Chapter 1
New and ongoing matters

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

Bills

Better and Fairer Schools (Information Management) Bill 2024[9]

Purpose	This bill seeks to amend the *Student Identifiers Act 2014* to extend the unique student identifier scheme to all primary and secondary school students. The bill sets out how a schools identifier for an individual student would be assigned, verified, collected, used and disclosed.
Portfolio	Education
Introduced	House of Representatives, 15 August 2024
Rights	Children's rights; education; privacy

Expanding the unique student identifier scheme

1.2 This bill would amend the *Student Identifiers Act 2014* (Student Identifiers Act) to extend the unique student identifier (USI) scheme to all primary and secondary school students. Currently, this scheme only applies to higher education students (including university, TAFE and nationally recognised training students).[10] A USI is an individual education number that is designed to remain with a person for life and is required for a student to be eligible for Commonwealth assistance and obtain their qualification or statement of attainment.[11] This bill would enable the assignment of a 'schools identifier' to school students – a unique education number that may later be

---

9 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Better and Fairer Schools (Information Management) Bill 2024, *Report 8 of 2024*; [2024] AUPJCHR 57.

10 The *Education Legislation Amendment (2020 Measures No. 1) Act 2020* amended the *Higher Education Support Act 2003* to provide that all new higher education students commencing study from 1 January 2021, and all students (including existing students) from 1 January 2023, are required to have a USI in order to be eligible for Commonwealth assistance. The Act also amended the *VET Student Loans Act 2016* to provide that all applications for VET student loans made on or after 1 January 2021 must include a student's USI. The Parliamentary Joint Committee on Human Rights commented on this Act when it was first introduced as a bill. See *Report 8 of 2020* (1 July 2020) pp. 28–31 and *Report 10 of 2020* (26 August 2020) pp. 11–19.

11 Office of the Student Identifiers Registrar, *What is a Unique Student Identifier (USI)?* (26 August 2024).

used as a 'student identifier' for the purposes of higher education. The bill sets out how a schools identifier would be assigned, verified, collected, used and disclosed.

1.3 The bill would enable specified entities—including an approved authority for the school, a prescribed public body of the state or territory in which the school is located, and an entity prescribed by the regulations—to apply to the Student Identifiers Registrar (the Registrar) for the assignment of a schools identifier to an individual student.[12] The application must include the individual's 'school identity management information', which is to be defined by the regulations.[13] If such an application is made, the Registrar must assign a schools identifier to the individual if they have not already been assigned a student identifier or a schools identifier.[14] The individual must be notified of the Registrar's decision, either by the Registrar or the applicant.

1.4 The bill would enable an individual or specified entities, such as a registered training organisation or higher education provider, to apply to the Registrar for validation of a schools identifier.[15] The effect of validating a schools identifier is that the identifier is considered to be a student identifier for the purposes of the Student Identifiers Act, meaning that an individual can use the same identifier for higher education.[16] If an application for validation of a schools identifier is made, the Registrar must validate the identifier if the identity of the individual has been verified; the identifier is the schools identifier of the individual; and the individual has not already been assigned a student identifier.[17] The Registrar's decision to either refuse to assign a schools identifier; refuse to validate a schools identifier; or revoke a schools identifier would be reviewable by the Administrative Appeals Tribunal.[18]

1.5 The bill would allow an individual's schools identifier and school identity management information (both of which would be classified as 'protected information' under the bill and would include personal information) to be verified, collected and used by, and shared or disclosed to, the Registrar as well as various

---

12 Schedule 1, item 25, section 13A. If the student is registered in an alternative schooling arrangement under state or territory law, then the specified entities that may apply for the assignment of a schools identifier are the relevant state or territory and an entity prescribed by the regulations (see subsection 13A(2)).

13 Schedule 1, item 4 and item 25, paragraph 13A(3)(b). See explanatory memorandum, p. 12.

14 Schedule 1, item 25, section 13B.

15 Schedule 1, item 25, section 13C.

16 Schedule 1, item 25, section 13D.

17 Schedule 1, item 25, section 13D.

18 Schedule 1, item 25, section 13F. It is noted that on 14 October 2024, the Administrative Appeals Tribunal will be replaced by the Administrative Review Tribunal. See Administrative Appeals Tribunal, *Transition to the Administrative Review Tribunal* (accessed 28 August 2024).

entities for various purposes.[19] With respect to the Registrar, the bill would authorise the Registrar to use or disclose protected information of an individual for the purposes of research that relates (directly or indirectly) to school education, or that requires the use of protected information or information about school education; and that meets the requirements specified by the Education Ministerial Council.[20] Using or disclosing personal information for this purpose would be taken, for the purposes of the *Privacy Act 1988* (Privacy Act), to be authorised, meaning that provisions in the Privacy Act relating to the prohibition on use or disclosure of personal information for a secondary purpose would not apply.[21] Further, the current requirement that the Registrar take reasonable steps to protect a record of student identifiers from misuse, interference and loss, and from unauthorised access, modification or disclosure, would be extended to apply to records of schools identifiers and school identity management information.[22]

1.6 The bill would enable specified entities, such as the approved school authority, state or territory public bodies, and the Secretary and Australian Public Service (APS) employees in the Education Department, to request the Registrar to verify that an identifier is the schools identifier of an individual or to give the entity the schools identifier of an individual.[23] A more limited number of entities, including the approved school authority and state or territory public bodies, would be able to request the Registrar to give them an individual's school identity management information or to verify any such information held by the entity.[24] If such an application is made, the Registrar may verify or give the individual's school identity management information to the entity (or provide reasons for their refusal to do so).[25] Entities that are prescribed by the regulations would also be authorised to collect, use or disclose

---

19 Schedule 1, item 4 defines 'protected information' as a student identifier, schools identifier or school identity management information. Items 39–49 extend the application of Division 5 of the *Student Identifiers Act 2014*, which relates to the collection, use and disclosure of student identifiers, to 'protected information'.

20 Schedule 1, item 46. The Education Ministerial Council comprises Commonwealth and state and territory education ministers. The Council generally meets four times a year to collaborate and make decisions about early childhood education and care, school education, higher education and international education. See Department of Education, *What is the Education Ministers Meeting?* (27 April 2024).

21 Schedule 1, item 55, which amends section 25 of the *Student Identifiers Act 2014*, which relates the circumstances in which use or disclosure of personal information is authorised for the purposes of the *Privacy Act 1988*. Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and is recorded in material form or not. See *Student Identifiers Act 2014*, section 4 and *Privacy Act 1998*, section 6.

22 Schedule 1, items 35–38.

23 Schedule 1, items 28 and 29.

24 Schedule 1, item 32, section 15A.

25 Schedule 1, item 32, section 15B.

protected information of an individual if it is for a purpose, or in circumstances, relating to school education and prescribed by the regulations.[26] Entities may also collect, use or disclose protected information with the express or implied consent of the individual to whom the information relates.[27]

1.7 Further, the bill would extend the application of provisions in the Student Identifiers Act that protect records of student identifiers and prohibit the unauthorised collection, use or disclosure of student identifiers—contravention of either provision constituting an interference with an individual's privacy for the purposes of the Privacy Act—to include schools identifiers and school identity management information.[28] Entities that keep a record of identifier information (including schools identifiers and school identity management information) would be required to take reasonable steps to protect that record from misuse, interference and loss; and from unauthorised access, modification or disclosure.[29] Entities must also not collect, use or disclose protected information if it is not authorised under the Act.[30] Contravention of these provisions may result in an investigation by the Privacy Commissioner or Information Commissioner.[31]

1.8 However, these provisions (relating to protecting records and prohibiting unauthorised disclosure—contravention of which would be an interference with privacy),[32] to the extent that they apply to schools identifiers and school identity management information, would not apply to a state or territory public body unless a declaration is made by the Commonwealth education minister by way of an exempt legislative instrument, at the request of the responsible state or territory education minister.[33] State and territory public bodies (primarily schools) would therefore not be subject to the protected information regulatory regime unless the responsible state or territory education minister requests this, and the Commonwealth education minister makes a declaration to that effect. Non-government schools and entities, however, would be subject to the protected information regulatory scheme.[34]

---

26 Schedule 1, item 47.

27 Schedule 1, items 48 and 49.

28 Schedule 1, items 34–38, 40, 41 and 50

29 Schedule 1, items 34–38.

30 Schedule 1, items 40 and 41.

31 Schedule 1, items 50 and 51.

32 *Student Identifiers Act 2014*, sections 16, 17 and 23.

33 Schedule 1, item 78. The declaration would be exempt and not subject to sunsetting. In its consideration of this bill, the Senate Standing Committee for the Scrutiny of Bills raised concerns about exemption from disallowance and sunsetting. See *Digest 10 of 2024*, pp. 10–12.

34 Explanatory memorandum, [119].

Preliminary international human rights legal advice

Rights of the child and rights to privacy and education

1.9 By authorising the verification, collection, use and disclosure of schools identifiers and school identity management information, the measures would engage and limit the right to privacy. As the measures would apply to primary and secondary school children, the rights of the child would also be engaged and limited. 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, as well as the right to control the dissemination of information about one's private life.[35] The United Nations (UN) High Commissioner for Human Rights has noted that an individual's ability to keep track of what personal information is collected about them and control the many ways in which that information can be used and shared becomes more difficult with larger datasets and the fusing of personal information from various sources.[36] The UN High Commissioner for Human Rights has also noted that the sharing of information and data with third parties as well as the long-term storage of personal data often amounts to further privacy intrusions and other adverse human rights impacts, many of which may not have been envisaged at the time of data collection.[37]

1.10 Children are guaranteed the right to privacy under international human rights law.[38] The UN Committee on the Rights of the Child has emphasised that '[p]rivacy is vital to children's agency, dignity and safety and for the exercise of their rights'.[39] The UN Committee on the Rights of the Child has observed that digital practices, such as automated data processing, mandatory identity verification and information filtering, are becoming routine and cautioned that such practices 'may lead to arbitrary or unlawful interference with children's right to privacy; they may have adverse consequences on children, which can continue to affect them at later stages of their lives'.[40]

1.11 Additionally, Australia is required to ensure that, in all actions concerning children, the best interests of the child are a primary consideration.[41] This requires

---

35 International Covenant on Civil and Political Rights, article 17. See UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [7].

36 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [13].

37 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [14].

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

39 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25 (2021) [67].

40 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25 (2021) [68].

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

legislative, administrative and judicial bodies and institutions to systematically consider how children's rights and interests are or will be affected directly or indirectly by their decisions and actions.[42] Children who are capable of forming their own views also have the right to express those views freely in all matters affecting them. The views of the child must be given due weight in accordance with the age and maturity of the child.[43] By not providing children or their parent or guardian with the opportunity to be involved in, or express views about, the assignment of a schools identifier or the subsequent collection, use and disclosure of the identifier and related information, the measures engage and limit these other rights of the child.

1.12 Further, if the measures had the effect of restricting access to primary or secondary education for students without a schools identifier, the right to education may be engaged and limited. The Parliamentary Joint Committee on Human Rights has previously raised concerns that requiring a USI in order to be eligible for Commonwealth financial assistance for higher education may constitute a retrogressive measure with respect to the obligation to progressively introduce free education, as the practical effect of this measure may be to restrict access to education for students without a USI and unable to pay tuition up front.[44] The committee concluded that this retrogressive measure may not constitute a proportionate limitation on the right to education.[45] With respect to the measures in this bill, noting that schools identifiers are assigned to students without their involvement in the application process or consent to the assignment, it is not clear how likely it would be that a student would not have a schools identifier or if this were the case, what the consequences would be of not having a schools identifier in terms of accessing education. Further information is therefore required with respect to these matters. To the extent that the measures in this bill were to restrict access to education for students without a schools identifier, the committee's previous concerns with respect to the right to education would be relevant. The right to education provides that education should be accessible to all, in particular by making primary education compulsory and free to all and by progressively introducing free secondary education in its different forms, including technical and vocational secondary education.[46] States

---

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

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

44 Parliamentary Joint Committee on Human Rights, *Education Legislation Amendment (2020 Measures No. 1) Act 2020*, *Report 8 of 2020* (1 July 2020) pp. 28–31 and *Report 10 of 2020* (26 August 2020) pp. 11–19.

45 Parliamentary Joint Committee on Human Rights, *Education Legislation Amendment (2020 Measures No. 1) Act 2020*, *Report 10 of 2020* (26 August 2020) p. 19.

46 International Covenant on Economic, Social and Cultural Rights, article 13 and Convention on the Rights of the Child, article 28.

have a duty to refrain from taking retrogressive measures, or backwards steps, in relation to the realisation of the right to education.[47]

1.13 The above rights may be subject to permissible limitations (noting that retrogressive measures are a type of limitation) where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

Legitimate objective

1.14 The statement of compatibility states that the measures in the bill will enable all school students to be assigned a schools identifier, starting in 2025, which will travel with them from their first year of school through to higher education.[48] In his second reading speech, the minister stated that this would support the robust and timely transfer of a student's information as they move from school to school.[49] The stated purpose of the schools identifier is to help identify and share information between schools, sectors and states and territories to support better understanding of student progress, protect student privacy and improve the national evidence base.[50] The statement of compatibility states that the purpose of using an individual's protected information is to meet the objectives of the Student Identifiers Act and support the administration of school education in a way that is reasonably necessary to meet policy objectives.[51] The minister further stated that the measures meet the Commonwealth's obligations under the National School Reform Agreement, which is a joint agreement between the Commonwealth, states and territories that sets out eight policy initiatives.[52]

1.15 It is not clear that these stated objectives would constitute legitimate objectives for the purposes of human rights law. A legitimate objective must be one that is necessary and addresses a public or social concern that is pressing and substantial enough to warrant limiting rights. Improving the transfer and sharing of students' personal information, and supporting the administration of school education, appear to be primarily directed towards administrative convenience, which in and of itself is unlikely to be sufficient to constitute a legitimate objective for the purposes of international human rights law. Further, as to necessity, the explanatory materials have not demonstrated why existing laws and practices are insufficient to achieve the

---

47 See, UN Committee on Economic, Social and Cultural Rights, *General Comment 13: the Right to education* (1999).

48 Statement of compatibility, pp. 6 and 8.

49 The Hon. Jason Clare, Minister for Education, Second reading speech, *House of Representatives Hansard*, 15 August 2024, p. 10.

