5.

144 Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 6 and Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 7.

145 Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024, statement of compatibility, p. 6.

material, which may involve providers scanning personal communication, applies to 'communication relevant electronic services', which are services that enable a user to communicate with another user, such as online messaging services, some video conferencing services and email services.

1.73 In conclusion, while the measures pursue legitimate objectives, questions arise as to whether regulating the full range of materials captured by the measures is rationally connected to the stated objectives, particularly that of preventing harm. Questions also arise as to whether the measures are sufficiently circumscribed, noting the broad range of materials captured by the measures and the lack of guidance as to how key terms in the standards are to be interpreted and applied by providers. It is also not clear how providers will comply with their obligations in practice without potentially significantly interfering with the right to privacy. While the statements of compatibility identified some safeguards accompanying the measures, it is not clear these are sufficient. Further information is therefore required to assess whether the measures constitute a proportionate limitation on the rights to freedom of expression and privacy.

Committee view

1.74 The committee notes that these legislative instruments establish industry standards for 'relevant electronic services' and 'designated internet services' with respect to classes 1A and 1B materials, which include child sexual exploitation material; pro-terror material; extreme crime and violence material; crime and violence material; and drug-related material. These standards are made under Part 9 of the *Online Safety Act 2021* (Online Safety Act), which relates to the online content scheme. The committee notes that it commented on the human rights compatibility of the Online Safety Act, including Part 9, when it was first introduced, concluding that while Part 9 of the Online Safety Act pursued the important and legitimate objective of enhancing online safety for Australian adults and children, it had not been established that the online content scheme was sufficiently circumscribed such that it constituted a permissible limitation on the right to freedom of expression.[146]

1.75 The committee notes that requiring relevant electronic service and designated internet service providers to implement measures to reduce the risk that their services will be used to solicit, generate, access, distribute and store harmful material, including material depicting child sexual exploitation and sexual violence, and pro-terror material, likely promotes numerous human rights, including the rights of

---

146 Parliamentary Joint Committee on Human Rights, *Report 5 of 2021* (29 April 2021) pp. 45–83. The committee has also previously raised concerns with respect to the compatibility of legislation that restricted and criminalised pro-terror expression with the right to freedom of expression. See Parliamentary Joint Committee on Human Rights, *Fourteenth Report of the 44th Parliament*, Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 (28 October 2014) pp. 50–52; *Report 9 of 2023*, Counter-Terrorism Legislation Amendment (Prohibited Hate Symbols and Other Measures) Bill 2023 (6 September 2023) pp. 61–121.

women and children to be free from sexual exploitation; the rights to life and security of the person; and the prohibition against inciting national, racial or religious hatred.

1.76 However, the committee also notes that the measures necessarily limit the rights to freedom of expression and privacy by regulating certain online material, including restricting access to, disrupting the dissemination of and removing the material. These rights may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate.

1.77 In relation to child sexual exploitation material, material depicting sexual violence and pro-terror material that reaches the threshold of incitement to national, racial or religious hatred, the committee considers that to the extent that regulating these types of material limits the rights to freedom of expression and privacy, such limitations are likely permissible under international human rights law. Indeed, regulating such material would assist Australia to meet its obligations under international human rights law.

1.78 However, noting that the scope of materials captured by the measures is much broader, it is necessary to undertake an analysis of whether the regulation of these other types of material, such as crime and violence or drug-related material that offends against the standards of morality, decency and propriety, is reasonable, necessary and proportionate. In this regard, the committee considers that the measures pursue the legitimate objectives of respecting and protecting the rights of victim-survivors, promoting and improving transparency and accountability of online services and improving online safety for Australians. However, questions arise as to whether the measures are rationally connected and proportionate to these objectives. The committee considers further information is required to assess these matters, and as such seeks the minister's advice in relation to:

(a) what evidence demonstrates that the full range of materials which would fall within classes 1A and 1B (excluding child sexual exploitation material, material depicting sexual violence and pro-terror material that constitutes incitement to national, racial or religious hatred), would be harmful to adult end-users who consent to view such materials;

(b) whether service providers are capable of effectively implementing the measures such that the measures would be, in practice, rationally connected to the stated objectives;

(c) whether there will be guidance provided to service providers to assist in interpreting and applying key terms used in the standards. For example, in the context of crime and violence material, the meaning of ‘promotes’, ‘incites’, ‘instructs’ or ‘violence’ and ‘offends against the standards of morality, decency and propriety generally accepted by reasonable adults’;

(d) why the exception to the requirement to identify, detect and remove known pro-terror material (on the basis that it is not technically feasible or reasonably practicable) does not apply to the obligation to disrupt and deter pro-terror material;

(e) why the exception to the requirement for providers to remove classes 1A and 1B materials if they become aware of such materials (on the basis that it is not technically feasible or reasonably practicable) only applies to relevant electronic services (and not designated internet services);

(f) how a provider would comply with their obligation to disrupt pro-terror material without first identifying it;

(g) what are some examples of appropriate alternative actions that providers may take if they do not implement systems or technologies because it is not technically feasible or reasonably practicable;

(h) if end-to-end encrypted service providers have existing decryption capability (and so would not need to implement or build new decryption capability), whether they would be required to scan encrypted communications to identify and remove known pro-terror material, even if doing so would render the encryption less effective;

(i) what specific safeguards in the *Privacy Act 1988*, *Telecommunications Act 1997* and *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* apply to the standards and how those safeguards would ensure that the limitation on the right to privacy is proportionate in practice;

(j) how a provider would become aware of a breach of the terms of use or the use of their service to access, distribute etc. classes 1A or 1B materials. For example, could a provider proactively scan private communications to monitor compliance with its terms of use;

(k) what other safeguards, if any, accompany the measures to ensure the limitations on the rights to freedom of expression and privacy are proportionate, such as access to review for decisions to remove material; and

(l) if an end-user's rights to freedom of expression or privacy were violated, for example where a provider restricted legitimate forms of expression, what remedy would be available to the end-user.

1.79 The committee notes that the disallowance period for these legislative instruments ends in the House of Representatives and the Senate on 22 August 2024. The committee notes that the disallowance procedure is the primary mechanism by which the Parliament may exercise control over delegated legislation. As the committee has not yet finalised its consideration of these instruments, the committee

has resolved to place a protective notice of motion to disallow the instruments, to extend the disallowance period in the Senate by a further 15 sitting days in order to ensure sufficient time for the committee to consider them.

Tax Agent Services Amendment (Register Information) Regulations 2024[147]

FRL No.	F2024L00856
Purpose	This legislative instrument amends requirements for the publication of information about tax practitioners on the Taxation Practitioner Board register
Portfolio	Treasury
Authorising legislation	*Tax Agent Services Act 2009*
Disallowance	15 sitting days after tabling (tabled in the House of Representatives and in the Senate on 12 August 2024. Notice of motion to disallow must be given by 4 November 2024 in the House and by 19 September 2024 in the Senate)[148]
Rights	Just and favourable conditions of work; privacy; work

Expansion of information on Tax Practitioner Board public register

1.80 This legislative instrument expands the scope of information to be included on the register maintained by the Tax Practitioner Board (the Board). The register is a publicly available database that includes the details of all currently registered, and in some cases formerly registered, tax practitioners (including individuals). People can search the register to identify tax practitioners and can view any conditions or sanctions imposed on the tax practitioners.

1.81 This legislative instrument enables the Board to publish more detailed reasons for tax practitioner sanctions, including terminations, on the register; publish a wider range of information, decisions and outcomes on the register; and removes time limits on how long certain information appears on the register. For example, the register would be required to include:

- past names and registration numbers during the previous 5 years for certain entities on the register for misconduct, and details of registration applications rejected on integrity grounds;

147 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Tax Agent Services Amendment (Register Information) Regulations 2024, *Report 7 of 2024*; [2024] AUPJCHR 50.

148 In the event of any change to the Senate or House's sitting days, the last day for the notice would change accordingly.

- details of Board orders, suspension and termination decisions for misconduct, and details of a Board investigation finding that an entity breached the Act;
- details or updates to Register information for any appeals to the Administrative Appeals Tribunal or a court, including the fact that an application was made and updates for the outcomes (could include removing an unregistered entity's record if they were exonerated); and
- details of applications by the Board to the Federal Court for a civil penalty or injunction, and details of decisions if the court finds a breach of the Act, orders a penalty, grants a non-interim injunction or makes a finding of contempt of court, and details of any appeals of those decisions.

1.82 Further, if the Board considers it 'appropriate' to include additional information about the order or injunction, other decisions or findings the Federal Court makes in the same proceedings, and other decisions or findings made by the Federal Court or another court in related proceedings, then that additional information must be entered on the register.

1.83 The legislative instrument provides for some flexibility in including information on the register. If the Board is satisfied that entering historical information about an entity (such as a previous name) on the register would pose a safety risk to the individual or a member of their family, and having regard to their safety, it would not be appropriate to enter that information on the Register for a certain period, that information is not to be entered.[149]

Preliminary international human rights legal advice

Rights to just and favourable conditions of work; work; privacy

1.84 By requiring the publication of personal information about tax practitioners on a public register, this legislative instrument engages the right to work, the right to just and favourable conditions of work and the right to privacy. The right to work provides that everyone must be able to freely accept or choose their work, and includes a right not to be unfairly deprived of work.[150] The right to just and favourable conditions of work includes the right of all workers to adequate and fair remuneration and safe working conditions.[151]

1.85 The right to privacy includes respect for informational privacy, including the right to respect for private and confidential information, particularly the storing, use

---

149 Section 25B.

150 International Covenant on Economic, Social and Cultural Rights, articles 6–7. See also, UN Committee on Economic, Social and Cultural Rights, *General Comment No. 18: the right to work (article 6)* (2005) [4].

151 See, UN Committee on Economic, Social and Cultural Rights, *General Comment No. 18: the right to work (article 6)* (2005) [2].

and sharing of such information.[152] It also includes the right to control the dissemination of information about one's private life, and protects against arbitrary and unlawful interferences with an individual's privacy and attacks on reputation.[153] These rights may be permissibly limited where the limitation pursues a legitimate objective, is rationally connected to (that is, effective to achieve) that objective and is a proportionate means of achieving that objective.

1.86 The statement of compatibility identifies that the measure engages and limits the rights to work and to privacy.[154] It states that the objective of the measure is to enable clients to make informed choices and promote the integrity of the tax profession and tax system.[155] It also states that compliance with relevant laws is 'a foundation of competence in this field', and that details about these decisions reflects the competence of the person, and would be relevant factors to consider for a promotion. Ensuring the integrity of the tax profession, and that members of the public may make informed choices, would likely be a legitimate objective for the purposes of international human rights law. Including this information on a public register would likely be rationally connected to (that is, effective to achieve) that objective.

1.87 However, a key aspect of whether a limitation on a right can be justified is whether the limitation is proportionate to the objective being sought. This necessitates consideration of: whether a limitation is sufficiently circumscribed; whether it is accompanied by sufficient safeguards; whether any less rights restrictive alternatives could achieve the same stated objective; and the possibility of oversight and the availability of review.

1.88 The statement of compatibility states that existing legislation already requires details of all currently registered tax practitioners to be included on the register, but a loophole enabled individuals to allow their registration to lapse (to avoid having their registration terminated and being listed on the register).[156] It states that this legislative instrument closes that loophole. It states that the scope of published information 'is limited to' current or former members of the profession, and of that cohort, only the subset of those who have breached the relevant legislation as determined by the Board, and of those, only those that the Board decides it is appropriate to include on

---

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

153 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).

154 Statement of compatibility, pp. 26–29.

155 Statement of compatibility, p. 26.

156 Statement of compatibility p. 27.

the register.[157] However, all tax practitioners registered with the Board are included on the register. Further, while only a small number of tax practitioners may have disciplinary and other matters listed as a matter of practice, all members of the profession are subject to the relevant requirements, and so would be liable for that information to be included on the register.

1.89 As to when the Board may consider it appropriate to include information on the register, the statement of compatibility states:

> The [Board] is guided by the object of the [*Tax Agent Services Act 2009*] to ensure tax agent services are provided to the public in accordance with appropriate standards of ethical and professional conduct. This means the [Board] can only make a decision to publish information for the purpose of achieving that outcome and protecting the public, not for any other purpose. Procedural fairness is provided to a tax practitioner who objects to a decision to publish information about the TPB's finding of misconduct, through the right to appeal to the AAT.[158]

1.90 It is not clear whether this discretion would provide any flexibility to not publish information on the register where an individual considered that such publication would unfairly damage their reputation, for example, and whether the person would have the opportunity to make submissions in this regard. There is one basis on which historical information may not be included on the register (for personal physical or safety grounds).[159] The explanatory statement states that this would apply where a person had changed (or proposed to change) their name to reduce a risk to their personal safety.[160] It states that entering information on the register would pose a safety risk to an individual 'if it would create, increase or maintain, or otherwise contribute to, such a risk', and 'if the person who threatens the individual is already aware of the individual's previous and new name or registration number, then publishing that information on the Register would be unlikely to be contributing to a safety risk'.[161] This would appear, therefore, to have very limited safeguard value. Further, it is not clear that an individual could seek the exercise of such a discretion regarding their current registration information if they had such concerns, but had not changed their name.

1.91 In addition, it is unclear why the register would include details about a contempt finding that has been made in relation to an individual,[162] and how including such information would be necessary to achieve the stated objective of the measure. Further, it is unclear why the register includes information from up to five previous

---

157 Statement of compatibility p. 27.

158 Statement of compatibility p. 27.

159 Subsection 25B(5).

160 Explanatory statement, p. 8.

161 Explanatory statement, p. 8.

162 Section 25K.

years, and why a shorter period of time would not be sufficient to achieve the stated objective.

1.92 The explanatory materials note that the register must include information about an application which the Board has made to the Federal Court seeking an order or other action in relation to a practitioner, before any criminal or civil misconduct has been proven. The statement of compatibility acknowledges that '[i]t is possible that Register users will draw inferences from the fact that an application has been made, even though the Federal Court has not yet made any finding or decision'.[163] It states that the delay in finalising a court matter, and the risk to consumers during the intervening period, was weighted as being more significant than the privacy impact on the individual. However, it is not clear that there would be flexibility in individual matters to not include information about such an application in certain cases. In addition, it is not clear that administrative judicial delays in having a matter heard (and determining whether a person is found to have engaged in the relevant conduct as a matter of law) would constitute a sufficient justification for an ongoing interference with the privacy of an individual for the purposes of international human rights law.

Committee view

1.93 The committee notes that requiring the publication of information about tax practitioners on a public register engages and limits the rights to work, just and favourable conditions of work, and privacy.

1.94 The committee considers further information is required to assess the compatibility of this measure with these rights, and as such seeks the minister's advice in relation to:

(a) whether the legislative instrument is compatible with the right to just and favourable conditions of work;

(b) whether there is flexibility to not publish information on the register where an individual submits that publication would unfairly damage their reputation, and whether the person would have the opportunity to make submissions in this regard;

(c) why the discretion to not include information on the register where there would be a risk to a person's safety does not apply in relation to a person's current registration information and whether any other flexibility would apply in relation to them;

(d) why the register would include details about any contempt findings in relation to an individual, and how including such information would be necessary to achieve the stated objective of the measure;

---

163 Statement of compatibility p. 28.

(e) why the register would include information from up to five previous years, and why a shorter period of time would not be sufficient to achieve the stated objective; and

(f) why there is no discretion for the register to not include information about an application made to a court or tribunal (before any criminal or civil conduct has been proven).

Work Health and Safety Amendment (Penalties and Engineered Stone and Crystalline Silica Substances) Regulations 2024[164]

FRL No.	F2024L00766
Purpose	This regulation amends the Work Health and Safety Regulations 2011 to increase monetary penalty levels; prohibit the use of engineered stone benchtops, panels and slabs; and regulate the processing of materials containing crystalline silica.
Portfolio	Employment and Workplace Relations
Authorising legislation	*Work Health and Safety Act 2011*
Disallowance	15 sitting days after tabling (tabled in the House of Representatives on 25 June 2024 and in the Senate on 26 June 2024. Notice of motion to disallow must be given by 9 September 2024 in the House and by 10 September 2024 in the Senate)[165]
Rights	Right to just and favourable conditions of work; health; privacy

Disclosure of worker health monitoring reports

1.95 The regulations amend the Work Health and Safety Regulations 2011 (WHS Regulations) to require an employer to provide health monitoring for all workers carrying out the processing of a crystalline silica substance (CSS) that is high risk in accordance with the health monitoring duties outlined in the WHS Regulations.[166] CSS is found in sand, stone, concrete and mortar and is used to make products including engineered stone (used to fabricate kitchen and bathroom benchtops).

1.96 The WHS Regulations require an employer to: provide for health monitoring by a medical practitioner; obtain a health monitoring report; and give the health monitoring report to the worker, regulator and relevant employers who have a duty to provide health monitoring for the worker.[167]

1.97 The health monitoring report must include the following information in relation to a worker:

---

164 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Work Health and Safety Amendment (Penalties and Engineered Stone and Crystalline Silica Substances) Regulations 2024, *Report 7 of 2024*; [2024] AUPJCHR 51.

165 In the event of any change to the Senate or House's sitting days, the last day for the notice would change accordingly.

166 Subsection 529CE(c).

167 Work Health and Safety Regulations 2011, Part 7.1, Division 6.

- the worker's name and date of birth;
- any test results that indicate whether or not the worker has been exposed to a hazardous chemical, and any advice that test results indicate that the worker may have contracted a disease, injury or illness as a result of carrying out the work that triggered the requirement for health monitoring;
- any recommendation that the employer take remedial measures, including whether the worker can continue to carry out the type of work that triggered the requirement for health monitoring; and
- whether medical counselling is required for the worker in relation to the work that triggered the requirement for health monitoring.

1.98 An employer must also ensure that health monitoring reports in relation to a worker are kept as a confidential record identified as a record in relation to the worker and held for at least 30 years after the record is made.[168]

1.99 The statement of compatibility explains that health monitoring is undertaken to detect the early signs of adverse health effects, help identify control measures that are not working effectively, and assist in protecting workers from the risk of exposure to silica dust.[169] Further, in undertaking risk assessments for any processing of CSS, employers must also have regard to any relevant health monitoring results previously undertaken at the workplace,[170] and previous incidents, illnesses or diseases associated with exposure to respirable crystalline silica at the workplace.[171]

1.100 The regulations also prohibit the use, supply and manufacture of engineered stone in the Commonwealth work health and safety jurisdiction.[172]

Preliminary international human rights legal advice

Right to just and favourable conditions of work, health and privacy

1.101 Insofar as the measure requires the health monitoring of workers carrying out the processing of a CSS that is high risk, and the disclosure of information to the regulator and employers to ensure monitoring, compliance and enforcement activities can be undertaken for the health and safety of workers, this measure would promote the rights to just and favourable conditions of work and the right to health. The right to just and favourable conditions of work includes the right to safe working

168 Work Health and Safety Regulations 2011, section 378.

169 Statement of compatibility, p. 38.

170 Subsection 529CA(2)(f).

171 Subsection 529CA(2)(g).

172 Schedules 2 and 3.

conditions,[173] and the right to health is the right to enjoy the highest attainable standard of physical and mental health.[174]

1.102 However, by requiring the provision of personal health information and permitting the use and disclosure of that personal information, this measure also 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.[175] 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 where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

1.103 As noted above, the statement of compatibility states that health monitoring is necessary to detect the early signs of adverse health effects, help identify control measures that are not working effectively, and assist in protecting workers from the risk of exposure to silica dust.[176] Protecting workers from health risks at work is a legitimate objective for the purposes of international human rights law, and gathering and using health information in the context of regulating exposure to a health risk appears to be rationally connected to (that is, capable of achieving) that objective.

