Chapter 1
New and ongoing matters

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

Bills

Defence Amendment (Safeguarding Australia's Military Secrets) Bill 2023[10]

Purpose	This bill seeks to amend the *Defence Act 1903* to create two new offences if an individual performs certain work without a foreign work authorisation
Portfolio	Defence
Introduced	House of Representatives, 14 September 2023
Rights	Private life; work

Offence to perform certain work or provide certain training without authorisation

1.2 The bill seeks to introduce two new offences, both subject to up to 20 years imprisonment, relating to performing work for, or providing training to, foreign organisations or bodies without prior ministerial authorisation. In particular, the bill would make it an offence:

(a) for a foreign work restricted individual to perform work for, or on behalf of, a military organisation or government body of a relevant foreign country;[11] and

(b) for an Australian citizen or permanent resident to provide training to, or on behalf of, a military organisation or government body of a relevant foreign country if the training relates to goods, software or technology that are designed or adapted for use by armed forces or are goods that are inherently lethal.[12]

---

10 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Defence Amendment (Safeguarding Australia's Military Secrets) Bill 2023, *Report 11 of 2023*; [2023] AUPJCHR 105.

11 Schedule 1, item 1, proposed section 115A.

12 Schedule 1, item 1, proposed section 115B. See also Part 1 of the Defence and Strategic Goods List and explanatory memorandum, p. 14.

1.3 The bill seeks to define a 'foreign work restricted individual' to be a former defence staff member, including a member of the Permanent Forces or full-time Reservist or an APS employee in the Department of Defence or the Australian Submarine Agency.[13] However, the bill also gives the minister the power to make a legislative instrument determining classes of defence staff members to whom these restrictions would not apply, and in making this determination the minister may consider the particular kinds of work performed by defence staff members and the period of time that has elapsed since the performance of that work.[14] The bill provides that all countries would automatically be considered to be a relevant foreign country unless the minister determines, in a legislative instrument, that a country not be a relevant foreign country.[15]

1.4 The offences would not apply if:

(a) the minister has granted a foreign work authorisation permitting the individual to perform the relevant work or provide the relevant training;

(b) the work or training is authorised by a written agreement to which the Commonwealth is a party;

(c) the work or training is solely in the course of, and as part of, the individual's service with any armed force and a declaration is in force on the basis that it is in the interests of the defence or international relations of Australia to permit that service;

(d) the work or training is part of the individual's employment or engagement by the Commonwealth;

(e) the work or training is solely or primarily for the purpose of providing aid of a humanitarian nature or performing an official duty for the United Nations or International Committee of the Red Cross.[16]

1.5 An individual may apply to the minister for authorisation to perform work or provide training and the minister may grant or refuse such authorisation, having regard to the kind of work performed by the person, and the kind of information accessed by the person while a defence staff member, as well as the kind of work or training to be performed. The minister must refuse to grant an authorisation if the minister reasonably believes that the work or training would prejudice the security,

---

13 Schedule 1, item 1, proposed section 113 definition of 'defence staff member' and proposed section 114. See also the Administrative Arrangements Order made 13 October 2022 which states that the Department of Defence is the department that administers the *Defence Act 1903*.

14 Schedule 1, item 1, proposed section 115.

15 Schedule 1, item 1, proposed section 113 definition of 'relevant foreign country' and proposed subsection 115(3).

16 Schedule 1, item 1, proposed subsections 115A(2)–(6) and 115B(2)–(6).

defence or international relations of Australia.[17] In granting an authorisation the minister may do so subject to any specified conditions (failure to comply with a condition would be an offence).[18] The minister would be empowered to cancel, suspend or vary an authorisation in a variety of circumstances.[19]

International human rights legal advice

Rights to private life and work

1.6 Limiting when particular persons may take up certain jobs engages and limits the rights to work and to a private life. The right to work provides that everyone must be able to freely accept or choose their work, and includes a right not to be unfairly deprived of work.[20] The right to privacy prohibits arbitrary and unlawful interferences with an individual's privacy, family, correspondence or home.[21] A private life is linked to notions of personal autonomy and human dignity. It includes the idea that individuals should have an area of autonomous development; a 'private sphere' free from government intervention and excessive unsolicited intervention by others.

1.7 These rights may be permissibly limited where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

1.8 The statement of compatibility recognises that these rights are limited by this bill. With respect to limiting when former defence workers may undertake particular work, it states that many former defence staff members have specialist skills and knowledge of defence secrets, particularly in relation to sensitive defence capability, personnel and operations.[22] It states that permitting these former members to perform work for, or on behalf of, foreign military organisations or foreign government bodies, without any oversight or restriction, could significantly undermine the interests of Australia and Australia's allies, and damage Australia's security, defence and international relations. With respect to limiting when any Australian citizen or permanent resident may provide certain training to, or on behalf of, a military organisation or government body of a certain foreign country, the statement of compatibility states that, with respect to training related to certain goods, software and technology the gravity of the threat posed by the relevant goods demonstrates a

---

17 Schedule 1, item 1, proposed section 115C.

18 Schedule 1, item 1, proposed subsection 115C(12) and section 115D.

19 Schedule 1, item 1, proposed sections 115E, 115F, 115G and 115H.

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

21 International Covenant on Civil and Political Rights, article 17. See also, UN Human Rights Committee, *General Comment No. 16: Article 17* (1988) [3]–[4].

22 Statement of compatibility, p. 46.

need to deter and prevent the performance of such training without regulation.[23] Seeking to prevent harm to Australia's national interests, security and defence would constitute a legitimate objective for the purposes of international human rights law, and the measure appears to be rationally connected to (that is, effective to achieve) that objective.

1.9 A key aspect of whether a limitation on a right can be justified is whether the limitation is proportionate to the objective being sought. In this respect, it is necessary to consider a number of factors, including whether a proposed limitation is sufficiently circumscribed; whether it is accompanied by sufficient safeguards; and whether any less rights restrictive alternatives could achieve the same stated objective. The statement of compatibility provides limited information in this regard, stating only that the bill aims to 'administer the least restrictive alternatives by balancing the right of every person to gain a living by work which they freely choose or accept, while promoting the general welfare, security, defence and international relations of Australia'.[24]

1.10 As to whether the measure is sufficiently circumscribed, some questions arise, largely because it is proposed that significant elements of the bill would be dealt with by delegated legislation. For example, the term 'foreign work restricted individual' (in relation to whom the proposed offence in section 115A would apply) would refer to someone who was previously a 'defence staff member', but they would not be considered such a person if they were included in a class of persons specified in a legislative instrument.[25] As the term 'defence staff member' would include all members of the defence force and all employees of the Department of Defence unless a legislative instrument limited the application of the offence, this could potentially capture a large number of people such that the potential interference with rights could be significant. Equally, however, if only narrow classes of persons were ultimately covered by the offence provisions (for example, if the legislative instrument specified a broad class of persons who would not be captured by the definition), the measure may be sufficiently constrained. Further, the bill would operate with respect to work and training in 'relevant foreign countries', meaning a country *other than* one specified by legislative instrument.[26] That is, the bill would apply to relevant work or training with respect to every country other than Australia unless a country was specified by legislative instrument and thereby excluded from the operation of this measure.

---

23 Statement of compatibility, p. 47.

24 Statement of compatibility, p. 46.

25 Schedule 1, item 1, proposed sections 114 and 115.

26 Schedule 1, item 1, proposed section 113.

Depending on the number of countries set out by legislative instrument, this element of the measure could either constrain it or facilitate its broad application.[27]

1.11 As to whether the bill is accompanied by sufficient safeguards, the bill would enable foreign work restricted individuals to apply for a foreign work authorisation, and provide for external review of decisions to refuse an authorisation. This would serve as an important safeguard. However, it is noted that proposed section 115E provides that the minister would have a broad discretion to cancel a foreign work authorisation, including the power to do so where they are satisfied that 'it would be appropriate in all the circumstances', and no explanation is provided as to the necessity of this broad discretionary power. With respect to the right to privacy, the statement of compatibility notes that the powers and functions of the bill would be subject to the operation of the *Privacy Act 1988*,[28] which would likely serve as a safeguard.

1.12 Lastly, some questions arise as to whether less rights restrictive alternatives would not be as effective to achieve the objective of the measure. For example, no information is provided as to why the definition of 'defence staff member' is not defined more narrowly in the bill, or why the bill does not provide that the measure only operates with respect to foreign countries that are specified by delegated legislation.

1.13 As such, there is a risk that this measure may not constitute a proportionate limit on the rights to work and to privacy. However, much would depend on matters specified by delegated legislation made pursuant to the bill. Until such legislative instruments are made, specifying the countries and classes of workers to whom these offences would not apply, it is difficult to assess proportionality.

Committee view

1.14 The committee notes that creating two new offences relating to where a former defence staff member, or an Australian citizen or permanent resident, performs certain work or training for a foreign country without a foreign work authorisation engages and limits the right to work and to a private life.

1.15 The committee considers this measure seeks to achieve the legitimate objective of seeking to prevent harm to Australia's national interests, security and defence. The committee considers that the bill sets out a number of safeguards, enabling work or training to be undertaken if authorisation is provided, and applying procedural and review rights to such a decision. However, the committee considers that, as the bill

---

27 Further, with respect to the proposed offence in proposed section 115B (offence of an Australian citizen or permanent resident providing training to a foreign government), neither the bill nor the explanatory materials define or further explain the meaning of the term 'military tactics, military techniques or military procedures', meaning its breadth is not immediately clear.

28 Statement of compatibility, p. 45.

proposes that several key matters would be set out by delegated legislation, it is not clear whether, in practice, the proposed offences would constitute a proportionate limit on these rights, as much would depend on the matters set out by delegated legislation. If such delegated legislation were made, the committee would scrutinise it for compatibility with human rights in the normal course. In this regard, the committee considers that some minor amendments, which would not frustrate the intention of the bill, may assist the proportionality of the bill.

Suggested action

1.16 The committee considers the proportionality of this measure may be assisted were the bill amended to:

(a) define 'defence staff member' by reference to a specific group of jobs/skillset; and

(b) provide that instead of the offence applying to work or training in all foreign countries, it would only apply to work or training conducted for a 'relevant foreign country', as being one specified by legislative instrument.

1.17 The committee recommends that the statement of compatibility be updated to provide a more fulsome assessment of the engagement of the rights to work and to privacy.

1.18 The committee draws its comments to the attention of the minister and the Parliament.

Identity Verification Services Bill 2023

Identity Verification Services (Consequential Amendments) Bill 2023[29]

Purpose	The Identity Verification Services Bill 2023 seeks to authorise the relevant department to develop, operate and maintain approved identity verification facilities and collect, use and disclose identification information. The bill also provides for when protected information would be permitted to be recorded, disclosed and accessed. The Identity Verification Services (Consequential Amendments) Bill 2023 seeks to amend the *Australian Passports Act 2005* to authorise the minister to disclose personal information to specified persons for the purpose of participating in the Document Verification Service, the Face Verification Service or any other service determined by the minister.
Portfolio	Attorney-General
Introduced	House of Representatives, 13 September 2023
Rights	Effective remedy; equality and non-discrimination; privacy; social security

Background

1.19 The Parliamentary Joint Committee on Human Rights has previously commented on similar measures to those proposed by these bills. In 2017, the committee examined the instrument providing legislative authority for the government to fund the National Facial Biometric Matching Capability (the Capability).[30] The Capability facilitated the sharing and matching of facial images as well as biometric information between agencies through a central interoperability hub and the National Driver Licence Facial Recognition Solution (the Driver Licence database). In relation to this measure, the committee concluded that there was a risk of incompatibility with the right to privacy through the use of the existing laws as a basis for authorising the collection, use, disclosure and retention of facial images. The committee stated that setting funding for the Capability without new primary

[29] This entry can be cited as: Parliamentary Joint Committee on Human Rights, Identity Verification Services Bill 2023 and Identity Verification Services (Consequential Amendments) Bill 2023, *Report 11 of 2023*; [2023] AUPJCHR 106.

[30] Parliamentary Joint Committee on Human Rights, Financial Framework (Supplementary Powers) Amendment (Attorney-General's Portfolio Measures No. 2) Regulations 2017, *Report 9 of 2017* (5 September 2017) pp. 25–27; *Report 11 of 2017* (17 October 2017) pp. 84–91.

legislation to circumscribe the Capability's operation raises serious concerns as to the adequacy of safeguards to ensure that the measure is a proportionate limitation on the right to privacy.[31]

1.20 In 2018, the committee examined the Identity-matching Services Bill 2018 and Australian Passports Amendment (Identity-matching Services) Bill 2018, both of which lapsed at the dissolution of Parliament in 2019.[32] The Identity-matching Services Bill 2018 sought to authorise the Department of Home Affairs to develop, operate and maintain the central interoperability hub (interoperability hub) and the Driver Licence database, and collect, use and disclose identification information about an individual if it occurred through the interoperability hub or the Driver Licence database and was for a range of specified purposes. The Australian Passports Amendment (Identity-matching Services) Bill 2018 sought to authorise the Department of Foreign Affairs and Trade to participate in a specified service to share and match information relating to the identity of a person, and use computer programs to make decisions or exercise powers under the *Australian Passports Act 2005*. The committee concluded that there may be a risk of incompatibility with the right to privacy if the interoperability hub facilitates the sharing of information where the authorisation for an agency to collect, use, share, or retain facial images or biographic information is not sufficiently circumscribed. The committee reiterated its comments when the bills were reintroduced in the subsequent Parliament in 2019.[33]

1.21 It is noted that the identity verification facilities and services (described below in paragraphs [1.22] to [1.28]) to which these bills relate are already operating. They are currently governed by the Intergovernmental Agreement on Identity Matching Services as well as state and territory laws and other policies and procedures.[34] For example, in 2022, the Document Verification Service was used over 140 million times by approximately 2,700 government and industry sector organisations, and there were approximately 2.6 million Face Verification Service transactions in the 2022–23

---

31 Parliamentary Joint Committee on Human Rights, *Report 11 of 2017* (17 October 2017) p. 91.

32 Parliamentary Joint Committee on Human Rights, *Report 3 of 2018* (27 March 2018), pp. 41–51; *Report 5 of 2018* (19 June 2018), pp. 109–143.

33 Parliamentary Joint Committee on Human Rights, *Report 4 of 2019* (10 September 2019), p. 10.

34 See *Intergovernmental Agreement on Identity Matching Services* (2017). This Agreement is between the Commonwealth and states and territories and is intended to 'promote the sharing and matching of identity information to prevent identity crime, support law enforcement, uphold national security, promote road safety, enhance community safety and improve service delivery, while maintaining robust privacy and security safeguards', p. 2. Part 4 of the Agreement relates to identification services, including the DVS, FVS and FIS. Part 6 relates to the systems supporting these services, including the DVS Hub, interoperability Hub (supports the FVS and FIS) and Driver Licence database. Parts 7 and 8 of the Agreement relate to the supporting agreements and legislative framework governing the services and systems. See also *Identity Matching Services – what are they?*.

financial year.[35] This bill seeks to provide a legislative framework to support the continued operation of these identity verification services.[36]

Identity verification facilities and services

1.22 The Identity Verification Services Bill 2023 seeks to authorise the Attorney-General's Department (the department) to develop, operate and maintain three approved identity verification facilities – namely, the DVS hub, the Face Matching Service hub and the Driver Licence database.[37] In developing, operating and maintaining a verification facility, the department would be required to maintain the security of electronic communications to and from the facility, including by encrypting the information, and protecting the information from unauthorised interference or unauthorised access.[38] These identity verification facilities and associated services are detailed below.

1.23 The DVS hub and Face Matching Service hub are defined as facilities that relay electronic communications between persons and bodies for the purposes of requesting and providing identity verification services, which include the Document Verification Service[39] and Face Verification Service,[40] which are 1:1 matching services, and the Face Identification Service, which is a 1:many matching service.[41] These hubs would essentially operate as routers by which parties may request identification services, via the department, from the relevant agency holding the data, and responses to these requests are returned through the relevant hub.[42] Each identity verification service is explained in turn.

1.24 In general terms, the Document Verification Service is a 1:1 matching service that verifies biographical information (such as a name or date of birth but not a facial image or biometric information) contained in a specimen document against information contained in Document Verification Service documents, which are government issued identity documents (such as a birth certificate, driver's licence or

---

35 Explanatory memorandum, p. 3; second reading speech, p. 1.

36 Explanatory memorandum, p. 3.

37 Identity Verification Services Bill 2023, subclause 3(a), clauses 23–25. Note the acronym 'NDLFRS' is used in the bill, being short for the National Driver Licence Facial Recognition Solution, a term used in the intergovernmental agreement, see clause 5.

38 Identity Verification Services Bill 2023, clause 25.

39 Note that the Identity Verification Services Bill 2023 refers to 'DVS' which is short for Document Verification Service, see clause 15.

40 Note that the Identity Verification Services Bill 2023 refers to 'FVS' which is short for Face Verification Service, see clause 19.

41 Identity Verification Services Bill 2023, clause 5.

42 Explanatory memorandum, [115] and [119].

passport).[43] The purpose of comparing information in a specimen document against information in such a document must be to help determine whether the specimen document is the same as a Document Verification Service document held in the of the kind identified in the request.[44] The comparison must be carried out in accordance with the conditions and any limitations provided for under the participation agreement (see below at paragraph [1.27]).[45] For example, as part of its standard customer identification procedures, a bank may make a request to verify a customer's driver's licence. In the request form, the bank would include information obtained from the customer's driver's licence, such as the name and date of birth of the customer, and the type of document, namely a driver's licence. The request would be communicated electronically through the DVS hub to the data hosting agency, which would be the relevant state or territory road authority that issued the customer's driver's licence. The information provided on the request form would be compared against the identification information held on the relevant agency's database and the bank would receive a response that the information was either a 'match' or 'no match'.[46]

1.25 The Face Verification Service is a 1:1 matching service that verifies the identity of a person by comparing face-matching service information relating to an individual against face-matching service information that is contained in a government identification document (which is provided by a government authority for the purpose of the comparison and the authority is a party to a participation agreement).[47] Face-matching service information includes: an individual's name, address, place or date of birth, age, sex, gender identity or intersex status; a facial image[48] of an individual or a biometric template derived from such an image;[49] information about the outcome of a biometric comparison or comparison involving an Face Verification Service request; and any information contained in certain government documents such as a driver's

---

43 Identity Verification Services Bill 2023, clause 15 sets out the criteria that must be met in order for a service to be defined as a DVS, clause 5 defines DVS document and clause 6 defines DVS information.

44 Identity Verification Services Bill 2023, paragraph 15(1)(f).

45 Identity Verification Services Bill 2023, paragraph 15(1)(e).

46 Explanatory memorandum, pp. 38–39.

47 Identity Verification Services Bill 2023, clauses 19 and 20.

48 Identity Verification Services Bill 2023, clause 5 defines 'facial image' as 'a digital still image of an individual's face (whether or not including the shoulders)'.

49 A biometric comparison involves accessing facial images to create biometric templates, which are a mathematical representation of a facial image that cannot be used to recreate the facial image. A biometric template is a type of face-matching service information that is used by the Face Verification Service and the Face Identification Service. Facial images in the Driver Licence database repository may be used to create biometric templates. See explanatory memorandum, [131].

licence or passport.[50] The comparison involved in the Face Verification Service must be for the purpose of verifying an individual's identity or protecting an individual who is a shielded person or someone else associated with a shielded person.[51] A shielded person is a person who has acquired or used, or is authorised to acquire or use, an assumed identity (for example an undercover police officer); a person to whom a witness identity protection certificate has been given; a participant or former participant of a witness protection program; or a person involved in administering a witness protection program.[52]

1.26 The Face Identification Service is a 1:many matching service that may only be used by certain Commonwealth, state or territory government authorities, including law enforcement and intelligence officers, for the purpose of protecting the identity of a shielded person or someone else associated with a shielded person.[53] It involves an electronic comparison of a single facial image of an individual and any other face-matching service information against face-matching service information that is contained in a government identification document (which is provided by a government authority for the purpose of the comparison and the authority is a party to a participation agreement).[54]

1.27 Parties requesting any of these three identification verification services as well as government authorities providing identification information used for comparison must be a party to a participation agreement with the department.[55] Among other things, a participation agreement must provide for privacy impact assessments of requesting identity verification services; the obtaining of an individual's consent to the collection, use and disclosure of identification information (unless certain exceptions apply); arrangements for dealing with complaints; reporting procedures in relation to data breaches; and the prohibition of unauthorised disclosure of identification information.[56] If parties do not comply with the agreement or access policy for the relevant identification verification service, their ability to request the service may be

---

50 Identity Verification Services Bill 2023, subclause 6(2). Subclause (4) specifies what is *not* face-matching service information, including health or genetic information, and information or an opinion that relates to the individual's racial or ethnic origin, political opinions, membership of a political association or trade union, religious or philosophical beliefs, sexual orientation or practices, and criminal record.

51 Identity Verification Services Bill 2023, subclause 20(3).

52 Identity Verification Services Bill 2023, clause 5.

53 Identity Verification Services Bill 2023, clauses 16, 17 and 18.

54 Identity Verification Services Bill 2023, clause 18.

55 Identity Verification Services Bill 2023, paragraph 15(1)(b). Clause 8 defines a participation agreement, which is a written agreement between the Department (AGD) and other parties that deals with the requesting and provision of identity verification services and meets the requirements in clauses 9–12, which relate to privacy obligations of parties to a participation agreement; limiting the use of identification information; and compliance requirements.

56 Identity Verification Services Bill 2023, clauses 9 and 10.

suspended or terminated.[57] Participation agreements must be published on the department's website (excluding any parts of the document that would create a risk to the security of identification information, an identification verification facility or Australia's national security, or unreasonably disclose an individual's personal information).[58]

1.28 The Driver Licence database is a database of identification information as well as a system for biometric comparison of facial images.[59] The information held in the database includes information contained in government identification documents issued by state or territory authorities (such as driver's licences) as well as information supplied by authorities to the department for inclusion in the database.[60] The Driver Licence database can access facial images obtained from individuals' driver's licences, which are stored in a central electronic repository, to create biometric templates that are used for biometric comparison.[61] Hosting agreements govern the Driver Licence database and the collection, use and disclosure of identification information in the database.[62] A hosting agreement is an agreement between the department and each state or territory authority that supplies identification information to the department for inclusion in the database.[63] The bill sets out the minimum privacy obligations and requirements that are to be included in an agreement, such as requirements relating to compliance with privacy laws, data breaches and dealing with complaints.[64] The hosting agreement must be published on the department's website (excluding any parts of the document that would create a risk to the security of identification information, an identification verification facility or Australia's national security, or unreasonably disclose an individual's personal information).[65]

1.29 In addition, the Identity Verification Services Bill 2023 would authorise the department to collect, use and disclose identification information electronically communicated to an approved identity verification facility, or generated using the Driver Licence database for specified purposes.[66] These purposes include verifying the identity of an individual using a Document Verification Service or Face Verification Service; protecting a shielded person or someone else associated with a shielded person using a Face Verification Service or Face Identification Service; developing

---

57 Identity Verification Services Bill 2023, subclause 12(c).

58 Identity Verification Services Bill 2023, subclauses 39(1) and (2).

59 Explanatory memorandum, [130]–[131]. See also *Identity Matching Services – what are they?*.

60 Identity Verification Services Bill 2023, clause 5.

61 Explanatory memorandum, [131].

62 Identity Verification Services Bill 2023, clause 13.

63 Identity Verification Services Bill 2023, subclause 13(1).

64 Identity Verification Services Bill 2023, subclauses 13(2)–(6).

65 Identity Verification Services Bill 2023, subclauses 39(1) and (2).

66 Identity Verification Services Bill 2023, subclause 3(b), clauses 26–28.

identity verification services or supporting facilities; or developing, operating or maintaining the Driver Licence database.[67]

1.30 The bill also sets out when protected information can be recorded, disclosed or accessed by entrusted persons.[68] Protected information includes electronic communications to or from an approved identity verification facility or the Driver Licence database, or information about the making, content or addressing of communications to or from a facility; information relating to a particular individual held in, or generated using, the Driver Licence database; and information that enables access to an identity verification facility.[69] An entrusted person includes the Secretary and APS employees of the department; officers or employees of a Commonwealth, state or territory government authority; officers or employees of an authority of a foreign country or public international organisation; or contractors engaged in services relating to an approved identity verification facility.[70] An entrusted person would commit an offence if they accessed protected information or obtained protected information in their capacity as an entrusted person and made a record of or disclosed the information to another person, unless the conduct was authorised by law or in compliance with a requirement under law.[71] Other circumstances in which an entrusted person would be authorised to make a record of, disclose or access protected information include in the course of exercising powers, or performing functions or duties, as an entrusted person; for the purpose of lessening or preventing a serious and imminent threat to life or health; for the purpose of an official from the Inspector-General of Intelligence and Security (IGIS) or an Ombudsman official exercising a power, or performing a function or duty; and with the consent of the person to whom the protected information relates or with the consent of the state or territory authority responsible for the Driver Licence database protected information.[72]

1.31 The Identity Verification Services (Consequential Amendments) Bill 2023 seeks to amend the *Australian Passports Act 2005* to authorise the minister to disclose personal information for the purpose of participating in the Document Verification Service, Face Verification Service or any other service specified in a minister's determination, to share or match information relating to the identity of a person.[73]

---

67 Identity Verification Services Bill 2023, subclause 27(2).

68 Identity Verification Services Bill 2023, clauses 29–35.

69 Identity Verification Services Bill 2023, subclause 30(4).

70 Identity Verification Services Bill 2023, subclause 30(4).

71 Identity Verification Services Bill 2023, subclauses 20(1)–(3).

72 Identity Verification Services Bill 2023, clauses 31–35.

73 Identity Verification Services (Consequential Amendments) Bill 2023, item 3.

The bill would also permit the automated disclosure of personal information to a person participating in the such services.[74]

Preliminary international human rights legal advice

Rights to an effective remedy; equality and non-discrimination; privacy; social security

Right to privacy

1.32 The bills engage and limit the right to privacy in a number of ways, including by authorising:

- the department to develop, operate and maintain the identity verification facilities, which support the operation of the identity verification services, and collect, use and disclose identification information;
- entrusted persons to make a record of, disclose and access protected information (which includes personal information) in certain circumstances; and
- the minister to disclose personal information for the purpose of the verification services as well as the automated disclosure of personal information for these purposes.[75]

1.33 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.[76] The type of information protected includes substantive information contained in communications as well as metadata.[77] The United Nations (UN) High Commissioner for Human Rights has stated that the generation and collection of data relating to a person's identity, family or life as well as the examination or use of that information interferes with the right to privacy, as the individual loses some control over information that could put his or her privacy at risk.[78] Indeed, 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 data from various sources.[79] The UN High Commissioner for Human Rights has also

---

74 Identity Verification Services (Consequential Amendments) Bill 2023, item 6.

75 Statement of compatibility, pp. 8 and 16.

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

77 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [6].

78 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [7].

79 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [13].

noted that the sharing of data with third parties as well as the long-term storage of personal data often amounts to further privacy intrusions and has other adverse human rights impacts, many of which may not have been envisaged at the time of data collection.[80] Additionally, biased or erroneous data can 'contribute to other human rights violations in a multitude of ways, for example, by erroneously flagging an individual as a likely terrorist or as having committed welfare fraud'.[81] The UN High Commissioner for Human Rights has raised particular concerns with 'biased data sets that lead to discriminatory decisions based on AI systems'.[82]

1.34 In the context of biometric data, such as facial geometry, the UN High Commissioner for Human Rights has observed the increasing trend of countries creating immense centralised databases storing information for a diverse range of purposes, including criminal investigation or identification of individuals for the purposes of providing essential services such as social security.[83] It stated:

> The creation of mass databases of biometric data raises significant human rights concerns. Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular

---

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

81 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [19].

82 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [19].

83 For a discussion on the use of automated facial recognition technology in Australia and the consequent human rights concerns, see Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight', *UNSW Law Journal*, vol 40, no. 1, 2–17, pp. 121–145. At pp. 122–123, Mann and Smith state that automated facial recognition technology, which involves the automated extraction, digitisation and comparison of the spatial and geometric distribution of facial features and the storage of facial templates in a database, is a significant development because it 'extends privacy considerations beyond the mere capture of photographs' and 'involves the emergence of a "surveillant assemblage" to create a "data double" enabling automated sorting, database storage, information sharing and integration'.

attention should be paid to questions of necessity and proportionality in the collection of biometric data.[84]

Right to social security

1.35 To the extent that the measures facilitate the use of biometric identity verification for the purposes of accessing social security and other government services, the measures would also engage the right to social security. The statement of compatibility states that the provision of welfare payments and other benefits are contingent on identity verification in order to ensure welfare is provided to the correct people and to prevent fraud and misuse of government funds. It states that in making identity verification more accessible, the measures will reduce the administrative burden on those seeking services; support the fast, secure and private provision of such services; and have a positive impact on the right to social security.[85] The explanatory materials note that biometric verification is a highly secure way of verifying identity and is currently required to create a 'strong' MyGovID which is needed to access certain Centrelink and Australian Tax Office services.[86] If the identity verification services improved the efficiency of government services and the provision of social security, the measures may facilitate the realisation of the right to social security.

1.36 However, imposing biometric identification requirements on recipients of social security benefits may also limit the right to social security to the extent that it would restrict access to social security for those individuals that are unable to complete the verification process (for example, because they do not have the required government identification documents or they do not consent to the verification service).

1.37 The right to social security encompasses the right to access and maintain benefits on a non-discriminatory basis in order to secure protection from various social risks and contingencies, such as lack of income due to disability, old age or

---

84 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [14]. The UN High Commissioner for Human Rights raised similar concerns in its 2021 report, with a particular emphasis on remote biometric recognition. It stated, '[r]emote biometric recognition is linked to deep interference with the right to privacy. A person's biometric information constitutes one of the key attributes of her or his personality as it reveals unique characteristics distinguishing her or him from other persons. Moreover, remote biometric recognition dramatically increases the ability of State authorities to systematically identify and track individuals in public spaces, undermining the ability of people to go about their lives unobserved and resulting in a direct negative effect on the exercise of the rights to freedom of expression, of peaceful assembly and of association, as well as freedom of movement': *The right to privacy in the digital age*, A/HRC/48/31 (2021) [27].

85 Statement of compatibility, pp. 15, 17–18.

86 Explanatory memorandum, p. 61; statement of compatibility, p. 7.

unemployment, insufficient family support or unaffordable health care.[87] The right to social security recognises the importance of adequate social benefits in reducing the effects of poverty and plays an important role in realising many other economic, social and cultural rights, in particular the right to an adequate standard of living and the right to health.[88] Key elements of the right to social security include availability, adequacy and accessibility.[89] Regarding the latter, the UN Committee on Economic, Social and Cultural Rights has stated that '[q]ualifying conditions for benefits must be reasonable, proportionate and transparent' and social security beneficiaries 'must be able to participate in the administration of the social security system' and have 'physical access to the social security services in order to access benefits and information'.[90]

1.38 More generally, the UN High Commissioner for Human Rights has emphasised that the 'digitization of welfare systems, despite its potential to improve efficiency, risks excluding the people who are most in need'.[91] It notes that digital welfare systems and data-matching are increasingly being used by states 'to expose, survey and punish welfare beneficiaries and conditions are imposed on beneficiaries that undermine individual autonomy and choice'.[92] The Special Rapporteur on extreme poverty and human rights has observed that while digitising identity verification processes has potential benefits, such as improving the efficiency and service delivery of social security systems, there are also risks, particularly with respect to the right to privacy.[93] In particular, there is a 'real risk of beneficiaries being effectively forced to give up their right to privacy and data protection to receive their right to social security, as well as other social rights'.[94]

1.39 Under international human rights law, Australia has obligations to progressively realise the right to social security using the maximum of resources available. Australia

---

87 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The right to social security (art. 9)* (2008) [2].

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

89 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The right to social security (art. 9)* (2008) [10]–[27].

90 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The right to social security (art. 9)* (2008) [24], [26] and [27].

91 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [4].

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

93 UN Human Rights Council, *Report of the Special Rapporteur on extreme poverty and human rights*, A/74/493 (2019) [11]–[17].

94 UN Human Rights Council, *Report of the Special Rapporteur on extreme poverty and human rights*, A/74/493 (2019) [64].

has a corresponding duty to refrain from taking retrogressive measures, or backwards steps, in relation to the realisation of this right. The imposition of a different or additional eligibility condition for social security benefits, such as requirements for biometric verification, may constitute a retrogressive measure if it were to amount to an unreasonable restriction on the right to access social security.

Right to equality and non-discrimination

1.40 In addition, the measures may engage the right to equality and non-discrimination. The statement of compatibility states that the bills promote the right to equality and non-discrimination by providing for the Driver Licence database.[95] It notes that the Driver Licence database supports the continued operation of the Face Verification Service as it provides the technical capability for biometric matching to occur against credentials obtained from state and territory data. The statement of compatibility explains that the Driver Licence database will enable individuals to verify their identity against information contained in their driver's licence in order to establish a 'strong' MyGovID.[96] It notes that without the Driver Licence database, only persons with an Australian passport, which accounts for 50 per cent of the population, would be able to create a 'strong' MyGovID and access critical services (whereas 80 per cent of Australians have a driver's licence).[97] In this way, the Driver Licence database would allow for a broader range of persons to verify their identity through the identity verification services.[98]

1.41 However, the statement of compatibility does not acknowledge that the measures may also limit the right to equality and non-discrimination in a number of ways. Large datasets, such as the Driver Licence database risk limiting the right to equality and non-discrimination to the extent that biased or erroneous data leads to discriminatory decisions and has a disproportionate impact on members of certain groups.[99] The right to equality and non-discrimination provides that everyone is entitled to enjoy their rights without discrimination of any kind and that all people are equal before the law and entitled without discrimination to equal and non-discriminatory protection of the law.[100] The right to equality encompasses both 'direct' discrimination (where measures have a discriminatory intent) and 'indirect' discrimination (where measures have a discriminatory effect on the enjoyment of

95 Statement of compatibility, p. 7.

96 Statement of compatibility, p. 7.

97 Statement of compatibility, p. 7.

98 Statement of compatibility, p. 7.

99 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [19], [26].

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

rights).[101] Indirect discrimination occurs where 'a rule or measure that is neutral at face value or without intent to discriminate' exclusively or disproportionately affects people with a particular protected attribute.[102]

1.42 The UN High Commissioner for Human Rights has observed that 'facial recognition technology can be used to profile individuals on the basis of their ethnicity, race, national origin, gender and other characteristics'.[103] With respect to the measures in the bills, while certain information is excluded from identity verification services, such as a person's racial or ethnic origin, such information may be inferred from other information communicated to a service or generated using the Driver Licence database (for example, an individual's gender or racial or ethnic origin may be inferred from their name and facial image).[104] This leaves open a risk that information held in or generated using this database could lead to decisions that have a discriminatory impact on members of certain groups, noting that law enforcement may access this information to support investigations (with the consent of the relevant state or territory authority that supplied the information).[105] The UN Committee on the Elimination of Racial Discrimination has raised human rights concerns with respect to the increasing use of facial recognition and surveillance technologies by law enforcement to track and control specific demographic groups.[106] It has noted that identifying individuals based on their facial geometry could 'potentially profile people based on grounds of discrimination such as race, colour, national or ethnic origin or gender'.[107] It further noted that 'the accuracy of facial recognition technology may differ depending on the colour, ethnicity or gender of the persons assessed, which may lead to discrimination'.[108]

---

101 UN Human Rights Committee, *General Comment 18: Non-discrimination* (1989).

102 Althammer v Austria, UN Human Rights Committee Communication no. 998/01 (2003) [10.2]. The prohibited grounds of discrimination are race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Under 'other status' the following have been held to qualify as prohibited grounds: age, nationality, marital status, disability, place of residence within a country and sexual orientation. The prohibited grounds of discrimination are often described as 'personal attributes'. See Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary*, 3rd edition, Oxford University Press, Oxford, 2013, [23.39].

103 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [26].

104 Identity Verification Services Bill 2023, subclause 6(4); statement of compatibility, p. 7

105 Identity Verification Services Bill 2023, clause 35; explanatory memorandum, [354].

106 UN Committee on the Elimination of Racial Discrimination, *General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials* (2020) [35].

107 UN Committee on the Elimination of Racial Discrimination, *General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials* (2020) [35].

108 UN Committee on the Elimination of Racial Discrimination, *General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials* (2020) [35].

1.43 Further, if it is more difficult to access the social security system and other government services for those individuals who are unable to complete biometric identity verification, the measures may have a disproportionate impact on persons who do not have access to government identification documents. Such persons may include Aboriginal and Torres Strait Islander peoples, particularly those who do not have a birth certificate and those living in remote communities; victim-survivors of domestic or family violence; people experiencing homelessness; recently released prisoners; people with disability; undocumented migrant workers; and refugees and asylum seekers.[109] Noting that those persons who may experience difficulties in verifying their identity are likely to be persons with a particular protected attribute, such as race, national origin and/or disability, the measures could have a disproportionate impact on persons or groups with certain protected attributes.[110] Where a measure impacts on a particular group disproportionately it establishes prima facie that there may be indirect discrimination.[111]

Right to an effective remedy

1.44 Further, if the measures impermissibly limited one or more of the above rights, it is not clear whether an individual would have access to an effective remedy with respect to any violation of rights. The right to an effective remedy requires the availability of a remedy which is effective with respect to any violation of rights and freedoms recognised by the covenant.[112] 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. In the context of violations of the right to privacy, possible remedies include judicial and non-judicial state-based grievance mechanisms, such as access to independent authorities with powers to monitor state and private sector data privacy practices, such as privacy and

---

109 Department of Social Services, *Social Security Guide (Version 1.281)*, 'Persons experiencing difficulty with identity confirmation and verification' (April 2021) [2.2.1.40]

110 See Parliamentary Joint Committee on Human Rights, Telecommunications Regulations 2021 [L2021L00289], *Report 6 of 2021* (13 May 2021) pp. 11–20. This instrument required all customers to provide documentary evidence verifying their identity. The committee raised concerns that the measure may disproportionately impact on certain groups, such as those who may be homeless, experiencing domestic violence, Aboriginal or Torres Strait Islander peoples, undocumented migrant workers and refugees and asylum seekers.

111 *D.H. and Others v the Czech Republic*, European Court of Human Rights (Grand Chamber), Application no. 57325/00 (2007) [49]; *Hoogendijk v the Netherlands*, European Court of Human Rights, Application no. 58641/00 (2005).

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

data protection bodies.[113] The UN High Commissioner for Human Rights has emphasised that to be effective, any non-judicial mechanism 'should be legitimate, accessible, predictable, equitable, rights-compatible, transparent, a source of continuous learning and, for operational level grievance mechanisms, based on dialogue and engagement'.[114]

Limitation analysis

1.45 The rights to privacy, social security and equality and non-discrimination may generally 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. With respect to the right to an effective remedy, while limitations may be placed in particular circumstances on the nature of the remedy provided (judicial or otherwise), state parties must comply with the fundamental obligation to provide a remedy that is effective.[115] As there are common concerns underlying each of the measures in the bills and the measures interact with one another the measures will be analysed collectively in this report.

1.46 The statement of compatibility states that the bills provide a legislative framework to support the continued operation of the identity verification services.[116] It states that these services are the only national capability that can be used by industry and government agencies to securely verify the identity of individuals.[117] It notes that secure and efficient identity verification is critical to preventing identity fraud and theft, preventing fraud and misuse of government funds in the context of the social security system, and protecting industry, governments and the wider Australian community when engaging with the digital economy.[118] With respect to the Document Verification Service and Face Verification Service, the statement of compatibility states that the services will enable individuals to securely access government and industry services without exposing themselves to identity fraud and theft.[119] It notes that the measures will reduce the administrative burden on those seeking services, including social security services, and support the fast, secure and private provision of such services.[120] The statement of compatibility states that the Face Identification Service will protect the identity of shielded persons and support

---

113 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [50].

114 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [51].

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

116 Statement of compatibility, pp. 6 and 15.

117 Statement of compatibility, p. 6.

118 Statement of compatibility, pp. 6 and 15.

119 Statement of compatibility, p. 8.

120 Statement of compatibility, p. 15.

agencies to identify whether the identity of an undercover officer could be compromised by a criminal organisation.[121] With respect to the Driver Licence database, the explanatory statement notes that its primary purpose is to create an electronic centralised repository of state and territory driver's licence information, enabling access to facial images and the creation of biometric templates that are used for biometric comparison.[122]

1.47 The general objectives of preventing identity fraud and theft; facilitating the fast, secure and private provision of government services; and protecting the identity and safety of shielded persons and undercover officers, are capable of constituting legitimate objectives for the purposes of international human rights law. As to the necessity of the measures, it is noted that the Parliamentary Joint Committee on Human Rights has previously raised concerns regarding the absence of a federal legislative framework governing the identity verification services.[123] Thus, despite the fact that the services are already operating, insofar as the bills provide a federal legislative framework to support the operation of the services, the measures appear to be necessary and address a legislative gap.[124]

1.48 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. The key question is whether the relevant measure is likely to be effective in achieving the objective being sought. The statement of compatibility states that by making identity verification more accessible, the measures will reduce the administrative burden on individuals, enable more Australians to access critical services online and facilitate the efficient provision of services.[125] It states that without the identity verification services, the privacy of individuals seeking to access government and industry online services may be compromised because there is no alternative national system to securely verify identity.[126]

1.49 The measures may be effective in facilitating the efficient provision of services, insofar as individuals may be able to verify their identity online and access services in a timely way. However, there is insufficient information in the explanatory materials to demonstrate how the measures would be effective in preventing identity theft and fraud, noting the risks of data breaches and misuse of information with respect to large

---

121 Statement of compatibility, p. 9.

122 Explanatory statement, p. 24.

123 Parliamentary Joint Committee on Human Rights, *Report 11 of 2017* (17 October 2017) p. 91.

124 The UN High Commissioner for Human Rights has emphasised the importance of ensuring 'that data-intensive systems, including those involving the collection and retention of biometric data, are only deployed when States can demonstrate that they are necessary and proportionate to achieve a legitimate aim': *The right to privacy in the digital age*, A/HRC/39/29 (2018) [61(c)].

125 Statement of compatibility, pp. 7 and 15.

126 Statement of compatibility, p. 8.

datasets. The Special Rapporteur on extreme poverty and human rights, for example, has raised concerns with the pooling of data from different government data sets for the purposes of cross-matching, data-sharing and cross-verification, stating:

> To the extent that assurances are given that leakage from one [government] silo to the next will not occur, such guarantees are largely illusory as a change of Government or a real or imagined emergency situation is all that is required to trigger a partial or comprehensive breaking down of the partitions, quite apart from the risks of electronic data breaches resulting from hacking or normal system breakdowns.[127]

1.50 It is also not clear whether the measures would be effective to prevent social security fraud and misuse of government funds. In this regard, the Special Rapporteur on extreme poverty and human rights has queried the effectiveness of digital technologies in preventing social security fraud, stating:

> fraud in the welfare state is often the result of confusion, complexity and the inability to correct the resulting errors. However, by deliberately using the power of new technologies to identify fraud or violations of "conditionalities" imposed on beneficiaries, Governments are likely to find inconsistencies that they can hold against claimants.…new abilities to collect information and store it digitally for an undefined period of time create a future in which a wealth of information can be held against someone indefinitely.[128]

1.51 Further information is therefore required to assess whether the measures would be effective to achieve some of the stated objectives.

1.52 A key aspect of whether a limitation on a right can be justified is whether the limitation is proportionate to the objective being sought. In this respect, it is necessary to consider a number of factors, including whether a proposed limitation is sufficiently circumscribed; whether it is accompanied by sufficient safeguards; and whether any less rights restrictive alternatives could achieve the same stated objective. With respect to the right to privacy, any limitation must also not render the essence of the right meaningless.[129]

1.53 In assessing whether the measures are sufficiently circumscribed, it is relevant to consider the breadth of the measures, including the scope of personal information and the purposes for which the information may be collected, stored, used and shared; the range of persons authorised to access the information; and the circumstances in

---

127 UN Human Rights Council, *Report of the Special Rapporteur on extreme poverty and human rights*, A/74/493 (2019) [69].

128 UN Human Rights Council, *Report of the Special Rapporteur on extreme poverty and human rights*, A/74/493 (2019) [64].

129 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [10]; UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [8].

which the right to privacy, in particular, may be limited. Regarding the latter, the UN Human Rights Committee has stated that legislation must specify in detail the precise circumstances in which interferences with privacy may be permitted.[130]

1.54 The scope of personal information that may be collected, used or disclosed by means of electronic communication to a facility or held in, or generated using, the Driver Licence database is extensive. It would include 'identification information', that is face-matching service information and Document Verification Service information (see paragraphs [1.24] and [1.25]), which includes an individual's name, address, place or date of birth, age, sex, gender identity or intersex status and facial image.[131] This type of information is particularly sensitive, not only because it includes facial images, which may be used to create biometric templates, but it involves the fusion of data from different sources. The UN High Commissioner for Human Rights has observed that a 'person's biometric information constitutes one of the key attributes of her or his personality as it reveals unique characteristics distinguishing her or him from other persons' and hence represents a 'deep interference with the right to privacy'.[132] Sensitive data should therefore 'enjoy a particularly high level of protection'.[133] As noted above (in paragraph [1.42]), while certain information is excluded from identity verification services (such as a person's racial or ethnic origin), which may assist with proportionality, such information may nonetheless be inferred from other identification information (for example, an individual's gender or racial or ethnic origin may be inferred from their name and facial image).[134]

1.55 The purposes for which the identity verification services may be used and personal information may be collected, stored, used and shared, are specified in the bill (as set out in paragraph [1.29]). Articulating the exact purposes for which information may be collected, used or disclosed in the text of the legislation assists with proportionality. In particular, the purpose for which the Face Identification Service may be used is restricted to protecting the identity of a shielded person or someone else associated with a shielded person.[135] However, other purposes for which information may be used are drafted in broad terms, such as to develop identity verification services or facilities and develop, operate or maintain the Driver Licence database. Further, there is a risk that information may be accessed, used and disclosed for purposes other than those for which the information was originally collected. For example, law enforcement agencies may use data held in or generated by the Driver

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

131 Identity Verification Services Bill 2023, clauses 27 and 30.

132 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [27].

133 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [29].

134 Identity Verification Services Bill 2023, subclause 6(4); statement of compatibility, p. 7

135 Identity Verification Services Bill 2023, clauses 16, 17 and 18.

Licence database to support investigations. While the state or territory authorities who supplied the information must consent to this use, there is no requirement that the individual to whom the information relates must provide consent. Thus, while information held in the database is collected for the purpose of identity verification, it may be used for other purposes, such as to support law enforcement investigations. The UN High Commissioner for Human Rights has cautioned that '[c]hanges 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'.[136]

1.56 The bills authorise various persons to access and disclose protected information in certain circumstances, including the department,[137] entrusted persons (which includes APS employees and contractors and employees of foreign governments and public international organisations)[138] and the minister.[139] Each identity verification service has different authorisations regarding who may access, use and disclose personal information. For example, both government and private sector organisations may use the Document Verification Service and Face Verification Service with the consent of the individual to whom the information relates. Whereas the Face Identification Service is restricted to officers from a limited group of government agencies. As to who the information may be disclosed to, some provisions specify the authorised recipient of the protected information. For example, entrusted persons may disclose protected information to an IGIS or Ombudsman official for the purpose of the official exercising a power, or performing a function or duty.[140] However, other provisions do not specify to whom information may be disclosed. For example, entrusted persons may generally disclose protected information for the purposes of the Act and in the course of exercising powers, functions or duties.[141] The department is authorised to use and disclose identification information, but it is not specified to whom the department may disclose the information.[142] Thus, questions arise as to the full range of persons who may access and use protected information.

1.57 As to the existence of safeguards, the measures contain a number of useful safeguards that are likely to assist with proportionality. A key safeguard is the requirement that all entities accessing identity verification services must be a party to a participation agreement (as discussed above in paragraph [1.27]). Participation

---

136 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [29].

137 Identity Verification Services Bill 2023, clauses 27 and 28.

138 Identity Verification Services Bill 2023, subclause 30(4).

139 Identity Verification Services (Consequential Amendments) Bill 2023, item 3.

140 Identity Verification Services Bill 2023, clauses 33 and 34.

141 Identity Verification Services Bill 2023, clause 31.

142 Identity Verification Services Bill 2023, clause 28.

agreements will themselves contain several safeguards, primarily with respect to the right to privacy, including:

- parties must be subject to and comply with privacy legislation, such as the *Privacy Act 1988* (Privacy Act) and the Australian Privacy Principles (APPs);
- a privacy impact assessment must be provided;
- an individual's consent must be obtained for the purposes of requesting identity verification services (unless the request is made by a government authority and the request is for the purposes of protecting a shielded person);
- individuals from whom such consent is sought must be provided with specified information, including how the information (including facial images) will be used and disposed of, whether facial images will be retained or used for other purposes, the rights of the individual and the consequences of declining to consent, how to make a complaint, and where further information can be obtained about the services);
- agreements must contain arrangements for dealing with complaints and reporting security breaches;
- parties must comply with the access policy for the relevant service;
- parties must not disclose identification information received as a result of using the service except as required or permitted by law; and
- if the party is a government authority, the officer or employee who makes the request must be trained in facial recognition and image comparison. This may mitigate the risk of erroneous data matches and misidentification.[143]

1.58 The requirement to publish participation agreements on the department's website (excluding any parts of the document that would unreasonably disclose an individual's personal information) would also serve as a safeguard.[144] Further, non-compliance with a participation agreement may result in the suspension or termination of an entity's ability to access and use the service. The statement of compatibility states that this is a significant penalty and will support compliance and act as a deterrent to non-compliance given the importance of the identity verification services to government and industry.[145] The statement of compatibility states that these are important safeguards and will ensure the Department implements

143 Identity Verification Services Bill 2023, clauses 9 and 10.

144 Identity Verification Services Bill 2023, subclauses 39(1) and (2).

145 Statement of compatibility, p. 10.

appropriate security measures to protect personal and sensitive information, and prevent unauthorised interference or access.[146]

1.59 Another key safeguard is the Driver Licence database hosting agreement (see above paragraph [1.28]), which requires parties to be subject to privacy legislation and imposes certain requirements on each state or territory party and the Department.[147] State or territory parties must take reasonable steps to inform each individual whose identification information is to be included in the database of that inclusion and provide information to individuals regarding how to find what information has been included and how to correct any errors in the database. Individuals must also be informed of data breaches that involve identification information and area reasonably likely to result in serious harm to the individual. The department is required to maintain the security of the Driver Licence database including by encrypting the information.

1.60 The safeguards contained in the hosting agreement would generally assist with proportionality, although some questions arise with respect to the requirement to inform individuals of the inclusion of their information in the database. In particular, it is not clear what 'reasonable steps' must be taken to satisfy this requirement and it is noted that an individual is not required to consent to their information being included in the database. As noted above, entrusted persons, including law enforcement authorities, may access information held in the database with the consent of the state and territory authority who supplied the information, but the consent of the individual is not required. It is not clear why an individual is not required to consent to the inclusion of their driver's licence information, including facial image, in the Driver Licence database. The absence of consent in this context is of particular concern given the sensitivity of the information held in the database, the broad purposes for which the information may be used (including secondary purposes by law enforcement) and the large number of persons to whom it would apply (noting that approximately 80 per cent of the population have a driver's licence).[148] Indeed, the UN High Commissioner for Human Rights has highlighted the importance of consent in this context, stating that:

> 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.[149]

---

146 Statement of compatibility, p. 12.

147 Identity Verification Services Bill 2023, clause 13.

148 Statement of compatibility, p. 8.

149 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [29].

1.61 The UN High Commissioner for Human Rights has further noted the importance of 'a right to object to personal data processing, at least for cases where the processing entity does not demonstrate legitimate, overriding grounds for the processing'.[150]

1.62 In addition, it is not clear how long an individual's data would be held in the Driver Licence database. International human rights law jurisprudence has raised concerns as to the compatibility of indefinite biometric data retention programs with the right to privacy.[151] In particular, the United Kingdom courts have concluded that the retention of photographs of unconvicted persons by the police was a breach of the right to privacy,[152] and that access to data should be strictly limited solely to fighting serious crime and be subject to prior review by a court or independent administrative authority.[153] Collectively, these authorities suggest that the indiscriminate retention of a person's data (including biometric information and photographs) may not be a proportionate limitation on the right to privacy.

1.63 Other safeguards accompanying the measures include:

---

150 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [30].

151 In *S and Marper v United Kingdom*, the European Court of Human Rights held that laws in the United Kingdom that allowed for fingerprints, cellular samples and DNA profiles to be indefinitely retained despite the affected persons being acquitted of offences was incompatible with the right to privacy. The court expressed particular concern about the 'indiscriminate and open-ended retention regime' which applied the same retention policy to persons who had been convicted to those who had been acquitted. The court considered that the 'blanket and indiscriminate nature of the powers of retention' failed to strike 'a fair balance between the competing public and private interests'. See, *S and Marper v United Kingdom*, European Court of Human Rights Application Nos.30562/04 and 30566/04 (2008) [127].

152 See *Wood v Commissioner of Police for the Metropolis* [2009] EWCA Civ 414 (21 May 2009), which concluded that the retention of photographs which had been taken by police of a person in circumstances where the person had not committed any criminal offence had a disproportionate impact on the right to privacy under the *Human Rights Act 1998 (UK)*, at [89] and [97].

153 *Secretary of State for the Home Department v Watson MP & Ors* [2018] EWCA Civ 70 (30 January 2018) applying the Court of Justice of the European Union decision in *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson and Others* [2016] EUECJ C-203/15; see also *Digital Rights Ireland Limited v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others* [2014] EUECJ C-293/12. The interpretation of the human right to privacy under the European Convention of Human Rights and the EU Charter of Fundamental Rights in those cases is instructive in informing Australia's international human rights law obligations in relation to the corresponding right to privacy under the International Covenant on Civil and Political Rights. See, also, for example, the committee's consideration of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 in its *Fiftieth Report of the 44th Parliament* (14 November 2014) pp. 10-22.

- private sector organisations are limited to receiving either a 'match' or 'no match' response in relation to a Face Verification Service request, meaning they will not receive additional information about the individual;[154]
- parties are required to comply with access policies, which include conditions providing for the parties to give the Secretary statements of the legal basis for disclosing and using identification information for the purposes of requesting and providing services of that kind to the parties;[155]
- the department is required to maintain the security of electronic communications, including by encrypting the information, and protecting it from unauthorised interference or access;[156]
- publication of key agreements, including intergovernmental agreement, participation agreement and the Driver Licence database hosting agreement to be published on the department's website;[157]
- an annual assessment of the operation and management of facilities by the Information Commissioner;[158]
- annual reports that must be tabled in Parliament;[159]
- oversight by the Commonwealth Ombudsman;[160] and
- review of the Identity Verification Services Bill 2023 within two years of commencement.[161]

1.64 In general, the safeguards contained in participation agreements and the hosting agreements, as well as the other safeguards identified above, would significantly assist with proportionality with respect to the right to privacy. Indeed, several safeguards have been recognised as being effective for the purposes of international human rights law, such as informing individuals when their personal information and data is being processed and used and requiring entities to comply with data processing laws and policy frameworks.[162] However, as outlined above, some questions arise as to the adequacy of some safeguards in practice.

---

154 Statement of compatibility, p. 8.

155 Identity Verification Services Bill 2023, clause 14.

156 Identity Verification Services Bill 2023, clause 25.

157 Identity Verification Services Bill 2023, clause 39.

158 Identity Verification Services Bill 2023, clause 40.

159 Identity Verification Services Bill 2023, clause 41.

160 Identity Verification Services Bill 2023, clause 34.

161 Identity Verification Services Bill 2023, clause 43.

162 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [29] and [30]

1.65 Further, it is noted that the above safeguards primarily relate to the right to privacy and the statement of compatibility did not identify any safeguards specific to the rights to social security or equality and non-discrimination.

1.66 An important safeguard with respect to the right to social security is the availability of alternative methods of identity verification. The UN High Commissioner for Human Rights has stated that 'imposing biometric identification requirements on recipients of welfare benefits is disproportionate if no alternative is provided'.[163] The explanatory materials state that biometric identity verification is *required* for certain Centrelink services.[164] It is not clear whether there is an alternative method available if the individual is unable to complete the verification process, for example because they do not have the required identity documents or they do not consent to the service. While individual consent is required for the Document and Face Verification Services, it is not clear whether such consent in the context of the social security system can be said to be 'free, specific, informed and unambiguous'.[165] This is because it appears the consequences of declining to consent would be an inability to access social security services, including benefits, if indeed biometric verification is required and there is no alternative method available.

1.67 Finally, with respect to the right to an effective remedy, the measures are accompanied by some safeguards that appear to protect this right, including:

- the requirements in participation agreements with respect to reporting breaches of security, having arrangements for dealing with complaints, and informing individuals about these matters; and
- the requirements in the Driver Licence database hosting agreement to inform individuals of data breaches which involve identification information that relates to the individual and are reasonably likely to result in serious harm to the individual, and provide a means for dealing with complaints.

1.68 Informing an individual about security breaches relating to their personal information would afford them the opportunity to make a complaint and potentially pursue a remedy for any violation of their rights, noting a key obstacle in accessing a remedy is lack of knowledge or proof of interference with privacy.[166] The explanatory memorandum states the requirement for participation agreements to have arrangements to deal with complaints 'will ensure individuals have an appropriate avenue to pursue any complaints directly with the party to the participation, and is

---

163 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [39].

164 Explanatory memorandum, p. 61; statement of compatibility, p. 7.

165 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31 (2021) [29].

166 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [54].

not intended to preclude any separate complaint mechanism an individual may have, including complaints under the Privacy Act or to an ombudsman'.[167] However, it is not clear how these complaint mechanisms will operate in practice and what specific complaint mechanisms would be available to individuals under the Privacy Act.

1.69 With respect to informing individuals about data breaches, it is not clear how 'reasonably likely to result in serious harm' will be assessed and why this high threshold is required (namely, why are individuals not informed when there is a data breach without there needing to be 'serious harm').

1.70 Further, the measure authorising the automation of decisions to disclose personal information to a person participating in the Document or Face Verification Service raises additional complexities with respect to the right to an effective remedy. The UN High Commissioner for Human Rights has stated that:

> Victims also face new and growing challenges in the context of algorithmic decision-making, where individuals may not be able to access the input data or challenge the findings reached by the algorithm itself or how such findings were used in the decision reached.[168]

1.71 Further information is therefore required to assess whether individuals whose rights may be limited would have access to an effective remedy.

Committee view

1.72 The committee understands the need to ensure secure and efficient identity verification, which is essential to minimise the risk of identity theft and fraud. The committee also considers this legislation is important to govern the use of identity verification services that already exist. However, the committee is concerned about the impact on the right to privacy for the millions of Australians whose data is contained in the National Driver Licence Facial Recognition Solution database and the use of biometric identity verification services. The committee also considers that facilitating the use of biometric identity verification for the purposes of accessing social security and other government services engages and may limit the right to social security. In addition, the measures may engage and limit the right to equality and non-discrimination if the measures were to have a disproportionate impact on members of certain groups or if biased or erroneous data led to discriminatory decisions. Further, if the measures impermissibly limited one or more of these rights, it is not clear whether an individual would have access to an effective remedy with respect to any violation of rights.

---

167 Explanatory memorandum, p. 31.

168 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29 (2018) [55].

1.73 The committee considers further information is required to assess the compatibility of the measures with these rights, and as such seeks the Attorney-General's advice in relation to:

(a) how the measures are effective to achieve the stated objectives of preventing identity theft and fraud, and preventing fraud and misuse of government funds in the context of the social security system;

(b) whether individuals need to consent to government authorities supplying identification information in the first instance to one of the identification verification services, and if so, can individuals withdraw consent at a later stage and request the information be removed from a service;

(c) why consent from the relevant individual is not required for their driver's licence to be included on the Driver Licence database (noting that individual consent is required for use of the Document and Face Verification Services);

(d) what constitutes 'reasonable steps' in the context of informing individuals whose identification information is, or is to be, included in the Driver Licence database;

(e) what are the consequences of declining to consent to biometric verification in the context of accessing government services, particularly Centrelink;

(f) whether there are alternative methods for individuals to authenticate or verify their identity, including for the purposes of creating a strong myGov account, to access social security services;

(g) whether consent in the context of accessing the social security system and other government services can be said to be genuinely free, given that such consent is required to access certain services and declining to consent would appear to restrict access to such services;

(h) with respect to informing individuals about data breaches, how will the threshold 'reasonably likely to result in serious harm'[169] be assessed and why is this threshold necessary (namely, why are individuals not informed when there is a data breach without there needing to be 'serious harm');

(i) to which persons or organisations are the department and entrusted persons authorised to disclose identification information to, noting the bill authorises disclosure of such information but does not clearly specify to whom it may be disclosed;

---

[169] See Identity Verification Services Bill 2023, paragraph 13(3)(c).

(j) what circumstances can law enforcement agencies access and use information communicated to an identity verification service or held in, or generated by, the Driver Licence database, and what safeguards are in place to ensure that any access and use of identification information is a proportionate limitation on the right to privacy;

(k) what safeguards are in place to mitigate the risk of data verification errors, including inaccurate face matching that may disproportionately affect one group over another, and the adverse impacts this may have on individuals, particularly in the context of the right to equality and non-discrimination;

(l) what safeguards are in place to mitigate the risk of data breaches and hacking, or what assurances have been given by technical experts regarding the risks in the system, noting that the consequential interference on the right to privacy arising from such an event would be significant given the extensive scope of information communicated to identity verification services and held in the Driver Licence database;

(m) how long will an individual's data be held in the Driver Licence database, and if it is indefinite, how is this a proportionate limit on the right to privacy;

(n) whether the measures are accompanied by any safeguards to ensure that any limitation on the rights to social security and equality and non-discrimination are proportionate in practice; and

(o) whether less rights restrictive alternatives were considered and if so, why these were not considered appropriate.

Legislative instruments

Social Security (Administration) Income Management Regime instruments[170]

FRL No.	F2023L01173; F2023L01172; F2023L01269; F2023L01273; F2023L01274
Purpose	These five legislative instruments specify various matters to operationalise aspects of enhanced income management and income management regimes
Portfolio	Social Services
Authorising legislation	*Social Security (Administration) Act 1999*
Disallowance	15 sitting days after tabling (tabled in the House of Representatives on 4 September 2023 and in the Senate on 5 September 2023). Notice of motion to disallow must be given by 16 November 2023 in the House and by 9 November 2023 in the Senate)[171]
Rights	Social security; adequate standard of living; equality and non-discrimination; rights of the child; privacy

The income management regimes

1.74 By way of background, the *Social Security (Administration) Amendment (Repeal of Cashless Debit Card and Other Measures) Act 2022* (2022 Act) introduced the enhanced income management regime under Part 3AA of the *Social Security*

[170] Social Security (Administration) (Enhanced Income Management Regime—State Referrals) Determination 2023 [F2023L01173]; Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023 [F2023L01172]; Social Security (Administration)(Specified Income Management Territory—Northern Territory) Instrument 2023 [F2023L01269]; Social Security (Administration) (Recognised State or Territory—Northern Territory) Determination 2023 [F2023L01273]; Social Security (Administration) (Declared Child Protection State—New South Wales, Queensland, South Australia and Victoria) Determination 2023 [F2023L01274].

This entry can be cited as: Parliamentary Joint Committee on Human Rights, Social Security (Administration) Income Management Regime instruments, *Report 11 of 2023*; [2023] AUPJCHR 107.

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

Administration Act 1999 (the Act).[172] This 2022 Act compulsorily transitioned former Cashless Debit Card participants in the Northern Territory and Cape York region to the new enhanced income management regime. The *Social Security (Administration) Amendment (Income Management Reform) Act 2023* (2023 Act) expanded access to the enhanced income management regime by introducing eligibility criteria for mandatory participation in the regime and restricting the way a person subject to this regime can spend the 'qualified' portion of their welfare payment.[173] The 2023 Act directed all new entrants to income management to the enhanced income management regime and closed entry to the old income management regime under Part 3B of the Act, and offered participants subject to income management under Part 3B, the choice to voluntarily transition to the enhanced income management regime. The income management regime under Part 3B has continued to operate in its current form for those participants who chose not to transition to the enhanced income management regime. These instruments operationalise key aspects of the enhanced income management regime under Part 3AA and the income management regime under Part 3B of the Act.

1.75 The *Social Security (Administration) (Enhanced Income Management Regime—State Referrals) