Chapter 1[1]

New and continuing matters

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

- bills introduced into the Parliament between 7 to 10 December 2020;
- legislative instruments registered on the Federal Register of Legislation between 2 to 23 December 2020;[2] and
- two bills previously deferred.[3]

1.2 Bills and legislative instruments from this period that the committee has determined not to comment on are set out at the end of the chapter, and bills the committee has deferred its consideration of are listed in the Appendix.

1.3 The committee comments on the following bills and legislative instrument, and in some instances, seeks a response or further information from the responsible minister.

1 This section can be cited as Parliamentary Joint Committee on Human Rights, New and continuing matters, *Report 1 of 2021*; [2021] AUPJCHR 2.

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

3 Australian Immunisation Register Amendment (Reporting) Bill 2020 and Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, which were previously deferred in *Report 15 of 2020*.

Bills

Australian Immunisation Register Amendment (Reporting) Bill 2020[4]

Purpose	This bill seeks to amend the *Australian Immunisation Register Act 2015* to: • introduce provisions under which recognised vaccination providers are required to report certain information in relation to certain vaccinations administered, both within and outside Australia; • authorise the collection and use of Commonwealth assigned identifiers, known as a 'provider identification information'; • introduce civil penalties should vaccination providers not comply with the legislated requirements; and • provide power for the secretary of the Department of Health to require a recognised vaccination provider to produce information if they do not comply with this reporting requirement
Portfolio	Health
Introduced	House of Representatives, 3 December 2020
Rights	Health; privacy

Requirement to report vaccination information

1.4 The *Australian Immunisation Register Act 2015* (AIR Act) establishes the Australian Immunisation Register (the Register), which records the vaccinations given to all people enrolled in Medicare in Australia. Currently, the AIR Act does not require vaccination providers to report information relating to vaccinations (it is done on a voluntary basis). This bill seeks to amend the AIR Act to create a requirement for vaccination providers to report information relating to certain relevant vaccinations administered both in and outside Australia to the Register.[5] It would also create a power to require a provider to give specified information if they do not comply with this requirement. The bill does not specify the kind of vaccination this will apply to, and the information that will be reported, leaving such matters to be set out in

4 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Australian Immunisation Register Amendment (Reporting) Bill 2020, *Report 1 of 2021*; [2021] AUPJCHR 3.

5 Schedule 1, item 7, proposed new Division 2A.

delegated legislation. Failure to comply with these reporting requirements would be subject to a civil penalty of up to 30 penalty units for each failure to report.[6]

Preliminary international human rights legal advice

Rights to health and privacy

1.5 In increasing the ability for the government to enhance the monitoring of vaccine preventable diseases, and contributing to enriched monitoring and statistics on health related issues, this measure appears to promote the right to health. The right to health is the right to enjoy the highest attainable standard of physical and mental health.[7] It is a right to have access to adequate health care as well as to live in conditions which promote a healthy life (such as access to safe drinking water, housing, food, and a healthy environment).[8]

1.6 However, in requiring vaccination providers to provide personal information about individuals who receive vaccinations (such as a COVID-19 vaccination),[9] while noting that access to information stored on the Register is strictly controlled and limited, the measure also appears to 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.[10] 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.

1.7 In assessing whether the measure seeks to achieve a legitimate objective, the statement of compatibility states that the bill provides the legislative infrastructure to assist in the objective of protecting the health of individuals and the community by enhanced monitoring of vaccine preventable diseases. This would appear to constitute a legitimate objective for the purposes of international human rights law and the measure appears rationally connected to that objective. In relation to proportionality, the statement of compatibility states that the type of information to be collected under the reporting obligation is the same as that currently collected on a voluntary basis, the amendments do not change the existing provisions in relation to the use and disclosure of information stored on the Register, and individuals have control under

6 Schedule 1, item 7, proposed subsections 10A(5) and 10B(3).

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

8 UN Economic, Social and Cultural Rights Committee, *General Comment No. 14: the right to the Highest Attainable Standard of Health* (2000) [4]. See also, *General Comment No. 12: the right to food (article 11)* (1999); *General Comment No. 15: the right to water (articles 11 and 12)* (2002); and *General Comment No. 22: the right to sexual and reproductive health* (2016).

9 See, explanatory memorandum, p. 1.

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

the AIR Act over how their personal information is used or disclosed.[11] It is noted that the ability of an individual to request that their personal information not be disclosed from the Register could constitute an important safeguard to ensure the consent of a person to the disclosure of their personal information. However, the effect of this as a safeguard in practice would depend on the availability and accessibility of information as to how a person can request their personal information not be disclosed.

1.8 Section 23 of the AIR Act currently provides that it is an offence for a person to record, disclose or use protected information (including personal information) obtained, or derived, under the AIR Act, unless they are authorised to do so. A person is authorised to record, disclose or use protected information if they do so in order to include the information on the Register or to otherwise perform functions under the AIR Act, to disclose the information to a court or coroner, or where authorised to do so under another law.[12] However, the AIR Act includes a broad power for the minister (or their delegate) to authorise a person to use or disclose protected information for a specified purpose where satisfied 'it is in the public interest' to do so.[13] Under international human rights law, when considering whether a limitation on a right is proportionate to achieve the stated objective, it is necessary to consider whether there are sufficient safeguards in place to protect the right to privacy and whether there are other less rights restrictive ways to achieve the stated objective. It is not clear why it is necessary for such a broad discretionary power to enable the disclosure of the personal vaccination information of almost all Australians to any person if it is considered to be in the (undefined) 'public interest'.

1.9 As was set out in the committee's analysis of the bill that subsequently became the AIR Act,[14] the measure, by empowering the minister to disclose protected information to 'a person' rather than 'a specified person or to a class of person', appears to enable disclosure without specifying or limiting the recipients of the information. In addition, it is not clear why specific purposes for disclosure are not set out in legislation, rather than being left to a broad ministerial discretion. The statement of compatibility states that one of the main purposes of the bill is to track and trace the administration of every COVID-19 vaccine administered, to ensure that the Register contains a complete and reliable dataset of vaccines administered in Australia.[15] It goes on to list the purposes for which this information could then be used, including to be able to 'prove vaccination for entry to child care, and school, and

11 Statement of compatibility, p. 4.

12 *Australian Immunisation Register Act 2015*, section 22.

13 *Australian Immunisation Register Act 2015*, subsection 22(3).

14 Parliamentary Joint Committee on Human Rights, *Thirty-Second Report of the 44th Parliament* (1 December 2015) p. 53.

15 Statement of compatibility, p. 3.

for employment purposes'.[16] It is not clear how information regarding an individual's vaccination status would be provided for such purposes. As a matter of statutory interpretation, it appears the measure would enable the minister to make broader authorisations to enable disclosure of personal information on the Register. It is difficult to assess the privacy implications of requiring vaccination providers to report information relating to vaccinations to the Register, without knowing the extent to which such information may be disclosed or the purposes for which it may be used.

1.10 In order to assess the compatibility of this measure with the right to privacy, further information is required as to:

(a) in what circumstances would personal information held on the Register be disclosed to employers, child-care centres and schools;

(b) if it is intended that the minister will specify classes of persons to whom information regarding individuals' COVID-19 vaccination status will be disclosed under the public interest exception (or any other basis), and if so, to whom will it be disclosed; and

(c) whether, in making disclosures of personal information on broad public interest grounds, the decision-maker would be required to consider the impact of such disclosure on the privacy of an affected individual.

Committee view

1.11 The committee notes that this bill would create a requirement for vaccination providers to report information relating to certain relevant vaccinations administered both in and outside Australia to the Australian Immunisation Register. The committee notes this will enable the government to track and trace every COVID-19 vaccine administered, and help to ensure this information can be used to monitor the effectiveness of the vaccines, monitor vaccination coverage across Australia and identify any parts of Australia at risk during the disease outbreak, and inform immunisation policy and research. The committee considers that increasing the ability for the government to enhance the monitoring of vaccine preventable diseases, this measure promotes the right to health.

1.12 The committee also notes that requiring vaccination providers to provide personal information about individuals who receive vaccinations also appears to limit the right to privacy. The committee notes that this right may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate.

1.13 The committee considers that monitoring information about vaccination coverage in order to identify health-related issues constitutes a legitimate objective for the purposes of international human rights law and the measure is rationally

16 Statement of compatibility, p. 3.

connected to that objective. The committee considers further information is required to assess the proportionality of the measure.

1.14 The committee has not yet formed a concluded view in relation to this matter. It considers further information is required to assess the human rights implications of this bill, and accordingly seeks the minister's advice as to the matters set out at paragraph [1.10].

Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill 2020[17]

Purpose	This bill seeks to amend various Acts relating to migration and Australian citizenship to: • provide a framework to protect disclosure of confidential information provided by gazetted law enforcement and intelligence agencies for consideration in visa decisions or citizenship decisions made on character grounds; • enable the minister to disclose confidential information to a court for the purposes of proceedings before the court; • allow the minister to issue a non-disclosure certificate on public interest grounds in relation to information relating to a decision made under the *Australian Citizenship Act 2007* where that decision is reviewable by the Administrative Appeals Tribunal; and • make it an offence for Commonwealth officers to disclose unauthorised confidential information relating to visa and citizenship decisions
Portfolio	Home Affairs
Introduced	House of Representatives, 10 December 2020
Rights	Fair hearing; prohibition against expulsion of aliens without due process

Protected information framework

1.15 The bill seeks to amend the *Migration Act 1958* (Migration Act) and the *Australian Citizenship Act 2007* (Citizenship Act), and make consequential amendments to other laws, for the purposes of introducing a 'protected information framework'. The framework would protect disclosure of confidential information[18] provided by intelligence and law enforcement agencies where the information is used for decisions made to refuse or cancel a visa on character grounds; or revoke or set

17 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill, *Report 1 of 2021*; [2021] AUPJCHR 4.

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

aside such decisions; or decisions made to refuse, cancel, revoke or cease citizenship.[19] The bill would prohibit an officer to whom confidential information is communicated to disclose that information to another person, except in very limited circumstances, or to be required to produce or give the information to a court, tribunal, parliament or parliamentary committee.[20] The bill would make unauthorised disclosure of confidential information an offence, carrying a penalty of 2 years' imprisonment.[21]

1.16 The bill would allow the minister, in specified circumstances, to declare that confidential information be disclosed to a specified minister, Commonwealth officer, court or tribunal.[22] Where information is disclosed in these circumstances, the receiving officer or member of a tribunal must not onwards disclose the information to any other person. In consideration or exercise of this power by the minister, the bill states that the rules of natural justice would not apply.[23]

1.17 Additionally, the bill would allow the High Court, Federal Court of Australia or Federal Circuit Court to order that confidential information be produced to the court if the information was supplied by law enforcement or intelligence agencies and the information is for the purpose of the substantive proceedings.[24] If information is ordered to be produced, any party to proceedings may make submissions concerning how the court should use the information, including any weight to be given to the information and the impact of disclosing the information on the public interest.[25] However, a party can only make submissions or tender evidence with respect to the information if they are lawfully aware of the content of the information.[26] The bill would require the court to order that any party which does not qualify to make submissions relating to the information must be excluded from the hearing of those submissions, including the applicant and their legal representative.[27] After considering the information and any submissions, the court would be required to make a determination as to whether disclosing the information would create a real risk of damage to the public interest and, if so, the court must not disclose the information

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

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

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

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

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

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

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

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

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

to any person, including the applicant and their legal representative.[28] In deciding whether such a risk exists, the court would be required to have regard to the list of matters set out in the bill (and only those matters), which includes the protection and safety of informants; Australia's relations with other countries; Australia's national security; and any other matters specified in regulations.[29] The bill would permit the court to give such weight to the information as it considers appropriate in the circumstances, having regard to any submission made regarding the use of the information.[30]

1.18 Schedule 2 of the bill would also establish a new framework for the management of disclosure of certain sensitive and confidential information to, and by, the Administrative Appeals Tribunal (AAT). The secretary of the Department would be prohibited from giving a document or protected information to the AAT in relation to the AAT's review of a decision if the minister certifies that disclosing the document or information would be contrary to the public interest because it would prejudice the security, defence or international relations of Australia, or involve the disclosure of cabinet deliberations or decisions.[31] Where a document or information has been given to the AAT and the minister has certified that disclosing that information would be contrary to the public interest, or the information was given to the minister in confidence, the AAT may disclose the information, including to the applicant, if it thinks it appropriate to do so having regard to any advice given to it by the secretary. If the information is disclosed, the AAT would be required to give a direction prohibiting or restricting the publication or other disclosure of that information if it is in the public interest to prohibit or restrict disclosure.[32]

Preliminary international human rights legal advice

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

1.19 As regards decisions relating to Australian citizens, the measure appears to engage and limit the right to a fair hearing to the extent that it would restrict such persons from accessing confidential information on which the decision was based and exclude such persons from making submissions relating to the use of that information

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

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

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

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

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

in proceedings.[33] Article 14(1) of the International Covenant on Civil and Political Rights requires that in the determination of a person's rights and obligations in a 'suit at law', everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law.[34] The concept of 'suit at law' encompasses judicial procedures aimed at determining rights and obligations, equivalent notions in the area of administrative law and also extends to other procedures assessed on a case-by-case basis in light of the nature of the right in question.[35] A decision involving the removal of an existing right, such as revocation of citizenship or an existing visa, would create a suit at law for the purposes of article 14.[36]

1.20 In order to constitute a fair hearing, the hearing must be conducted by an independent and impartial court or tribunal, before which all parties are equal, and have a reasonable opportunity to present their case.[37] The UK courts and the European Court of Human Rights have held that the right to a fair hearing is violated where a person is not provided with sufficient information about the allegations against them so that they are able to give effective instructions in relation to those allegations, and

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

34 International Covenant on Civil and Political Rights, article 14

35 UN Human Rights Committee, *General Comment 32: Article 14, Right to Equality before Courts and Tribunals and to Fair Trial* (2007) [16]. At [17], the UN Human Rights Committee has indicated that the guarantees in article 14 do not generally apply to expulsion or deportation proceedings, although the procedural guarantees of article 13 are applicable to such proceedings. See, for example, *PK v Canada*, UN Human Rights Committee Communication No.1234/03 (2007), especially at [7.5] where the Committee rejected the applicability of article 14 to a claim relating to the complainant's right to receive protection in the state party's territory. See also, *Zündel v Canada*, UN Human Rights Committee Communication No.1341/2005, (2007) at [6.7] which held that 'proceedings relating to the determination of whether a person constitutes a threat to national security, and his or her resulting deportation' do not fall within the scope of article 14.

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

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

have an opportunity to challenge the allegations, even in circumstances where full disclosure of information is not possible for reasons of national security.[38] There can be no fair hearing if a case against a person is based solely or to a decisive degree on closed materials or where open material consists only of general assertions.[39] As regards this bill, a person's right to a fair hearing may be limited by the measure insofar as it would restrict the disclosure of information to the person, including information that was used in character-related decision-making, such as criminal allegations against a person, as well as excluding the person from making submissions about the use of the information in proceedings. The measure appears to have the effect of withholding sufficient information from the person to the extent that they are unable to effectively provide instructions in relation to, and challenge, the information, including possible criminal allegations against them.

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

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

1.22 Article 13 incorporates notions of due process also reflected in article 14 of the International Covenant on Civil and Political Rights and should be interpreted in

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

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

light of that right.[40] In particular, the United Nations (UN) Human Rights Committee has stated that article 13 encompasses 'the guarantee of equality of all persons before the courts and tribunals as enshrined in [article 14(1)] and the principles of impartiality, fairness and equality of arms implicit in this guarantee are applicable'.[41] The UN Committee has further stated that article 13 requires that 'an alien…be given full facilities for pursuing [their] remedy against expulsion so that this right will in all circumstances of [their] case be an effective one'.[42]

1.23 The measure limits the due process requirements in article 13 to the extent that it restricts a person's access to information that informed the decision leading to their expulsion or deportation, as well as their ability to make submissions on the use of that information or the weight to be attributed to the information by the court. Such restrictions would appear to have the effect of preventing a person in Australia whose visa is refused or cancelled from effectively contesting or correcting potentially erroneous information, thereby hindering their ability to effectively challenge the decision and pursue a remedy against expulsion.[43]

1.24 The due process guarantees in article 13 may be departed from, but only when 'compelling reasons of national security' so require.[44] It is unclear whether this exception would apply to this measure. The bill seeks to depart from due process requirements where there is a real risk of damage to the 'public interest'. While Australia's national security is a factor to be considered by the court in determining whether disclosing the information would create a real risk of damage to the public interest, it is not the only factor. There are other factors to be considered by the court which are broader than national security reasons, such as Australia's relations with

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

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

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

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

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

other countries and the risk of discouraging informants. Furthermore, the UN Human Rights Committee appears to have interpreted the exception of 'compelling reasons of national security' to be a reasonably high threshold which States parties must meet before departing from their due process obligations.[45] As such, it would appear that article 13 is engaged and limited, yet the statement of compatibility did not identify it as being engaged by the bill, and accordingly no assessment was provided as to whether the limitation was permissible.

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

1.26 As regards the objective being pursued by the bill, the statement of compatibility states that it aims to uphold the good order of the Australian community and protect the public interest by protecting confidential information as well as the methodologies, priorities and capabilities of law enforcement agencies in obtaining that information.[46] It notes that disclosure of confidential information has the potential to expose and jeopardise intelligence and law enforcement capabilities and activities.[47] The statement of compatibility explains that the existing threshold for public interest immunity does not adequately protect the type of confidential information used in character-related decisions, such as a person's criminal background and associations, thereby creating a real risk of onwards disclosure by the

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

46 Statement of compatibility, p. 47.

47 Statement of compatibility, p. 48.

AAT or courts of confidential information and its source to other persons, including non-citizens.[48] Additionally, the statement of compatibility notes that the bill responds to the High Court of Australia decisions of *Graham* and *Te Puia*.[49] The objective of protecting national security and associated law enforcement and intelligence capabilities would likely constitute a legitimate objective for the purposes of international human rights law. Insofar as the measure seeks to establish a framework to prevent the disclosure of confidential information in circumstances where disclosure may damage the public interest, including national security, the measure would appear to be rationally connected to the stated objective.

1.27 In assessing proportionality, it is necessary to consider whether the proposed limitation is sufficiently circumscribed. The matters specified in proposed subsections 52C(5) and 503C(5) that are to be considered by the court in determining whether disclosing the information would create a real risk of damage to the public interest, would appear, in some ways, to be quite broad. Indeed, the statement of compatibility notes that the bill would require the courts to consider the potential damage to the wider concept of public interest, not only national security, in determining whether to order onwards disclosure.[50] The use of the broader concept of public interest rather than the narrower concept of national security would appear to create a lower threshold which must be met in order to prohibit the disclosure of information to any person, including the person to whom the information pertains. Additionally, some matters specified in proposed subsections 52C(5) and 503C(5) are drafted in vague terms, such as 'Australia's relations with other countries' or 'other matters specified in regulations', making it difficult to ascertain the precise circumstances in which rights may be limited. It is also not clear that all of the listed matters are relevant to achieving the stated objective of protecting law enforcement and intelligence capabilities. This raises questions as to whether the measure is sufficiently circumscribed.

1.28 Other relevant factors in assessing the proportionality of the measure include whether it is accompanied by sufficient safeguards; whether it provides sufficient flexibility to treat different cases differently; and whether any less rights restrictive alternatives could achieve the same stated objective. The statement of compatibility states that any limits to human rights are reasonable, necessary and proportionate but does not identify any safeguards which assist with the proportionality of the measure.[51] While the role of the court could operate as a safeguard or oversight mechanism, its role is severely restricted by the practical operation of the measure. The court is only permitted to hear submissions regarding the use of the information

48 Statement of compatibility, pp. 46 and 48.

49 Statement of compatibility, p. 42. See *Graham v Minister for Immigration and Border Protection; Te Puia v Minister for Immigration and Border Protection* [2017] HCA 33.

50 Statement of compatibility, p 48.

51 Statement of compatibility, pp. 47 and 49.

and any weight to be given to the information from parties who are lawfully aware of the content of that information. Given the confidential nature of the information and its source, as well as the intent of the measure to prevent disclosure of the information to other parties, particularly non-citizens, it appears unlikely that any other party except the minister would be aware of the content of the information. In effect, the person to whom the information pertains, and their legal representative, would be excluded from proceedings.

1.29 The jurisprudence of the European Court of Human Rights offers some guidance in considering possible safeguards in the context of domestic laws that restrict disclosure of information to parties for reasons of national security. The European Court of Human Rights has identified special advocates as an important safeguard to 'counterbalance procedural unfairness' through 'questioning the State's witnesses on the need for secrecy and through making submissions to the judge regarding the case for additional disclosure'.[52] The European Court of Human Rights has stated:

> the special advocate could perform an important role in counterbalancing the lack of full disclosure and the lack of a full, open, adversarial hearing by testing the evidence and putting arguments on behalf of the detainee during the closed hearings. However, the special advocate could not perform this function in any useful way unless the detainee was provided with sufficient information about the allegations against him to enable him to give effective instructions to the special advocate.[53]

1.30 It is noted that in other Commonwealth legislation where information is withheld from the affected person on national security grounds, there is a process by which the affected person is provided with a summary of the information and a special advocate is appointed to represent the person's interests in closed hearings.[54]

1.31 Additionally, by prescribing an exhaustive list of matters to which the court must have regard, the court has minimal flexibility to treat individual cases differently and consider matters and information that it considers appropriate and necessary, having regard to the merits of each individual case. The court is prevented from considering procedural fairness and the rights of the affected person in determining whether to disclose the information, notwithstanding that the human rights implications for the affected person may be profound, such as detention and deportation.

---

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

53 *A v United Kingdom*, European Court of Human Rights (Grand Chamber), Application no. 3455/05 (2009) [220].

54 See *National Security Information (Criminal and Civil Proceedings) Act 2004*. Although note the human rights concerns regarding the adequacy of these measures to safeguard the right to a fair hearing, see Parliamentary Joint Committee on Human Rights, *Report 13 of 2020* (13 November 2020) pp. 54–61.

1.32 The proportionality of the measure would likely be assisted if the court was able to undertake some form of balancing exercise, whereby it may weigh the risk of damage to the public interest against the right to a fair hearing or other matters that it considers appropriate and necessary.[55] Without being able to properly test the evidence and to receive submissions from the person to whom the information relates, it would appear very difficult for the court to effectively perform its judicial review task, including determining the appropriate weight to be given to the information in substantive proceedings.[56] The court also has no flexibility to treat individual cases differently as regards disclosure of information. Where it has been determined that disclosure would create a real risk of damage to the public interest, the court is prevented from disclosing even part of the confidential information, such as a summary of the information or a discrete element of the information, even in circumstances where partial disclosure could assist the court without creating a real risk of damage to the public interest. As such, an applicant could be left in the situation of trying to challenge a decision without having any understanding of the reasons for which the decision was made.

1.33 Noting the lack of safeguards to protect the rights of affected persons and the inability of the court to consider procedural fairness in determining whether to disclose the information, it is not apparent that the measure would be the least rights restrictive means of achieving the stated objective. Insofar as information is sought to be protected from disclosure to the public or the affected person for reasons of public interest, the statement of compatibility does not address alternative means that may be available that would protect such information only to the extent required for the public interest, or alternative processes that would still allow such information to be tested in some way before a court. It seems that a less rights restrictive means of achieving the stated objective would be to allow the court to order the disclosure of as much information as possible without compromising the public interest so as to ensure the applicant has the possibility to challenge the information and any allegations against them.

1.34 The availability of review is also relevant in assessing proportionality, as well as being a key component of States parties' procedural fairness obligations under international human rights law. Importantly, as discussed above, the right to review

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

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

under article 13 must be in all the circumstances an *effective* one.[57] The statement of compatibility states that the bill does not amend the relevant procedures and review mechanisms under the Migration Act and Citizenship Act. It states that review of decisions made under these Acts is available, including merits review by the AAT and/or judicial review for decisions made by a delegate, and judicial review of decisions made by the minister.[58] However, while review is theoretically available, the measure would appear to render the practical efficacy of review meaningless in many cases. Without access to all relevant information, notably critical information on which the decision was based, it is unclear on what basis an affected person would be able to effectively challenge the decision. Furthermore, as discussed above, the court's ability to properly perform its judicial review task is severely hampered by the measure. This raises serious concerns that there may not be *effective* access to review.

1.35 In conclusion, the measure seeks to achieve the legitimate objective of protecting national security and associated law enforcement and intelligence capabilities. However, there are concerns as to whether the proposed limitation on the right to a fair hearing and the prohibition against expulsion of aliens without due process is proportionate. The use of the broader concept of public interest as opposed to national security raises questions as to whether the measure is sufficiently circumscribed. The statement of compatibility does not identify any safeguards or address whether there are less rights restrictive means of achieving the stated objective, making it difficult to assess the proportionality of the measure. While review is available, its effectiveness is significantly weakened by the measure insofar as it prevents the applicant's access to potentially all relevant information and places restrictions on the court's ability to consider all matters appropriate and necessary to perform its judicial review task, such as being able to consider procedural fairness obligations or receive submissions from the applicant to test the reliability, relevance and accuracy of the information.

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

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

57 UN Human Rights Committee, *General Comment No. 15: The position of aliens under the Covenant* (1986) [10]. See also, UN Human Rights Council, *Arbitrary deprivation of nationality: report of the Secretary-General*, A/HRC/10/34 (2009) at [31], with respect to decisions relating to nationality, such as cessation or revocation of citizenship, the former UN Secretary-General emphasised States' obligations under international law 'to provide for an opportunity for meaningful review of nationality decisions, including on substantive issues'.

58 Statement of compatibility, pp. 48–49.

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

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

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

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

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

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

Committee view

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

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

1.39 The committee considers that the bill pursues the legitimate objective of upholding law enforcement and intelligence capabilities, and insofar as the measure protects disclosure of confidential information where disclosure may jeopardise law enforcement or intelligence activities, the bill is rationally connected to this

objective. The committee considers further information is required to assess the proportionality of the measure.

1.40 The committee has not yet formed a concluded view in relation to this matter. It considers further information is required to assess the human rights implications of this bill, and accordingly seeks the minister's advice as to the matters set out at paragraph [1.36].

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020[59]

Purpose	This bill seeks to amend the *Surveillance Devices Act 2004* and other Acts to introduce new powers and warrants to enhance the enforcement and intelligence gathering powers of the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC), including: • data disruption warrants to enable the AFP and the ACIC to disrupt data by modifying, adding, copying or deleting data in order to frustrate the commission of serious offences online; • network activity warrants to allow agencies to collect intelligence on serious criminal activity being conducted by criminal networks; and • account takeover warrants to provide the AFP and the ACIC with the ability to take control of a person's online account for the purposes of gathering evidence to further a criminal investigation
Portfolio	Home Affairs
Introduced	House of Representatives, 3 December 2020
Rights	Privacy; effective remedy; life; and torture or cruel, inhuman or degrading treatment or punishment

Enhanced law enforcement and intelligence gathering powers and warrants

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

1.42 Schedule 1 would introduce a data disruption warrant which would allow the AFP and ACIC to access data held in computers to frustrate the commission of relevant offences (being offences generally subject to imprisonment of three years or more).[60] The AFP or ACIC may apply to an eligible judge or nominated Administrative Appeals

59 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, *Report 1 of 2021*; [2021] AUPJCHR 5.

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

Tribunal (AAT) member for a data disruption warrant if they suspect on reasonable grounds that:

- one or more relevant offences have been, are being, are about to be, or are likely to be committed;[61]
- the offences involve or are likely to involve data held in a computer; and
- disruption of that data is likely to substantially assist in frustrating the commission of one or more relevant offences.[62]

1.43 An eligible judge or nominated AAT member may issue a data disruption warrant if satisfied that there are reasonable grounds for the suspicion founding the application for the warrant; and the disruption of data authorised by the warrant is justifiable and proportionate, having regard to the offences.[63] In considering issuing the warrant, the judge or AAT member must have regard to various considerations, including the:

- nature and gravity of the offences;
- likelihood the disruption of data will frustrate the commission of the offences; and
- existence of any alternative means of frustrating the commission of the offences.[64]

1.44 A non-exhaustive list of things that may be authorised by a data disruption warrant are set out in proposed subsection 27KE(2), including entering a premises; using computers, telecommunications facilities, electronic equipment or data storage devices to obtain access to and disrupt data, including adding, copying, deleting or altering data; and intercepting a passing communication.[65] Additionally, the bill would authorise a broad range of things to be done for the purposes of concealing anything done in relation to the data disruption warrant.[66]

1.45 Schedule 2 would introduce a network activity warrant which would authorise the AFP and ACIC to access data held in computers and collect intelligence on criminal

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

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

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

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

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

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

networks operating online. An AFP or ACIC officer may apply to an eligible judge or nominated AAT member for a network activity warrant if they suspect on reasonable grounds that:

- a group of individuals is a criminal network of individuals;[67] and
- access to data held in a computer that is, from time to time, used or likely to be used by any of the individuals in the group, will substantially assist in the collection of intelligence that relates to the group or individuals in the group, and is relevant to the prevention, detection or frustration of one or more relevant offences.[68]

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

- nature and gravity of the alleged offences;
- extent to which access to data will assist in the collection of intelligence;
- likely intelligence value of any information sought to be obtained and whether the things authorised by the warrant are proportionate to that intelligence value; and
- existence of any alternative, or less intrusive, means of obtaining the information sought.[69]

1.47 Similarly to a data disruption warrant, a broad range of things may be authorised by a network activity warrant in relation to the computer that holds the data sought to be obtained, including things to be done for the purposes of concealing anything done in relation to the warrant.[70]

1.48 Schedule 3 would introduce an account takeover warrant which would authorise the AFP or ACIC to take control of a person's online account for the purposes of gathering evidence of criminal activity.[71] A law enforcement officer may apply to a

67 A criminal network of individuals is defined as an electronically linked group of individuals, where one or more of the individuals in the group have engaged, are engaging, or are likely to engage, in conduct that constitutes a relevant offence; or have facilitated, are facilitating, or are likely to facilitate, the engagement, by another person (where or no an individual in the group), in conduct that constitutes a relevant offence. It is immaterial whether the identities of the individuals in the groups or the details of the offences can be ascertained; or there are changes in the composition of the group from time to time: Schedule 2, item 8, proposed section 7A.

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

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

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

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

magistrate for an account takeover warrant if they suspect on reasonable grounds that:

- one or more relevant offences have been, are being, are about to be, or are likely to be, committed; and
- an investigation into those offences is being, will be, or is likely to be, conducted; and
- taking control of one or more online accounts is necessary, in the course of the investigation, to enable evidence to be obtained of the offence.[72]

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

- nature and gravity of the alleged offence;
- any alternative means of obtaining the evidence;
- extent to which the privacy of any person is likely to be affected; and
- likely evidentiary value of the evidence sought.[73]

1.50 Similarly to the other warrants, a broad range of things may be authorised by an account takeover warrant in relation to the target account, including taking exclusive control of the account; accessing, adding, copying, deleting or altering account-based data and account credentials; and the doing of anything reasonably necessary to conceal anything done in relation to the warrant.[74]

Preliminary international human rights legal advice

Multiple rights

1.51 To the extent that the new powers and warrants would facilitate the investigation, disruption and prevention of serious crimes against persons, including protecting children from harm, the measure may promote multiple rights, including the right to life and the rights of the child. The right to life imposes an obligation on the state to protect people from being killed by others or identified risks.[75] The right imposes a duty on States to take positive measures to protect the right to life, including an obligation to take adequate preventative measures in order to protect persons

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

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

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

75 International Covenant on Civil and Political Rights, article 6(1) and Second Optional Protocol to the International Covenant on Civil and Political Rights, article 1. UN Human Rights Committee, *General Comment No. 6: article 36 (right to life)* (2019) [3]: the right 'concerns the entitlement of individuals to be free from acts and omissions that are intended or may be expected to cause their unnatural or premature death, as well as to enjoy a life with dignity'.

from reasonably foreseen threats, such as terrorist attacks or organised crime, as well as an obligation to take appropriate measures to address the general conditions in society that may threaten the right to life, such as high levels of crime and gun violence.[76] Furthermore, States have an obligation to investigate and, where appropriate, prosecute perpetrators of alleged violations of the right to life, even where the threat to life did not materialise.[77] Regarding the rights of the child, children have special rights under human rights law taking into account their particular vulnerabilities.[78] States have an obligation to protect children from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual exploitation and abuse.[79]

1.52 The statement of compatibility states that the bill promotes the right to life by providing the AFP and ACIC with additional tools to manage the risk posed by cyber-enabled serious and organised crime and respond to a heightened online threat environment.[80] It states that the bill is intended to target serious and organised offenders who are using anonymising technologies to engage in online criminal activity, such as terrorism, child exploitation and drugs and firearms trafficking.[81] The second reading speech noted that the threat of online child sexual abuse has recently increased. It stated that the Australian Centre to Counter Child Exploitation has identified a 163 per cent increase in child abuse material downloaded in the three months of April to June 2020 compared to the same period in 2019.[82] If the measure was effective in preventing or disrupting serious crime and facilitating the investigation and prosecution of alleged violations of rights, it may promote multiple rights, including the right to life and the rights of the child.

1.53 However, the measure also engages and limits other rights, notably the right to privacy, by authorising the AFP and ACIC to access and interfere with personal data and information.

76 UN Human Rights Committee, *General Comment No. 6: article 36 (right to life)* (2019) [21], [26]. See also UN Human Rights Committee, *General Comment No. 6: article 6 (right to life)* (1982) [5].

77 UN Human Rights Committee, *General Comment No. 6: article 36 (right to life)* (2019) [27]. The UN Human Rights Committee has stated that investigations in alleged violations of the right to life 'must always be independent, impartial, prompt, thorough, effective, credible and transparent': [28].

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

79 Convention on the Rights of the Child, articles 19, 34, 35 and 36.

80 Statement of compatibility, p. 16.

81 Statement of compatibility, p. 16.

82 Second reading speech, p. 2.

Right to privacy

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

- access, use and modify an individual's personal data, such as altering a person's bank account credentials or monitoring and re-directing a person's funds held in a bank account;
- collect personal information and intelligence about individuals;
- add, copy, delete or alter other data to obtain access to data held in a target computer in order to determine whether the data is covered by a warrant;
- take control of an individual's online account through accessing and modifying data, such as changing a person's password in order to take control of a person's account and assume that person's identity; and
- enter an individual's home or workplace to do a thing specified in the warrant.[83]

1.55 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.[84] It also includes the right to control the dissemination of information about one's private life. Additionally, the right to privacy prohibits arbitrary and unlawful interferences with an individual's privacy, family, correspondence or home.[85] 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.

1.56 The statement of compatibility acknowledges that the bill limits the right to privacy. It states that the objective of the bill is to protect national security, ensure public safety, address online crime, and protect the rights and freedoms of individuals by providing law enforcement agencies with the tools they need to keep the Australian community safe.[86] Such objectives would appear to constitute legitimate objectives

83 See eg explanatory memorandum, pp. 32, 33, 38, 39, 152.

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

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

86 Statement of compatibility, p. 13.

for the purposes of international human rights law, and the measure appears to be rationally connected to this objective.

1.57 The key question is whether the measure is proportionate to achieving the stated objective. Of particular relevance in assessing proportionality is whether the limitation is only as extensive as is strictly necessary to achieve its legitimate objective; whether the measure is accompanied by sufficient safeguards; whether any less rights restrictive alternatives could achieve the same stated objective; and whether there is the possibility of oversight and the availability of review.

1.58 The statement of compatibility details numerous safeguards that exist in the bill to ensure that any interference with the right to privacy is not unlawful or arbitrary, including:

- mandatory considerations to which the issuing authority must have regard before granting a data disruption, network activity or account takeover warrant;
- limited interference with data and property through statutory prohibitions on certain actions;
- protection of information collected under the warrants; and
- measures governing security requirements and record keeping for protected information gathered under the warrants.[87]

1.59 These are important safeguards and likely assist with the proportionality of the measure. However, questions arise as to whether these safeguards are adequate in all circumstances. The strength of the above safeguards, as well as additional safeguards identified in the bill, are assessed in turn below.

Issuing authority

1.60 The bill provides that an application for data disruption and network activity warrants may be made to an eligible judge or a nominated AAT member.[88] An application for an account takeover warrant may be made to a magistrate.[89] Where the relevant issuing authority is a judicial officer, including an eligible judge or magistrate, the right to privacy is more likely to be safeguarded, noting that judicial

87 Statement of compatibility, pp. 13–15.

88 Schedule 1, item 13, proposed new subsection 27KA(2); Schedule 2, item 9, proposed new subsection 27KK(3). The explanatory memorandum states that an eligible judge is a person who is a judge of a court and has consented to be declared as an eligible judge by the Attorney-General. A nominated AAT member is a person who is either the Deputy President, senior member or member of the AAT, and has been nominated by the Attorney-General: Explanatory memorandum, pp. 26–27. See *Surveillance Devices Act 2004*, sections 12–13.

89 Schedule 3, item 4, proposed new subsection 3ZZUN.

authorisation of surveillance methods is considered to be 'best practice'[90] at international law. However, where the issuing authority is an AAT member, questions arise as to whether it is appropriate to entrust supervisory control to a non-judicial officer. As the European Court of Human Rights has stated in relation to interception:

> In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.[91]

1.61 The European Court of Human Rights has further stated that 'control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny'.[92] This approach has also been supported by the United Nations Special Rapporteur on the right to privacy, who included, in the 2018 draft general principles of the right to privacy, that where domestic law provides for the use of surveillance systems, that law shall:

> provide that the individual concerned is likely to have committed a serious crime or is likely to be about to commit a serious crime and in all such cases such domestic law shall establish that an independent authority, having all the attributes of permanent independent judicial standing, and operating from outside the law enforcement agency or security or intelligence agency concerned, shall have the competence to authorise targeted surveillance using specified means for a period of time limited to what may be appropriate to the case.[93]

1.62 Noting that AAT members do not have security of tenure, or generally the same level of expertise as judges, it is not clear that they would necessarily have all the attributes of permanent independent judicial authority. As such, there are concerns that the right to privacy may not be adequately safeguarded by enabling non-judicial officers, with potentially only five years of experience as a legal

90 See *Case of Big Brother Watch and Others v The United Kingdom*, European Court of Human Rights, application nos. 58170/13, 62322/14 and 24960/15, (13 September 2019), [320].

91 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, application no. 47143/06 (4 December 2015) [233]. See also *Klass and Others v Germany*, European Court of Human Rights, application no. 5029/71), (6 September 1978) [55]: 'The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure'.

92 *Szabó and Vissy v Hungary*, European Court of Human Rights, application no. 37138/14 (6 June 2016) [77].

93 United Nations Special Rapporteur on the right to privacy, *Draft Legal Instrument on Government-led Surveillance and Privacy*, Version 0.6 (2018), p. 16.

practitioner, to issue warrants that have the potential to significantly interfere with an individual's privacy.[94]

Mandatory considerations prior to issuing warrants

1.63 The bill provides that in considering whether to grant a warrant, the issuing authority must have regard to specific considerations, including the nature and gravity of the alleged offences; the likely value of the intelligence or evidence to be obtained; the likelihood that the doing of the thing specified in the warrant would be effective in preventing, detecting or frustrating the alleged offence; and the existence of any alternative means of realising the intention of the warrant.[95] With respect to a network activity warrant, the issuing authority must also consider whether the things authorised by the warrant are proportionate to the likely intelligence value of any information obtained, and the extent to which the warrant will result in access to data of persons who are lawfully using the computer. With respect to an account takeover warrant, the issuing authority must also have regard to the extent to which the privacy of any person is likely to be affected.

1.64 The statement of compatibility states that when considering whether the actions authorised by the warrants are justified and proportionate, the issuing authority will consider, for example, the scope of the warrant in terms of who and how many people are affected, the exact nature of the potential intrusion on people's private information, and whether that intrusion is justified by the serious nature of the criminality that is being targeted.[96] The statement of compatibility notes that consideration of alternative means of realising the intention of the warrant is particularly important for ensuring that avenues of investigation, information collection and disruption that are less intrusive on individual privacy are considered. It states that where there are narrower activities that involve a more targeted approach, for example, this should be taken into account by the issuing authority.[97] The explanatory memorandum notes that considering alternative means does not require exhaustion of all other methods of access but rather requires the issuing authority to take into account the circumstances before them and balance the impact on privacy against the benefit to the intelligence operation.[98]

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

95 Schedule 1, item 13, proposed subsection 27KC(2); Schedule 2, item 9, proposed subsection 27KM(2); Schedule 3, item 4, proposed subsection 3ZZUP(2).

96 Statement of compatibility, p. 13.

97 Statement of compatibility, pp. 13–14.

98 Explanatory memorandum, p. 76.

1.65 These mandatory considerations are important safeguards to mitigate the risk of arbitrary interference with the right to privacy. The consideration of alternative means of frustrating an offence with respect to the data disruption warrant and alternative or less intrusive means of obtaining information with respect to the network activity and account takeover warrants, assists with the proportionality of the measure by ensuring that less rights restrictive ways of achieving the objective are considered and pursued where appropriate. However, noting the particular value of an issuing authority explicitly considering the extent to which the privacy of any person is likely to be affected, it is unclear why this mandatory consideration is limited to account takeover warrants only and cannot also apply to data disruption and network activity warrants. Likewise, it is unclear why issuing authorities are not required to consider, with respect to all warrants rather than only network activity warrants, whether the warrant is proportionate having regard to the nature and gravity of the offence and the likely value of information sought to be obtained, as well as the extent of possible interference with the privacy of third parties.

Statutory limits on interference with data and property

1.66 The measure prohibits certain actions under the warrants, except in certain circumstances, in order to limit interference with data and property. All three warrants would prohibit the addition, deletion or alteration of data or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer, unless the action is necessary to do one or more of the things specified in the warrant.[99] The warrants would also prohibit actions that cause any material loss or damage to other persons lawfully using a computer, unless in the case of a data disruption warrant, the loss or damage is justified and proportionate having regard to the offences covered by the warrant.[100] Additional statutory conditions apply to data disruption and account takeover warrants, including that the warrants cannot be executed in a manner that results in loss or damage to data unless justified and proportionate, and cannot cause a person to suffer permanent loss of money, digital currency or property (other than data).[101] However, the bill provides that these statutory conditions do not, by implication, limit the conditions to which the warrants may be subject.[102] The statement of compatibility states that the prohibition of certain actions and the additional statutory

99 Schedule 1, item 13, proposed subsection 27KE(7); Schedule 2, item 9, proposed subsection 27KP(6); Schedule 3, item 4, proposed subsection 3ZZUR(5). See also Statement of compatibility, p. 14.

100 Schedule 1, item 13, proposed subsection 27KE(7); Schedule 2, item 9, proposed subsection 27KP(6); Schedule 3, item 4, proposed subsection 3ZZUR(5).

101 Schedule 1, item 13, proposed subsection 27KE(12); Schedule 3, item 4, proposed subsection 3ZZUR(8).

102 Schedule 1, item 13, proposed subsection 27KE(13); Schedule 3, item 4, proposed subsection 3ZZUR(9).

conditions protect against unlawful and arbitrary interference with privacy and ensure that activities carried out under the warrants are justified and proportionate.[103]

1.67 The statutory limits on interference with data and property would appear to be an important safeguard against arbitrary interference with privacy. With respect to data disruption and account takeover warrants, the additional statutory conditions requiring that loss or damage to data in the execution of the warrants be justified and proportionate would appear to assist with the proportionality of the measure by ensuring that any interference with privacy is only as extensive as is strictly necessary. However, the strength of this safeguard may be weakened by the qualification that the statutory conditions do not limit the conditions to which a warrant may be subject. As a matter of statutory interpretation, it would appear that in specifying things that may be authorised by a data disruption warrant or an account takeover warrant, the issuing authority is not bound by the statutory conditions and may authorise actions that do, perhaps indirectly, result in loss or damage to data or cause a person to suffer a permanent loss of money, digital currency or property. It is unclear to what extent the statutory qualification would lessen the effectiveness of this safeguard in practice.

Restrictions on the use and disclosure of protected information

1.68 The measure contains restrictions regarding the use and disclosure of protected information. With respect to data disruption and account takeover warrants, information gathered under these warrants is deemed protected information and as such, can only be used, recorded, communicated or published in limited circumstances.[104] With respect to network activity warrants, the statement of compatibility states that intelligence gathered under this warrant cannot be used in evidence in a criminal proceeding except in limited circumstances, including further investigations into criminal conduct made under other warrants or to promote the right to a fair trial and facilitate adequate oversight mechanisms.[105] The bill sets out numerous circumstances in which protected information obtained under a network activity warrant can be lawfully used and admitted into evidence, such as disclosure in proceedings in open court, for the purposes of the AFP collecting, correlating, analysing or disseminating criminal intelligence, or the doing of a thing authorised by the warrant.[106]

1.69 The measure also prohibits the unauthorised use or disclosure of protected information with respect to all warrants. The statement of compatibility notes that it is an offence to use, disclose, record, communicate or publish protected information except in limited circumstances, such as where necessary for the investigation of a

103 Statement of compatibility, p. 14.

104 Schedule 1, item 28; Schedule 3, item 4, proposed section 3ZZVH. See also *Surveillance Devices Act 2004,* part 6, division 1.

105 Statement of compatibility, p. 15.

106 Schedule 2, item 19, proposed subsections 45B(3)–(9); Statement of compatibility, p. 15.

relevant offence, a relevant proceeding or the making of a decision as to whether or not to prosecute a person for a relevant offence, or where necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to a property.[107]

1.70 While restricting the use and disclosure of protected information would appear to be an important safeguard, the broad range of exceptions to the statutory protections raises concerns as to whether this safeguard is adequate. For example, the bill would allow protected network activity warrant information to be shared with ASIO or any agency within the meaning of the *Intelligence Services Act 2001* if it relates or appears to relate to any matter within the functions of those organisations or agencies.[108] As drafted, these exceptions would appear to allow protected information obtained under a warrant for a specified purpose to be shared for other broader purposes and potentially purposes that are unrelated to the objectives of this bill. There are questions as to whether some of the exceptions are drafted in broader terms than is strictly necessary.

Storage and destruction of protected information

1.71 The measure requires that protected information obtained under all warrants is kept in a secure location that is not accessible to unauthorised persons and that records or reports are destroyed as soon as practicable if no civil or criminal proceedings have been or are likely to be commenced and the material is unlikely to be required, or within five years after the making of the report or record (which must be reviewed every five years).[109] The statement of compatibility states that requiring the security and destruction of records ensures that private data of individuals subject to a warrant is not handled by those without a legitimate need for access, and is not kept in perpetuity where there is not a legitimate reason for doing so.[110]

1.72 The requirement that protected information be securely stored and destroyed within a specified period of time may operate as a safeguard against arbitrary interference with privacy. In particular, it may ensure that irrelevant data or data that is no longer necessary for a purpose specified under the bill is destroyed and not retained. However, it is unclear whether the specified time period of five years is an

107 Statement of compatibility, p. 14.

108 Schedule 2, item 19, proposed subsection 45B(4); Statement of compatibility, p. 14.

109 Schedule 1, item 38 and *Surveillance Devices Act 2004*, section 46; Schedule 2, item 20, proposed section 46AA; Schedule 3, item 4, proposed section 3ZZVJ; Statement of compatibility, p. 15.

110 Statement of compatibility, p. 15.

appropriate period of time for the purposes of operating as an effective safeguard.[111] In particular, it is not clear why the chief officer is not required to review the continued need for the retention of such records or reports on a more regular basis.

Discontinuance and revocation provisions

1.73 The measure includes discontinuance and revocation provisions that apply in circumstances where the warrant is no longer necessary. The warrants can be issued for no more than 90 days but an extension can be sought more than once if certain conditions are met.[112] If a warrant is no longer required, the necessary steps must be taken to revoke the warrant and ensure that the things authorised under the warrant are discontinued.[113] The measure also places an obligation on law enforcement officers to immediately inform the chief officer of the law enforcement agency when they believe that the warrant is no longer necessary. These provisions would likely serve as an important safeguard against arbitrary interference with privacy and help to ensure that any limitation is only as extensive as is strictly necessary.[114]

Oversight frameworks and access to review

1.74 The statement of compatibility states that the Commonwealth Ombudsman will have oversight functions regarding the use of account takeover and data disruption warrants by the AFP and ACIC. It notes that the Inspector-General of Intelligence and Security (IGIS) will have oversight functions with respect to network activity warrants, including the power to review the activities of the AFP and ACIC in relation to the legality, propriety and human rights implications of the warrant.[115] Regarding the availability of review, the statement of compatibility states that the bill does not provide for merits review and excludes judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act), although notes that courts will retain jurisdiction for judicial review of decisions by a judge or AAT member

111 In *Roman Zakharov v Russia*, the European Court of Human Rights held that the 'six-month storage time-limit set out in Russian law for such data reasonable. At the same time, it deplore[d] the lack of a requirement to destroy immediately any data that are not relevant for the purpose for which they have been obtained…the automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8': *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, application no. 47143/06 (4 December 2015) [254].

112 Schedule 1, item 13, proposed sections 27KD and 27KF; Schedule 2, item 9, proposed sections 27KN and 27KQ; Schedule 3, item 4, proposed section 3ZZUQ.

113 Schedule 1, item 13, proposed sections 27KG and 27KH; Schedule 2, item 9, proposed sections 27KR and 27KS; Schedule 3, item 4, proposed sections 3ZZUT and 3ZZUU.

114 International case law provides that legislation authorising surveillance warrants should set out the circumstances in which it must be cancelled when no longer necessary, and that without this, the law will not contain sufficient guarantees against arbitrary interference with the right to privacy: *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, application no. 47143/06 (4 December 2015) [250]-[252].

115 Statement of compatibility, p. 17.

to issue a warrant under the *Judiciary Act 1903*. The statement of compatibility states that this approach is consistent with similar decisions made for national security and law enforcement purposes, noting that such decisions are unsuitable for merits review.[116]

1.75 While the measure provides the possibility of oversight by the Commonwealth Ombudsman and IGIS, there is limited access to review. Additionally, there are concerns regarding the likely effectiveness of any review mechanisms given the covert nature and purpose of the measure. Persons whose privacy would be interfered with are invariably excluded from participating in any review proceedings or indeed, the proceedings dealing with the initial warrant application. In these circumstances, it is unclear why additional safeguards, such as public interest monitors,[117] are not available. As the person whose data or information is sought to be obtained is not able to be personally represented at the application for the warrant, having an independent expert to appear at the hearing to test the content and sufficiency of the information relied on, to question any person giving information, and to make submissions as to the appropriateness of granting the application, is an important safeguard to protect the rights of the affected person. As the European Court of Human Rights has held:

> the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his rights.[118]

1.76 The statement of compatibility does not include information regarding the possibility of public interest monitors or similar safeguards. Noting the inclusion of a role for public interest monitors in similar legislation,[119] it is not clear why this measure does not include public interest monitors as a safeguard to ensure the interests of the affected person are protected in any warrant application or review proceedings.

Further information sought

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

(a) why the power to issue a data disruption warrant and network activity warrant is conferred on a member of the AAT, of any level and with a

116 Statement of compatibility, p. 17.

117 Such as the Victorian or Queensland Public Interest Monitor.

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

119 See *Telecommunications (Interception and Access) Act 1979* in relation to Public Interest Monitors (for example, see section 44A, 45, 46 and 46A).

minimum of five years' experience as an enrolled legal practitioner, and whether this is consistent with the international human rights law requirement that judicial authorities issue surveillance warrants;

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

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

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

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

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

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

Right to an effective remedy

1.78 If warrants were to be issued inappropriately, or unauthorised actions carried out under the warrant, a person's right to privacy may be violated. The right to an effective remedy requires access to an effective remedy for violations of human rights.[120] 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),

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

states parties must comply with the fundamental obligation to provide a remedy that is effective.[121]

1.79 The statement of compatibility identifies that the right to an effective remedy is engaged by the measure. It states that the bill does not provide merits review and excludes judicial review under the ADJR Act, although notes that judicial review is still available for decisions by a judge or AAT member to issue a warrant.[122] This would provide an avenue to challenge unlawful decisions where there has been a jurisdictional error. The statement of compatibility also notes the oversight functions of the Commonwealth Ombudsman and IGIS. It states that, with respect to network activity warrants, the IGIS would be able to review AFP and ACIC activities to ensure they are legal, proper, and consistent with human rights.

1.80 While the oversight functions of the Commonwealth Ombudsman and IGIS may serve as a useful safeguard to help ensure decision-makers are complying with the legislation, this would not appear to provide any remedy to individuals. Further, given that the warrants are designed to be sought covertly and noting the broad concealment powers, it is also unclear how an applicant could practically seek judicial review of a decision of which they are unaware. United Nations bodies and the European Court of Human Rights have provided specific guidance as to what constitutes an effective remedy where personal information is being collected in the context of covert surveillance activities. The United Nations High Commissioner for Human Rights has explained that in the context of violations of privacy through digital surveillance, effective remedies may take a variety of judicial, legislative or administrative forms, but those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated.[123] The European Court of Human Rights has also stated that if an individual is not subsequently notified of surveillance measures which have been used against them, there is 'little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his knowledge and thus able to challenge their legality retrospectively'.[124] The court acknowledged that, in some instances, notification may not be feasible where it would jeopardise long-term surveillance activities.[125] However, it explained that:

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

122 Statement of compatibility, p. 17.

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

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

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

> [a]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned.[126]

1.81 It is not clear that a person whose privacy might have been interfered with through, for example, their online account being taken over or their personal data being accessed, used, copied, modified or deleted, would ever be made aware of that fact (if it does not lead to a prosecution). It is therefore unclear how such a person could have access to an effective remedy for any potential violation of their right to privacy.

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

(a) whether a person who was the subject of a warrant will be made aware of that after the investigation has been completed; and

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

Committee view

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

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

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

1.86 The committee considers that the measure, in seeking to protect national security and ensure public safety, pursues a legitimate objective and these new law enforcement and intelligence gathering powers and warrants would appear to be

126 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, (Application no. 47143/06) 2015 [287]. See also *Klass and Others*, [58].

rationally connected to that objective. The committee considers further information is required to assess the proportionality of the measure and determine whether the measure limits the right to an effective remedy.

1.87 The committee has not yet formed a concluded view in relation to these matters. It considers further information is required to assess the human rights implications of this bill, and accordingly seeks the minister's advice as to the matters set out at paragraphs [1.77] and [1.82].

Assistance orders

1.88 The bill would allow the AFP or ACIC to apply to an eligible judge, nominated AAT member or magistrate for an assistance order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to do a specified thing with respect to data disruption, network activity or account takeover warrants.[127] A specified person includes a person reasonably suspected of having committed the alleged offence as well as third parties who may have relevant knowledge, such as an employee of the owner of the computer that holds data sought to be obtained.[128] A person would commit an offence if they are subject to an assistance order, are capable of complying with a requirement in the order and they fail to comply with the requirement of the order.[129] The maximum penalty for contravention of an assistance order is 10 years imprisonment.

Preliminary international human rights legal advice

Right to privacy

1.89 To the extent that the measure may compel a person to provide personal information to the AFP or ACIC, such as a password to access their computer or other personal device, or information enabling the decryption of personal data, the measure engages and limits the right to privacy. The right to privacy includes respect for informational privacy, including the right to respect for private and confidential information, particularly the storing, use and sharing of such information.[130] It also includes the right to control the dissemination of information about one's private life. The right to privacy may be subject to permissible limitations which are provided by law and are not arbitrary. In order for limitations not to be arbitrary, the measure must pursue a legitimate objective, and be rationally connected to (that is, effective to achieve) and proportionate to achieving that objective. The statement of compatibility

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

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

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

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

does not identify that the right to privacy is engaged and limited by this measure, and as such does not provide an assessment as to the compatibility of assistance orders with the right to privacy.

1.90 The statement of compatibility states that the overall objective of the bill is to enhance the enforcement powers of the AFP and ACIC in order to combat cyber-enabled serious and organised crime.[131] Regarding this measure specifically, the explanatory memorandum states that assistance orders would ensure that should a warrant be issued under this bill, the AFP or ACIC would have the power to compel a person to assist in accessing devices, accessing and disrupting data, copying data, converting documents and accessing and taking control of an online account.[132] It states that the purpose of this measure is to compel assistance from a person with the relevant knowledge, rather than assistance from industry. Assistance orders could be used to compel suspects to provide access to computers or devices to assist law enforcement officers to do a specified thing, such as disrupt data held in their personal computer.[133] The explanatory memorandum notes, however, that the measure would not abrogate the common law right to freedom from self-incrimination. It states that assistance orders do not engage this right because they do not compel individuals to provide evidence against their legal interest.[134]

1.91 The objective pursued by this measure would appear to be combatting serious online crime, which would be a legitimate objective for the purposes of international human rights law. By facilitating the investigation and disruption of crime, the measure would appear to be rationally connected to this objective. However, there are questions as to whether the measure is proportionate to this objective, particularly, whether the measure is accompanied by sufficient safeguards.

1.92 In considering whether to grant an assistance order, the issuing authority must be satisfied of specified criteria. The applicable criteria differ in relation to each warrant. In considering whether to grant an assistance order with respect to a data disruption warrant, the issuing authority must be satisfied that disruption of data held in the computer is likely to substantially assist in frustrating the commission of the offence and is justifiable and proportionate, having regard to the offence.[135] In considering whether to grant an assistance order with respect to a network activity warrant, the issuing authority must be satisfied that access to data held in the computer will substantially assist in the collection of intelligence that relates to the group and is relevant to the prevention, detection or frustration of a relevant

131 Statement of compatibility, p. 9.

132 Explanatory memorandum, pp. 54 and 95.

133 Explanatory memorandum, p. 56.

134 Explanatory memorandum, pp. 56, 164.

135 Schedule 1, item 47, proposed subsection 64B(2).

offence.[136] In considering whether to grant an assistance order with respect to an account takeover warrant, the issuing authority must be satisfied that taking control of the account is necessary, in the course of the investigation, for the purpose of enabling evidence to be obtained relating to the alleged offence to which the warrant is issued.[137]

1.93 The criteria to grant an assistance order would appear to operate as some form of a safeguard against arbitrary interference with privacy. In particular, in relation to a data disruption warrant, the criterion that disruption of data held in the computer is justifiable and proportionate, having regard to the offences, would appear to assist with the proportionality of the measure by ensuring that any interference with privacy is only as extensive as is strictly necessary. However, it is unclear why the issuing authority is not required to be satisfied of this criterion with respect to assistance orders relating to all warrants.

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

(a) why the issuing authority is not required to be satisfied that an assistance order is justifiable and proportionate, having regard to the offences to which it would relate, with respect to all warrants, noting that this criterion only applies to an assistance order with respect to data disruption warrants; and

(b) whether the measure is accompanied by any other safeguards that would ensure that any interference with the right to privacy is not arbitrary and only as extensive as is strictly necessary.

Committee view

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

1.96 The committee notes that this measure would appear to engage and limit the right to privacy insofar as it may compel a person to provide personal information to the AFP or ACIC. The committee notes that the right to privacy may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate. The committee notes that the statement of compatibility did not identify this right as being limited and therefore did not provide an assessment as to the compatibility of the measure. The committee considers that the measure

136 Schedule 2, item 31, proposed subsection 64(6A).

137 Schedule 3, item 4, proposed subsection 3ZZVG(2).

pursues the legitimate objective of combatting serious online crime, and as the assistance order would facilitate the investigation and disruption of crime, the measure is rationally connected to this objective. The committee considers further information is required to assess the proportionality of the measure.

1.97 The committee has not yet formed a concluded view in relation to this matter. It considers further information is required to assess the human rights implications of this bill, and accordingly seeks the minister's advice as to the matters set out at paragraph [1.94].

Information sharing with foreign governments

1.98 The bill would allow protected information obtained under the warrants to be disclosed to foreign countries in certain circumstances. For example, protected information obtained under an account takeover warrant and a network activity warrant (other than through the use of a surveillance device), may be used or disclosed in connection with the functions of the AFP under section 8 of the *Australian Federal Police Act 1979.*[138] The AFP's functions include providing police services to assist or cooperate with a foreign law enforcement or intelligence or security agency.[139]

Preliminary international human rights legal advice

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

1.99 By authorising the sharing of protected information to foreign governments the measure engages and limits the right to privacy. The right to privacy includes respect for informational privacy, including the right to respect for private and confidential information, particularly the storing, use and sharing of such information.[140] It also includes the right to control the dissemination of information about one's private life.

1.100 To the extent that the measure authorises protected information to be shared with foreign police, intelligence or security agencies and results in the investigation and prosecution of an offence that is punishable by the death penalty in that foreign country, the measure may also engage and limit the right to life.[141] The right to life imposes an obligation on Australia to protect people from being killed by others or from identified risks. While the International Covenant on Civil and Political Rights

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

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

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

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

does not completely prohibit the imposition of the death penalty, international law prohibits states which have abolished the death penalty (such as Australia) from exposing a person to the death penalty in another state.[142] The provision of information to other countries that may be used to investigate and convict someone of an offence to which the death penalty applies is also prohibited.[143] In 2009, the UN Human Rights Committee stated its concern that Australia lacks 'a comprehensive prohibition on the providing of international police assistance for the investigation of crimes that may lead to the imposition of the death penalty in another state', and concluded that Australia should take steps to ensure it 'does not provide assistance in the investigation of crimes that may result in the imposition of the death penalty in another State'.[144]

1.101 The statement of compatibility states that protected information can be shared with a foreign country, the International Criminal Court or a War Crimes Tribunal if relevant to an international assistance authorisation.[145] It also notes that similar allowances are made for protected information to be shared under the *Mutual Assistance in Criminal Matters Act 1987* (Mutual Assistance Act) and the *International Criminal Court Act 2002.*[146] The Mutual Assistance Act provides that a request by a foreign country for assistance under the Act must be refused if the offence is one in respect of which the death penalty may be imposed.[147] However, the Act qualifies this by stating that this prohibition will not apply if 'the Attorney-General is of the opinion, having regard to the special circumstances of the case, that the assistance requested should be granted'.[148] Consequently, it appears that the Mutual Assistance Act creates a risk of facilitating the exposure of individuals to the death penalty.[149]

1.102 Additionally, the sharing of protected information, including personal information, with foreign countries, may, in some circumstances, expose individuals to a risk of torture or other cruel, inhuman or degrading treatment or punishment. International law absolutely prohibits torture and cruel, inhuman or degrading

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

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

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

145 Statement of compatibility, p. 14.

146 Statement of compatibility p. 14.

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

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

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

treatment or punishment.[150] There are no circumstances in which it will be permissible to subject this right to any limitations.

1.103 The statement of compatibility acknowledges that the measure engages and limits the right to privacy. However, it does not identify that the right to life or the prohibition against torture or cruel, inhuman or degrading treatment or punishment may be engaged. As such, there is no compatibility assessment provided with respect to either of these rights.

1.104 The rights to privacy and life 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.

1.105 Regarding the objective pursued, the broader purpose of the bill is to protect national security, ensure public safety, and to address online crime.[151] While this objective may be capable of constituting a legitimate objective for the purposes of international human rights law, the statement of compatibility provides no information about the importance of this objective in the specific context of the measure. In order to demonstrate that the measure pursues a legitimate objective for the purposes of international human rights law and has a rational connection to that objective, further information is required as to the specific objective being pursued by the measure, including the substantial and pressing concern that is being addressed. Further, as the statement of compatibility does not address the right to life or the prohibition against torture or cruel, inhuman or degrading treatment or punishment, it is not clear what safeguards, if any, exist to ensure that protected information is not shared with a foreign country in circumstances that could expose a person to the death penalty or lead to a person being tortured, or subjected to cruel, inhuman or degrading treatment or punishment.

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

(a) what is the objective being pursued by the measure and how is the measure rationally connected to that objective;

(b) what safeguards are in place to ensure that protected information obtained under the warrants is not shared with a foreign country in circumstances that could expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment. In particular, why is there no legislative requirement that where there are substantial grounds for believing there is a real risk that disclosure of information to a foreign government may expose a person to the death

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

151 Statement of compatibility, p. 13.

penalty or to torture or cruel, inhuman or degrading treatment or punishment, protected information must not be shared with that government.

Committee view

1.107 The committee notes that the bill would allow protected information obtained under the warrants to be shared with foreign countries in certain circumstances. The committee notes that the disclosure of protected information with foreign police, intelligence or security agencies engages and limits the right to privacy. To the extent that there may be a risk that disclosure of protected information to a foreign country could expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment, the measure may also engage and limit the right to life and have implications for the prohibition against torture or cruel, inhuman or degrading treatment or punishment.

1.108 The committee notes that the right to privacy may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate. The committee notes that the statement of compatibility did not provide information regarding the specific objective being pursued by this measure and did not provide an assessment of the compatibility of the measure with the right to life and the prohibition against torture or cruel, inhuman or degrading treatment or punishment.

1.109 The committee has not yet formed a concluded view in relation to this matter. It considers further information is require to assess the human rights implications of this bill, and accordingly seeks the minister's advice as to the matters set out at paragraph [1.106].

Legislative instruments

Commonwealth Grant Scheme Guidelines 2020 [F2020L01609][1]

Purpose	This instrument re-makes the Commonwealth Grant Scheme Guidelines 2012, including specifying which units of higher education study will be included in each funding cluster.
Portfolio	Education, Skills and Employment
Authorising legislation	*Higher Education Support Act 2003*
Last day to disallow	15 sitting days after tabling (tabled in the Senate and the House of Representatives on 2 February 2021). Notice of motion to disallow must be given by 18 March 2021[2]
Rights	Education

Increasing the cost of student contribution amounts for certain disciplines

1.110 Chapter 5 of the guidelines specifies which of the four higher education funding clusters (or part of those clusters) a unit of study will be included in.[3] As the explanatory statement notes, these changes are primarily intended to give effect to amendments made by the *Higher Education Support Amendment (Job-Ready Graduates and Supporting Regional and Remote Students) Act 2020.*[4] By establishing which funding cluster a unit of study falls within, the instrument establishes the cost to a Commonwealth-supported student for a place within that unit of study.[5]

International human rights legal advice

Right to education

1.111 In specifying which funding cluster (or part of a cluster) a unit of study will be included in, and thereby establishing how much that unit of study will cost a

1 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Commonwealth Grant Scheme Guidelines 2020 [F2020L01609], *Report 1 of 2021*; [2021] AUPJCHR 6.

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

3 For the purposes of section 33-35 of the *Higher Education Support Act 2003*.

4 Explanatory statement, p. 1.

5 For example, the maximum student contribution amount for a place in a unit of study within funding cluster 1 (Law, Accounting, Administration, Economics, Commerce, Communications, Society and Culture) is $14,500. See, *Higher Education Support Act 2003,* section 93-10.

Commonwealth-supported student, this instrument largely raises the same human rights issues as those raised with respect to the bill that became the *Higher Education Support Amendment (Job-Ready Graduates and Supporting Regional and Remote Students) Act 2020*.[6] As such, the advice provided in relation to that bill in *Report 11 of 2020*,[7] and *Report 13 of 2020*[8] is reiterated in relation to this instrument.

Committee view

1.112 The committee notes that this instrument specifies which units of higher education study will be included in each funding clusters, and that this has the effect of establishing how much that unit of study will cost a Commonwealth-supported student.

1.113 The committee notes that these changes are primarily intended to give effect to amendments made by the *Higher Education Support Amendment (Job-Ready Graduates and Supporting Regional and Remote Students) Act 2020.* The committee assessed the human rights compatibility of the bill that became that Act in *Report 13 of 2020*,[9] including the human rights implications of amending the maximum student contribution amounts for a place in a unit of study.

1.114 As such, the committee refers the minister and parliamentarians to that report in relation to the assessment of the human rights compatibility of this instrument.

6 The bill passed both houses of Parliament on 19 October 2020.

7 Parliamentary Joint Committee on Human Rights, *Report 11 of 2020* (24 September 2020), pp. 48–59.

8 Parliamentary Joint Committee on Human Rights, *Report 13 of 2020* (13 November 2020), pp. 91–109.

9 Parliamentary Joint Committee on Human Rights, *Report 13 of 2020* (13 November 2020), pp. 91–109.

Bills and instruments with no committee comment[1]

1.115 The committee has no comment in relation to the following bills which were introduced into the Parliament between 7 to 12 December 2020. This is on the basis that the bills do not engage, or only marginally engage, human rights; promote human rights; and/or permissibly limit human rights:[2]

- COAG Reform Fund Amendment (No Electric Vehicle Taxes) Bill 2020;
- Customs Amendment (Banning Goods Produced By Uyghur Forced Labour) Bill 2020; and
- Data Availability and Transparency (Consequential Amendments) Bill 2020;
- Defence Amendment (Parliamentary Approval of Overseas Service) Bill 2020;
- Environment Protection and Biodiversity Conservation Amendment (Regional Forest Agreements) Bill 2020;
- Fair Work Amendment (Ten Days Paid Domestic and Family Violence Leave) Bill 2020;
- Fair Work Amendment (Ten Days Paid Domestic and Family Violence Leave) Bill 2020 [No. 2];
- Fair Work (Registered Organisations) Amendment (Withdrawal from Amalgamations) Bill 2020;
- Financial Sector Reform (Hayne Royal Commission Response No. 2) Bill 2020;
- Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020;
- Live Animal Export Prohibition (Ending Cruelty) Bill 2020;
- National Consumer Credit Protection Amendment (Supporting Economic Recovery) Bill 2020;
- Offshore Petroleum and Greenhouse Gas Storage Amendment (Benefit to Australia) Bill 2020;
- Security Legislation Amendment (Critical Infrastructure) Bill 2020;
- Therapeutic Goods Amendment (2020 Measures No. 2) Bill 2020; and

1 This section can be cited as Parliamentary Joint Committee on Human Rights, Bills and instruments with no committee comment, *Report 1 of 2021*; [2021] AUPJCHR 7.

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

- Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020.

1.116 The committee has examined the legislative instruments registered on the Federal Register of Legislation between 2 to 23 December 2020.[3] The committee has reported on one legislative instrument from this period earlier in this chapter. The committee has determined not to comment on the remaining instruments from this period on the basis that the instruments do not engage, or only marginally engage, human rights; promote human rights; and/or permissibly limit human rights.

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