1.104 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. In this case, while generally a health monitoring report and results of a worker cannot be disclosed to another person without the worker's written consent, this does not apply to health monitoring reports given to the regulator and to a relevant employer.[177] It is not clear whether a worker would be informed that their health monitoring report has been shared with the regulator or other relevant employers. It is also unclear whether individual health information needs to be shared with the regulator and employers in order to achieve the stated objective. Further, it appears that a report could include other health information relating to the worker that may be relevant to assessing whether the worker has contracted a disease (for example, comorbidities that are otherwise unrelated to CSS exposure). The statement of compatibility does not explain why such individual health information needs to be provided to the regulator in order to consider control measures in a business, for example, rather than more generalised information that someone at the particular business has contracted silicosis or another

---

173 See, UN Committee on Economic, Social and Cultural Rights, *General Comment No. 18: the right to work (article 6)* (2005) [2].

174 International Covenant on Economic, Social and Cultural Rights, article 12(1).

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

176 Statement of compatibility, p. 38.

177 Work Health and Safety Regulations 2011, subsections 378(2) and (3).

silica-related disease. It is unclear whether reports can be anonymised or redacted before being provided to the regulator and employers or, if not, why it is necessary to provide individual health information in all circumstances. As such, it is not clear whether this constitutes the least rights-restrictive means by which to achieve the objective of the measure.

1.105 As to safeguards, the statement of compatibility explains that once health monitoring reports are received by the regulator and employers, protections apply to the information. Comcare, the regulator, is subject to confidentiality provisions under the *Work Health and Safety Act 2011*,[178] and personal information collected is subject to the *Privacy Act 1988* (Privacy Act).[179] Commonwealth, public authorities and non-Commonwealth licensees (large companies) are also subject to the Privacy Act. While compliance with the Privacy Act and Australian Privacy Principles (APPs) may offer some safeguard value, it is not a complete answer to concerns about interference with the right to privacy for the purposes of international human rights law. The APPs contain a number of exceptions to the prohibition on use or disclosure of personal information for a secondary purpose, including where its use or disclosure is authorised under an Australian law,[180] which may be a broader exception than permitted in international human rights law. There is also a general exemption in the APPs regarding the disclosure of personal information for a secondary purpose where it is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.[181]

1.106 In addition, it appears that there would be circumstances where the Privacy Act does not apply. The statement of compatibility explains that 'there may be scope for contractors to be provided information where the Commonwealth entity and the contractor are both responsible for a worker's health monitoring. Whether the Privacy Act applies would be a question of fact'.[182] Where the Privacy Act does not apply, the explanatory materials do not identify what safeguards would protect the confidential health information of a worker.

Committee view

1.107 The committee notes that the regulation requires health monitoring for all workers carrying out the processing of a crystalline silica substance (a substance used to make products including engineered stone) where that is high risk. The committee

---

178 *Work Health and Safety Act 2011*, section 271 provides for a civil penalty and an offence both with a tier D monetary penalty (currently $14,000 for an individual; $70, 000 for a body corporate).

179 Statement of compatibility, p. 39.

180 APP 9; APP 6.2(b).

181 APP 6.2(e).

182 Statement of compatibility, p. 39.

considers that this is an important measure that promotes the rights to just and favourable work conditions and the right to health.

1.108 However, the committee considers that disclosing health monitoring reports (including a worker's personal health information) to the regulator and employers, engages and limits the right to privacy. The committee notes that the health monitoring framework to which this regulation applies (the Work Health and Safety Regulations 2011) was established prior to the committee's establishment, meaning that the committee has not assessed its human rights compatibility as a whole.

1.109 The committee considers that further information is required to assess the proportionality of the measure with the right to privacy, and as such the committee seeks the minister's advice in relation to:

(a) why the provision of anonymised or redacted health monitoring reports to the regulator and employers would be ineffective to achieve the objective of the measure (having regard to the functions of the entities receiving the information);

(b) whether there is any flexibility for individual employees to request that certain information not be disclosed, or only be subject to limited disclosure; and

(c) in circumstances where the *Privacy Act 1988* does not apply, what safeguards would protect the confidentiality of a worker's health monitoring report.