50 Statement of compatibility, pp. 8–9.

51 Statement of compatibility, p. 8.

52 Mr Jason Clare, Minister for Education, Second reading speech, *House of Representatives Hansard*, 15 August 2024, p. 10. See, Department of Education, *The National School Reform Agreement* (19 December 2023).

stated objectives. For instance, while the statement of compatibility explains that schools identifiers will enable the government to better understand students' progress and facilitate the transfer of student information between schools and educational institutions, it appears that this may already be possible through information sharing agreements between schools and entities, as well as through consent of the student to whom the information relates or their parent or guardian. For example, the Interstate Student Data Transfer Note and Protocol—a joint initiative between the Commonwealth, state and territory education departments and independent and Catholic education sectors—allows the transfer of student information between schools when a child moves from one state or territory to another.[53] The type of information that may be shared between schools includes the child's personal details (such as name and date of birth), information about the school and an outline of the child's attendance, progress in learning areas, subjects studied, support and health care needs.[54] However, in contrast to the measures in this bill, the consent or permission of the parent or guardian and, if appropriate, the child must be obtained in order for information to be shared between schools.[55]

Rational connection

1.16 Under international human rights law, it must also be demonstrated that any limitation on a right has a rational connection to the objective sought to be achieved. In this regard, the key question is whether the relevant measures are likely to be effective in achieving the stated objectives. To answer this question, it is necessary to understand the information that would sit behind, or be associated with, a schools identifier, as well as the type of information that would be captured by 'school identity management information'. The meaning of 'school identity management information' will be prescribed by future regulations. The explanatory memorandum states that it is appropriate to define school identity management information in the regulations so that its meaning is defined with agreement from the Educational Ministerial Council.[56] Without any legislative or other guidance as to its likely meaning, the type and scope of personal information that may be captured by this term is unclear.

1.17 Regarding schools identifiers, the bill does not provide any guidance as to what information would be associated with an identifier. In his second reading speech, the minister referred to possible use cases for schools identifiers, indicating the kind of information that may be associated with an identifier. The minister stated that currently there is only one agreed use case—that is, allowing a schools identifier to

---

53 Department of Education, *Transferring Student Data Interstate* (13 June 2024).

54 Department of Education, *Interstate Student Data Transfer Note Parent/Guardian Fact Sheet* (accessed 2 September 2024).

55 Department of Education, *Interstate Student Data Transfer Note Parent/Guardian Fact Sheet* and *Interstate Student Data Transfer Note Parent/Guardian Frequently Asked Questions* (accessed 2 September 2024).

56 Explanatory memorandum, p. 12.

travel with a student between schools and educational institutions, which would facilitate the timely transfer of the student's information.[57] The minister flagged other potential future use cases of schools identifiers, including monitoring a student's enrolment; allowing teachers and parents to monitor a student's progress over time, for example using NAPLAN reports; allowing policy makers to observe student pathways; and linking Senior Secondary Certificates to the National Skills Passport, which is currently under consideration by the government.[58] Further, it is noted that the current USI Registry System keeps information about a student's name, date and place of birth, gender, contact details and the type of identification provided to verify their identity when applying for a USI.[59] Having regard to the use cases referred to by the minister and the information that is currently associated with a USI, it seems possible that a vast array of personal information could be associated with a schools identifier, including information relating to a student's identity, enrolment, attendance, and NAPLAN and other test results. Additionally, if a student's entire record were to be associated with a schools identifier, there is a risk that highly sensitive personal information could be captured, such as a student's health, counselling, psychological and behavioural records.

1.18 While the breadth of information that could be associated with a schools identifier raises concerns with respect to proportionality (as detailed below), the measures may nonetheless be rationally connected to the stated objectives. For example, collecting and sharing information about a student's test results and NAPLAN records would likely be rationally connected to the stated objective of monitoring a student's academic progress over time. However, depending on the scope of personal information captured by 'school identity management information' and associated with schools identifiers, questions may arise as to whether the full scope of information would be necessary to effectively achieve the stated objectives. For example, if a student's health, counselling and psychological records were captured by the measures, it is not clear that such information would be necessary to monitor a student's academic progress or enrolment status, or support the administration of school education.

Proportionality

1.19 In assessing whether the potential limitations on rights are proportionate to the objectives being sought, it is necessary to consider a number of factors, including whether the proposed limitations are sufficiently circumscribed; whether the

---

57 The Hon. Jason Clare, Minister for Education, Second reading speech, *House of Representatives Hansard*, 15 August 2024, p. 10.

58 The Hon. Jason Clare, Minister for Education, Second reading speech, *House of Representatives Hansard*, 15 August 2024, p. 11. A National Skills Passport would allow people to view and share evidence of their skills and qualifications in an integrated digital system. See Department of Education, *National Skills Passport Consultation* (21 August 2024).

59 Office of the Student Identifiers Registrar, *Privacy* (6 February 2024).

measures are accompanied by sufficient safeguards; and whether there are any less rights restrictive alternatives that could achieve the same stated objectives.

1.20 The breadth of personal information that would be collected and the circumstances in which the information would be used and shared are relevant in considering whether the measures are sufficiently circumscribed. Indeed, the UN Human Rights Committee has stated that legislation must specify in detail the precise circumstances in which interferences with the right to privacy may be permitted.[60] As set out above, the type of personal information that may be captured by school identity management information and associated with schools identifiers is unclear, as it will generally be set out in future regulations. However, given the vast array of personal information collected and held by schools currently, such as a student's personal details (name, date of birth, address and contact details); enrolment and attendance records; health, psychological and counselling records; and behavioural information, the potential breadth of information that may be used and shared could be extensive.

1.21 As to the purposes for which such information may be collected, used and shared, the Registrar would be authorised to use or disclose protected information of an individual for the purposes of research that relates (directly or indirectly) to school education, or that requires the use of protected information or information about school education; and that meets the requirements specified by the Education Ministerial Council.[61] With respect to entities, entities that are prescribed by the regulations would be authorised to collect, use or disclose protected information for a purpose, or in circumstances, relating to school education and prescribed by the regulations.[62] These stated purposes are vague and neither the bill nor the explanatory materials provide guidance in this regard, noting that with respect to entities, most of the detail is to be set out in future regulations. For example, it is unclear what the potential research areas are for which protected information may be shared, and whether information would be de-identified when shared for these purposes. It is also unclear what is meant by the term 'school education' and when a research purpose will be sufficiently related to 'school education' so as to authorise the use or disclosure of protected information. With respect to information used and disclosed by the Registrar, it is unclear what requirements are likely to be specified by the Education Ministerial Council.

---

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

61 Schedule 1, item 46. The Education Ministerial Council comprises Commonwealth and state and territory education ministers. The Council generally meets four times a year to collaborate and make decisions about early childhood education and care, school education, higher education and international education. See Department of Education, *What is the Education Ministers Meeting?* (27 April 2024).

62 Schedule 1, item 47.

1.22 As to whom information may be shared with, the legislation specifies the entities that may request a schools identifier or school identity management information from the Registrar.[63] While specifying the entities in the legislation assists with proportionality, given the large number of entities listed, a significant number of people would, in practice, be authorised to receive and use protected information. For example, all APS employees in the Education Department would be authorised to request the Registrar to give them a schools identifier of an individual.[64] However, there are other circumstances in which the persons to whom protected information may be shared are not specified. For example, the provisions that would authorise the Registrar and entities to disclose protected information for purposes relating to research and school education do not specify to whom the information may be disclosed.[65]

1.23 The vast array of personal information that may potentially be captured by the measures as well as the broad purposes for which, and the lack of specificity regarding to whom, such information may be used and disclosed, raises concerns that the measures may not be sufficiently circumscribed. Relevantly, the UN Committee on the Rights of the Child has highlighted the importance of legislation clearly specifying the purposes for which personal information may be used and disclosed, and the persons or entities authorised to do so:

> Children's personal data should be accessible only to the authorities, organizations and individuals designated under the law to process them in compliance with such due process guarantees as regular audits and accountability measures. Children's data gathered for defined purposes, in any setting…should be protected and exclusive to those purposes and should not be retained unlawfully or unnecessarily or used for other purposes. Where information is provided in one setting and could legitimately benefit the child through its use in another setting, for example, in the context of schooling and tertiary education, the use of such data should be transparent, accountable and subject to the consent of the child, parent or caregiver, as appropriate.[66]

1.24 By not defining the purposes for which a student's personal information may be used and disclosed with sufficient clarity, there appears to be a risk that such information may be used for secondary purposes—some of which may not have been contemplated when the legislation was drafted.

1.25 The measures appear to be accompanied by some legislative safeguards with respect to the right to privacy. The relevant provisions would:

---

63 Schedule 1, items 28, 29 and 32.

64 Schedule 1, item 28.

65 Schedule 1, items 46 and 47.

66 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25 (2021) [73].

(a) require the Registrar and entities to take reasonable steps to protect a record of student identifiers, schools identifiers and school identity management information from misuse, interference and loss; and from unauthorised access, modification or disclosure;[67]

(b) prohibit the unauthorised collection, use or disclosure of protected information;[68]

(c) provide that contraventions of the above provisions (with respect to protecting records and unauthorised collection, use and disclosure of information) would constitute an interference with privacy for the purposes of the Privacy Act;[69] and

(d) extend the Information Commissioner's functions under the Privacy Act to include protected information, meaning the Commissioner could investigate an act or practice that may be an interference with privacy.[70]

1.26 However, to the extent that the provisions outlined in (a) to (c) above would apply to schools identifiers and school identity management information, those provisions would not apply to state and territory public bodies unless a declaration is made by way of an exempt legislative instrument by the education minister.[71] The explanatory memorandum states that this would allow states and territories to agree to the application of the protected information regulatory regime at their discretion.[72] By disapplying these provisions with respect to state and territory public bodies, the strength of the safeguards outlined in (a) to (c) are considerably weakened, given the majority of schools are public.

1.27 The explanatory materials and the minister's second reading speech identify the following additional safeguards with respect to the right to privacy:

(e) the application of the Privacy Act and relevant state and territory privacy legislation;

(f) requiring the disclosure of information for research purposes to meet the requirements set by the Educational Ministerial Council; and

(g) the establishment by education ministers of a data governance framework for schools identifiers, which would:

---

67 Schedule 1, items 35–38.

68 Schedule 1, items 39–41. See also item 74.

69 Schedule 1, item 50.

70 Schedule 1, item 51.

71 Schedule 1, item 78.

72 Explanatory memorandum, [119].

- implement national uniform restrictions on the use and disclosure of schools identifiers and specified information associated with administration by education authorities;
- set out Education Ministers' agreed approach to the handling of requests for schools identifier data made under the *Data Availability and Transparency Act 2022* (Cth);
- provide guidance and information on authorised adoption, uses and disclosures of schools identifiers; and
- provide guidance and information on data entry requirements for schools identifier assignment and maintenance.[73]

1.28 As to the safeguard value of (e), the Parliamentary Joint Committee on Human Rights has stated on a number of occasions that compliance with the Privacy Act is not a complete answer to concerns about interference with the right to privacy for the purposes of international human rights law. The Privacy Act contains a number of exceptions to the prohibition on use or disclosure of personal information for a secondary purpose, including where its use or disclosure is authorised under an Australian law, which may be a broader exception than permitted in international human rights law. Indeed, this bill would expand the circumstances in which the use or disclosure of personal information by the Registrar is taken to be authorised for the Privacy Act.[74] Further, a 2022 review of the Privacy Act (the review) identified numerous inadequacies in the Act in protecting privacy and personal information. It made several recommendations to strengthen privacy protections, including requiring that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances, which would involve consideration of a range of factors such as the potential adverse impact or harm to the individual, whether any privacy impact is proportionate to the benefit, and whether there are less intrusive means of achieving the same objective.[75] The government's recent response to the review agreed to a number of recommendations and agreed in principle with others, such as the recommendation with respect to fair and reasonable handling of personal information.[76] With respect to state and territory privacy legislation, without a comprehensive review of this broader legislative framework, it is not possible to conclude whether the safeguards contained in this other legislation are sufficient to protect the right to privacy for the purposes of international human rights law.

---

73 Explanatory memorandum, pp. 3–4; statement of compatibility, pp. 7–8; The Hon. Jason Clare, Minister for Education, Second reading speech, *House of Representatives Hansard*, 15 August 2024, p. 10.

74 Schedule 1, item 55.

75 Attorney-General's Department, *Privacy Act Review: Report 2022* (February 2023) Recommendation 12, pp. 1, 8.

76 Australian Government, *Government Response: Privacy Act Review Report* (September 2023) p. 27.

1.29 The value of the other non-legislative safeguards outlined in (f) and (g) will depend on how they operate in practice. In general, discretionary safeguards alone may not be sufficient for the purpose of a permissible limitation under international human rights law.[77] This is because discretionary safeguards are less stringent than the protection of statutory processes as there is no requirement to follow them. The importance of strong legislative safeguards has been emphasised by the UN Committee on the Rights of the Child:

> Legislation should include strong safeguards, transparency, independent oversight and access to remedy. States parties should require the integration of privacy-by-design into digital products and services that affect children. They should regularly review privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy.[78]

1.30 It is not clear that the safeguards outlined above would be sufficient to ensure that any limitation the right to privacy is proportionate. Further, many key safeguards recognised as being effective for the purposes of international human rights law have not been included in the bill. The UN High Commissioner on Human Rights has outlined the minimum safeguards that are necessary to protect personal data:

> First, processing of personal data should be fair, lawful and transparent. The individuals whose personal data are being processed should be informed about the data processing, its circumstances, character and scope, including through transparent data privacy policies. In order to prevent the arbitrary use of personal information, the processing of personal data should be based on the free, specific, informed and unambiguous consent of the individuals concerned, or another legitimate basis laid down in law. …the amount and type of data and the retention period need to be limited, data must be accurate and anonymization and pseudonymization techniques used whenever possible. Changes of purpose without the consent of the person concerned should be avoided and when undertaken, should be limited to purposes compatible with the initially specified purpose. Considering the vulnerability of personal data to unauthorized disclosure, modification or deletion, it is essential that adequate security measures be taken. Moreover, entities processing personal data should be accountable for their compliance with the applicable data processing legal and policy framework. Finally, sensitive data should enjoy a particularly high level of protection.[79]

---

77 See e.g. UN Human Rights Committee, *General Comment 27, Freedom of movement (Art.12)* (1999).

78 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25 (2021) [70].

79 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [29].

1.31 More specifically with respect to children's data and information, the UN Committee on the Rights of the Child has stated:

> States parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations. They should further ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing. They should also provide information to children, parents and caregivers on such matters, in child-friendly language and accessible formats.[80]

1.32 Many of the safeguards described above are absent from the bill. In particular, neither the Registrar nor entities are required to obtain the consent of the child or their parent or guardian in order to collect, use and disclose their personal information. Indeed, the child and their parent or guardian would not need to be informed about an application for a schools identifier; they would only be notified after a schools identifier had been assigned. The bill does not contain any mechanism by which a child or their parent or guardian could object to, or express their views about, the collection, use or disclosure of their personal information and data, and does not provide for any exemptions to the assignment of a schools identifier. It would appear that there may be many reasons why a student or their parent or guardian may wish to seek an exemption from having a schools identifier assigned to them or their child, including, for example, victims of family violence who have concerns about their personal information being stored in such a centralised way. The lack of flexibility to treat different cases differently raises concerns with respect to proportionality. Further, the ability to apply for an exemption may operate as a safeguard with respect to the right to education (noting that the statement of compatibility did not address whether the measures may limit this right and so provided no information as to safeguards that would protect this right).

1.33 The inclusion of these additional safeguards, particularly the requirement to obtain an individual's consent for the collection, use and disclosure of their personal information, would appear to be a less rights restrictive approach to achieving the stated objectives. In this regard, as noted above, the Interstate Student Data Transfer Note and Protocol requires the consent or permission of the parent or guardian and, if appropriate, the child in order for the child's personal information to be shared

---

80 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25 (2021) [72]. See also UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [30].

between schools.[81] It is not clear why a similar approach cannot be taken with respect to these measures.

Committee view

1.34 The committee notes that the bill seeks to extend the Unique Student Identifier scheme to all Australian primary and secondary school students by enabling the assignment of a schools identifier to each student. By authorising the verification, collection, use and disclosure of schools identifiers and school identity management information (both of which would be classified as 'protected information' under the bill and would include personal information), the measures would engage and limit the right to privacy. As the measures would apply to primary and secondary school children, the rights of the child would also be engaged and limited. If the measures had the effect of restricting access to primary or secondary education for students without a schools identifier, the right to education may also be engaged and limited.

1.35 The committee notes that the stated objectives, including to improve the transfer of student information between entities and support the administration of education, appear to largely be directed towards administrative convenience, raising questions as to whether these would constitute legitimate objectives for the purposes of international human rights law. Having regard to the vast array of personal information that may potentially be captured by the measures, as well as the broad purposes for which, and the lack of specificity regarding to whom, such information may be used and disclosed, it is not clear that the measures would be sufficiently circumscribed. The committee also notes that while there are some safeguards accompanying the measures, it is not clear that these would be sufficient, noting that key safeguards recognised as being effective under international human rights law are missing, such as obtaining the consent of the child or their parent or guardian for the collection, use and disclosure of their personal information. The committee therefore considers that further information is required to assess the compatibility of these measures with the right to privacy, the rights of the child and the right to education, and as such seeks the minister's advice in relation to:

(a) how likely is it that a student would not have a schools identifier assigned to them; and if that were the case, what are the consequences of not having a schools identifier in terms of accessing primary and secondary education;

(b) what is the pressing and substantial public or social concern that the measures seek to address;

(c) what are the existing arrangements for the sharing of a students' personal information, including school records, between schools or

---

81 Department of Education, *Interstate Student Data Transfer Note Parent/Guardian Fact Sheet* and *Interstate Student Data Transfer Note Parent/Guardian Frequently Asked Questions* (accessed 2 September 2024).

educational institutions (for example, in the event that a student transfers to another school);

(d) why current laws and practices, particularly the Interstate Student Data Transfer Note and Protocol, are insufficient to achieve the stated objectives;

(e) why the bill does not require the consent of the student and/or their parent or guardian in order to collect, use and share the student's personal information;

(f) what type of information is likely to be captured by 'school identity management information' and why is it necessary to define this term in regulations rather than the bill itself;

(g) what information would sit behind, or be associated with, a schools identifier. For example, would a student's full school record be associated with their schools identifier, including potentially highly sensitive personal information, such as a student's health, counselling, psychological and behavioural records;

(h) how long would a student's personal information be retained by the Registrar, and who is able to access this information;

(i) in circumstances where the Registrar discloses student identifiers to entities, would this involve sharing the number of the identifier only or would it involve sharing associated information (such as a student's name, age, gender identity, language, test results, health and behavioural information etc);

(j) what are examples of potential research areas for which protected information may be shared;

(k) what is meant by the term 'school education' in the context of sharing information for purposes relating to this;

(l) whether guidance will be provided as to when a research purpose will be sufficiently related to 'school education' so as to authorise the use or disclosure of protected information;

(m) why is it necessary that protected information be shared for research that indirectly relates to school education;

(n) what requirements are likely to be specified by the Education Ministerial Council for the purposes of sharing protected information for research;

(o) when sharing information for research purposes, would the information be required to be de-identified and if not, why not;

(p) whether students and their parents or guardians would be informed of the various ways in which their personal information is being, or may be, used and disclosed;

(q) to whom the Registrar and entities may disclose protected information for purposes relating to research or school education (with respect to proposed subsection 18(5) and 18C);

(r) what entities and what purposes or circumstances are likely to be prescribed by the regulations with respect to proposed section 18C, which would authorise entities prescribed by the regulations to use or disclose protected information for a purpose or in circumstances prescribed by the regulations;

(s) what remedies would be available to students and their parents or guardians in circumstances where their right to privacy has been violated (for example if personal information is used or disclosed unlawfully or without authorisation), and would they be notified of such a violation;

(t) when would the data governance framework likely be established and what, if any, safeguards would it contain with respect to the right to privacy and the rights of the child (beyond those set out above);

(u) whether there is any mechanism by which a child or their parent or guardian could object to, or express their views about, the assignment of a schools identifier or the collection, use or disclosure of their personal information and data; and if not, why not;

(v) whether, as the bill is currently drafted, a student or their parent or guardian could choose not to have a schools identifier or choose to opt-out of the scheme at a later stage, and if not, why not;

(w) will schools identifiers become compulsory for all primary and secondary school students, noting that while proposed section 13A provides that entities *may* apply to the Registrar for schools identifiers to be assigned to school students, the statement of compatibility states that the bill will see a USI issued to every Australian school student;

(x) if a schools identifier will be compulsory for all students in the near future, are exemptions available for those who do not wish to have a schools identifier;

(y) why is it necessary that state and territory public bodies only be subject to the protected information regulatory regime (sections 16, 17 and 23 of the Act) if the education minister makes a declaration to that effect;

(z) what safeguards accompany the measures to ensure that, in all actions concerning children, the best interests of the child are a primary consideration; and

(aa) whether less rights restrictive alternatives were considered and if so, what these are and why they are insufficient to achieve the stated objectives.

Family Law Amendment Bill 2024[82]

Purpose	This bill seeks to amend the *Family Law Act 1975* and make consequential amendments to the *Evidence Act 1995*, *Federal Circuit and Family Court of Australia Act 2021*, *Federal Proceedings (Costs) Act 1981*, *Child Support (Registration and Collection) Act 1988* and *Child Support (Assessment) Act 1989* Schedule 1 seeks to amend the property framework in the *Family Law Act 1975* to codify aspects of the common law and ensure the economic effects of family violence are considered in property and spousal maintenance proceedings Schedule 2 seeks to provide a regulatory framework for Children's Contact Services Schedule 3 seeks to improve case management in family law proceedings by, amongst other matters: permitting the family law courts to determine if an exemption to the mandatory family dispute resolution requirements applies; safeguarding against the misuse of sensitive information in family law proceedings; and amending Commonwealth Information Order powers and expanding the category of persons about which violence information must be provided to the family law courts in child related proceedings Schedule 4 seeks to insert definitions of 'litigation guardian' and 'manager of the affairs of a party', remake costs provisions, and require superannuation trustees to review actuarial formulas used to value superannuation interests to ensure courts have access to accurate and reasonable valuations Schedule 5 provides for review of the operation of the bill and tabling of a report of the review in the Parliament
Portfolio	Attorney-General
Introduced	House of Representatives, 22 August 2024
Rights	Rights of the child; protection of the family; privacy; effective remedy

Use and disclosure of safety-related information by Children's Contact Services

1.36 Schedule 2 to the bill seeks to amend Part II of the *Family Law Act 1975* (Family Law Act) to provide for the accreditation and regulation of existing services referred

82 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Family Law Amendment Bill 2024, *Report 8 of 2024*; [2024] AUPJCHR 58.

to as 'Children's Contact Services' (CCS). These are services that facilitate contact between a child and a member of the child's family with whom the child is not living, and where members of the family may not be able to safely manage such contact, and are provided on a professional, commercial or charitable basis.[83] The bill would provide that accreditation rules may be made in relation to individuals as CCS practitioners, and to persons (whether or not individuals) and other entities as CCS businesses.[84]

1.37 The bill would regulate the confidentiality of certain safety-related information held by a service. Specifically, it would provide that a person who is or has been an 'entrusted person' must not use or disclose safety information obtained by the person in their capacity as an entrusted person, unless the use or disclosure is required or authorised by section 10KE.[85] An 'entrusted person' is a CCS practitioner or CCS business,[86] a director or other officer of a CCS business, or a person employed or engaged to perform work (whether paid or unpaid) for or on behalf of a CCS business.[87] 'Safety information' is information that relates to the risks of harm to a child or a member of a child's family, or to the identification and management of such risks, if CCS have been, are being or will be, provided to the child, and the risks are those that may arise in connection with the use, facilitation or provision of the service.[88]

1.38 Subsections 10KE(4)–(9) provide for permitted uses or disclosure of safety information by an entrusted person. These include that an entrusted person:

- must disclose safety information if they reasonably believe it is necessary for the purpose of complying with a law of the Commonwealth, state or territory;
- may use safety information for the purposes of performing the person's functions as an entrusted person;
- may disclose safety information to one or more other entrusted persons if they are engaged by a particular CCS business and it is reasonable to disclose the safety information to enable the CCS business to appropriately provide children's contact services in respect of the child;

---

83 Schedule 2, item 15, subsection 10KB(1). CCS do not include services provided as a result of intervention by a child welfare officer of a state or territory; supervision of contact between a child and a family member who is in a correctional institution or services prescribed by delegated legislation. See, subsection 10KB(3).

84 Schedule 2, item 4, paragraph 10A(1)(b).

85 Schedule 2, item 15, subsection 10KE(1).

86 Schedule 2, item 15, section 10KC defines a 'CCS practitioner' to mean an individual accredited as a CCS practitioner under the Accreditation Rules. Section 10KD defines a 'CCS business' to mean a person or other entity that is accredited as a CCS business under the Accreditation Rules.

87 Schedule 2, item 15, subsection 10KE(2).

88 Schedule 2, item 15, subsection 10KE(3).

- may use or disclose safety information that is a communication (including an admission) made by an individual to an entrusted person, if consent is given by the person if 18 or over, or where the person is 15, 16 or 17 with the consent of the person if they have the capacity to consent, or where under 15 with the consent of each person who has parental responsibility for the child or a court;
- may use or disclose safety information where they reasonably believe that the use or disclosure is necessary to protect a child from the risk of serious harm or preventing or lessening a serious and imminent threat to the life or health of a person, or reporting the commission of an offence involving violence or a threat of violence to a person;
- may use or disclose safety information where they reasonably believe it is necessary for preventing or lessening a serious and imminent threat to the property of a person, or reporting the commission of an offence involving intentional property damage or the threat of property damage;
- may use or disclose safety information where they reasonably believe it is necessary to assist an independent children's lawyer to represent the child's interests; and
- may disclose safety information in order to provide information other than personal information for research relevant to families.

Preliminary international human rights legal advice

Rights of the child and right to protection of the family

1.39 Insofar as the measure provides for regulations to be made for the accreditation of CCS to support the safety and quality of services offered for facilitating contact between a child and members of their family, this measure would promote the rights of the child and the right to protection of the family. Children have special rights under human rights law taking into account their particular vulnerabilities.[89] The rights of children include protection from harmful influences, abuse and exploitation and, in all actions concerning children, the best interests of the child are a primary consideration.[90] The right to respect for the family requires the state not to arbitrarily or unlawfully interfere in family life and to adopt measures to protect the family.[91] The family is recognised as the natural and fundamental group unit of society and, as such, entitled to protection. In this regard, the explanatory memorandum states that CCS have provided a critical function in the family law sector since the late 1990's, and that

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

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

91 International Covenant on Civil and Political Rights, articles 17 and 23; and the International Covenant on Economic, Social and Cultural Rights, article 10.

'the increased recognition of risk factors in separating families (including family violence, abuse and mental health concerns) has increased concerns that lack of oversight could result in avoidable risks to the safety of clients and staff not being adequately addressed'.[92] It notes that prior inquiries have recommended that an accreditation scheme be established to standardise quality and safety practices, provide a complaints mechanism for clients, and ensure that providers have the skills and tools to supervise and protect children effectively. The statement of compatibility identifies that these measures promote the best interests of the child and the right to protection of the family.[93]

Right to privacy

1.40 However, by providing for the use and disclosure of safety information in certain circumstances, this measure also engages and limits the right to privacy. The right to privacy includes respect for informational privacy, including the right to respect for private and confidential information, particularly the storing, use and sharing of such information**.[94]** 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.

1.41 The statement of compatibility briefly identifies that providing for the use and disclosure of personal information by CCS engages the right to privacy.[95]

1.42 It appears that supporting the operation of a workable and effective CCS, and thereby supporting children to see members of their family in a safe manner, would constitute a legitimate objective for the purposes of international human rights law. Permitting the use and disclosure of safety information would, in some circumstances, appear to be rationally connected to (that is, capable of achieving) that objective. For example, an entrusted person would be permitted to use or disclose safety information if they reasonably believed that it was necessary to prevent or lessen a serious or imminent threat to the life or health of a person.[96]

1.43 However, a key aspect of whether a limitation on the right to privacy can be justified is whether the limitation is proportionate to the objective being sought. In this respect, it is necessary to consider a number of factors, including whether a proposed limitation is sufficiently circumscribed, whether it is accompanied by

---

92 Explanatory memorandum, p. 99.

93 Statement of compatibility, pp. 14 and 30.

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

95 The assessment of Schedule 2 in relation to the right to protection of the family does include a brief discussion of the privacy implications of regulating the use and disclosure of safety information. See pp. 28–29.

96 Schedule 2, item 15, paragraph 10KE(8)(b).

sufficient safeguards, and whether any less rights restrictive alternatives could achieve the same stated objective.

1.44 In relation to whether the measure is appropriately circumscribed, the range of people who may use and disclose safety information, the range of persons to whom safety information may be disclosed, and the circumstances in which safety information may be used and disclosed, are broad. Further, 'safety information' itself is defined very broadly. 'Safety information' means information that relates to the risks of harm to a child or a member of their family, or to the identification and management of such risks, in the course of using the CCS.[97] The explanatory memorandum states that this includes, but is not limited to, contact details and addresses, vehicle details (if required for parking) or transport routes, arrangements for parties to enter the CCS premises or contact location, the level and extent of supervision or monitoring that is required for the sessions, and information relating to the development of, revision of, or content of any safety plans developed for the purposes of service provision.[98]

1.45 An 'entrusted person' encompasses a wide range of individuals including a CCS practitioner, a CCS business, and directors or persons employed or engaged by a CCS business. This would also include volunteers in a CCS business. The statement of compatibility does not explain why such a broad range of individuals should be entrusted persons and therefore able to access, use and disclose safety information. It is unclear whether entrusted persons would be required to be provided with appropriate training to be able to make decisions regarding when to use or disclose the information. For example, it is not clear that all workers would understand what constitutes a 'reasonable belief' as to when disclosure of safety information is necessary to comply with Commonwealth, state or territory laws, necessary to protect a child from the risk of harm or preventing or lessening a serious and imminent threat to the life or health of a person. It is also unclear how, and based on what training or expertise, an entrusted person would accurately assess whether a child who is aged 15, 16 or 17 years old may have capacity to consent.

1.46 In addition, the statement of compatibility does not explain to whom safety information may be disclosed and what they may do with that information. For example, paragraph 10KE(8) would permit an entrusted person to disclose safety information to *any* person or entity, provided they reasonably believed that the disclosure (or use) was necessary to do a range of things, including to: report the likely commission of an offence involving violence or a threat of violence to a person; and prevent, or lessen a serious and imminent threat to the life and health of a person or to property. It also does not explain why each of the exceptions listed are necessary and whether they are appropriately targeted. For example, where safety information may be used for the purposes of performing the person's functions as an entrusted

97 Schedule 2, item 15, subsection 10KE(3).

98 Explanatory memorandum, p. 104.

person, it is not clear what the functions of an entrusted person are, and it could conceivably cover a large range of activities that may or may not directly relate to the safety of a child.

1.47 As to safeguards, the explanatory memorandum explains that, where an entrusted person discloses safety information for research relevant to families, this information must be de-identified.[99] This may be an important safeguard in relation to this particular use. However, for the other listed exceptions for the use and disclosure of safety information, it is not clear what safeguards are in place. Section 10KG provides that the accreditation rules may prescribe civil penalty provisions to be made in relation to requirements to be complied with by CCS practitioners and CCS businesses. This may serve as an important safeguard, provided such provisions are made. However given the broad permitted use and disclosure of safety information, it may have limited safeguard value in practice. It is unclear whether entrusted persons will have any obligations in the accreditation rules to consider the privacy and security of the safety information they have access to, for example, who has access to safety information disclosed, where it will be stored and how long it will be stored for. In addition, no information is provided as to what, if any, other existing legal or regulatory frameworks regulated the use and disclosure of information that would be 'safety information' under this bill prior to its introduction, and whether any such frameworks would continue to apply to CCS.

1.48 As to the availability of review and the capacity for oversight, the bill would require a review of amendments (including those relating to CCS) three years after commencing.[100] However, it is unclear whether and how CCS are subject to oversight and review with respect to the use and disclosure of safety information.

Committee view

1.49 The committee notes that the accreditation of Children's Contact Services (CCS) is an important measure to improve the safety and quality of services facilitating contact between children and their families and that the regulation of the use and disclosure of safety information is an important aspect of this measure. The committee considers that the measure promotes the rights of the child and the right to protection of the family, but that the use and disclosure of safety information necessarily engages and limits the right to privacy.

1.50 The committee considers further information is required to assess the compatibility of this measure with the right to privacy, and as such seeks the Attorney-General's advice in relation to:

(a) why it is appropriate for the definition of entrusted persons to be so broad and whether such persons will be appropriately trained;

---

99 Explanatory memorandum, p. 105.

100 Schedule 5.

(b) why is the definition of entrusted persons not confined to a class of persons whose role involves access to and assessment of this information;

(c) why the bill does not require that an entrusted person who is permitted to use and disclose safety information in certain circumstances must receive training relating to identifying those circumstances in practice;

(d) to whom an entrusted person can disclose safety information, and what that individual or body can then do with that information;

(e) why each of the exceptions permitting the use and disclosure of safety information in subsections 10KE(4)–(9) are necessary; and

(f) what safeguards exist, if any, to protect safety information disclosed or used pursuant to these exceptions;

(g) whether entrusted persons will have any obligations in the accreditation rules to consider the privacy and security of the safety information they have access to, for example, who has access to safety information disclosed, where it will be stored and how long it will be stored for;

(h) what, if any, other existing legal or regulatory frameworks regulated the use and disclosure of information that would be 'safety information' under this bill prior to its introduction and whether any such frameworks would continue to apply to CCS; and

(i) whether and how CCS are subject to oversight and review with respect to the use and disclosure of safety information.

Immunity from criminal and civil proceedings

1.51 Section 10A of the Family Law Act provides that regulations may prescribe accreditation rules, relating to the accreditation of persons as family counsellors, family dispute resolution practitioners, and to perform other roles prescribed by the regulations.

1.52 The bill would provide that accreditation rules may relate to individuals as CCS practitioners, and persons and other entities as CCS businesses.[101] It also seeks to insert section 10AA into the Family Law Act to provide that no action, suit or proceeding lies against the Commonwealth, or an officer of the Commonwealth, in relation to any act done, or omitted to be done, in good faith in the performance or exercise, or the purported performance or exercise, of a function, power or authority conferred by the accreditation rules.

[101] Schedule 2, item 4, paragraph 10A(1)(b).

Preliminary international human rights legal advice

Right to an effective remedy

1.53 By excluding the Commonwealth from civil and criminal liability for actions done or not done in good faith in accordance with the accreditation rules, this measure engages the right to an effective remedy. This is because if such an act done or omitted by the Commonwealth or an officer of the Commonwealth resulted in a violation of a person's human rights (such as the right to privacy), they would be unable to seek a remedy for that violation from the Commonwealth.

1.54 The right to an effective remedy requires the availability of a remedy which is effective with respect to any violation of rights and freedoms recognised under the International Convention on Civil and Political Rights (such as the right to privacy).[102] It includes the right to have such a remedy determined by competent judicial, administrative or legislative authorities or by any other competent authority provided for by the legal system of the state. While limitations may be placed in particular circumstances on the nature of the remedy provided (judicial or otherwise), States parties must comply with the fundamental obligation to provide a remedy that is effective.[103]

1.55 While the explanatory memorandum states that 'it is considered reasonable and appropriate to indemnify officers of the Commonwealth against actions for negligence arising from a good faith policy decision as to a person or entity's compliance with the accreditation rules, made in the performance of their duties and based on information provided by that person or entity',[104] the statement of compatibility does not identify that this engages the right to an effective remedy. As such, no information is provided as to whether and how this proposed measure is consistent with the right.

Committee view

1.56 The committee notes that providing that no action, suit or proceeding can be made against the Commonwealth, or an officer of the Commonwealth, for actions done or not done in good faith in accordance with the accreditation rules engages the right to an effective remedy. The committee considers further information is required

---

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

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

104 Explanatory memorandum, pp. 101–102.

to assess the compatibility of this measure with this right, and as such seeks the Attorney-General's advice in relation to:

(a) whether and how the measure is consistent with the right to an effective remedy; and

(b) what remedies are available to persons where performance by the Commonwealth, or an officer of the Commonwealth, in good faith in accordance with the Accreditation Rules results in a violation of their human rights.

Migration Amendment (Overseas Organ Transplant Disclosure and Other Measures) Bill 2024[105]

Purpose	This bill seeks to amend the *Migration Act 1958* to require the disclosure of information about overseas organ transplants by persons entering Australia
Portfolio	Private Senator's Bill
Introduced	Senate, 22 June 2023 (third reading agreed to 21 August 2024)
Rights	Privacy

Requiring provision of information about overseas organ transplants

1.57 This bill seeks to amend the *Migration Act 1958* to require a person to answer questions on their passenger card about whether they have received an organ transplant outside Australia in the five years prior, and if so to provide further information.[106]

1.58 The bill would require a person to answer:

- Have you received an organ transplant outside Australia in the past five years?
- If yes, for each organ transplant you received outside Australia within the last five years, what is the place (the country, and the town or city) of the medical facility, and the name of the medical facility, at which you received the transplant?

International human rights legal advice

Right to privacy

1.59 Requiring the provision of information about organ transplants which have taken place in the previous five years outside Australia 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.[107] It also includes the right to control the dissemination of information about one's private life.

---

105 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Migration Amendment (Overseas Organ Transplant Disclosure and Other Measures) Bill 2024, *Report 8 of 2024*; [2024] AUPJCHR 59.

106 Schedule 1, item 1. The bill initially included further provisions relating to the migration visa character test, but these did not proceed.

107 International Covenant on Civil and Political Rights (ICCPR), article 17.

1.60 The right to privacy may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective. The statement of compatibility does not identify that requiring the provision of personal medical information would engage and limit the right to privacy, meaning no assessment of its compatibility is provided.

1.61 As the bill is intended to facilitate the gathering of information about organ transplants (including to identify where a person may have obtained a trafficked organ), it may promote the human rights of people outside Australia who are affected by the trafficking of human organs (and by related human rights abuses in some cases). The statement of compatibility with human rights identifies that these provisions seek to give effect to international law related to organ trafficking and trafficking in persons.[108]

1.62 The statement of compatibility states that the bill seeks to better inform the Commonwealth about people entering Australia who have received an organ transplant.[109] This may be capable of constituting a legitimate objective under international law (though it is noted that a legitimate objective must be one which is pressing and substantial). The statement of compatibility also notes that it seeks broadly to address organ trafficking, which is a clear legitimate objective (though noting that the explanatory materials do not identify the numbers of persons believed to be entering Australia who have received an organ as a result of trafficking). However, it is not clear how requiring a person to answer these questions with respect to organ transplants in the past five years would be rationally connected to (that is, capable of achieving) that objective. For example, it is not clear whether, and to what extent, providing the name and location of a particular medical facility would assist in identifying whether the organ in question was provided as a result of trafficking. It is also unclear whether the responses to these questions trigger subsequent investigations or other inquiries. While the bill would require the minister to report annually on the answers to these questions, this report would not be required to identify the name of medical facilities.[110]

1.63 As to proportionality, no information is provided as to: why a period of five years and not a shorter period is necessary; why a person would be required to disclose the information every time they enter Australia; the consequences of failing to answer; whether in answering the questions a person may risk incriminating themselves and if so whether any immunities would apply; how the information is used (for example, is it used to initiate further investigations); who the information may be disclosed to (and whether this may include domestic law enforcement agencies); where the information is stored; why there would not be an option to not

---

108 Statement of compatibility, p. 7.

109 Statement of compatibility, p. 7.

110 Explanatory memorandum, p. 2.

disclose the information for privacy reasons; and why less rights restrictive alternatives would be ineffective to achieve the stated objective of the measure. It is also unclear whether the information could be disclosed to foreign countries. If, for example, the information could be disclosed to a foreign country where organ trafficking was suspected to be occurring, and a person was subsequently placed at risk of the death penalty, or of torture or other cruel, inhuman or degrading treatment, or another human rights violation, this measure would raise broader human rights concerns.[111]

1.64 Consequently, it is not clear that this bill would be rationally connected to (that is, effective to achieve) its stated objective, and constitute a proportionate limit on the right to privacy.

Committee view

1.65 The committee notes that this private Senator's bill seeks to amend the *Migration Act 1958* to require the provision of information about overseas organ transplants by persons entering Australia.

1.66 The committee notes that it initially considered this bill in its scrutiny *Report 8 of 2023*, noting that if the bill proceeded further it may make a substantive comment. The committee notes that the bill has since passed the Senate.

1.67 The committee notes that requiring the provision of personal medical information by all persons entering Australia engages and limits the right to privacy, which the statement of compatibility does not identify. While the committee notes the seriousness of unethical organ trafficking, the committee considers that it is unclear whether and how the bill would be effective to achieve its stated objective, or a proportionate means of achieving it, and as such considers that it is not clear that the bill would constitute a permissible limit on the right to privacy.

1.68 The committee draws these human rights concerns to the attention of the legislation proponent and the Parliament, and makes no further comment.

---

111 The right to life imposes an obligation on Australia to protect people from being killed by others or from identified risks. International law prohibits states which have abolished the death penalty (such as Australia) from exposing a person to the death penalty in another state. International Covenant on Civil and Political Rights, article 6. Australia has an obligation not to subject any person to torture or to cruel, inhuman or degrading treatment or punishment. The prohibition on torture is absolute and can never be subject to permissible limitations (see ICCPR article 7 and the Convention Against Torture).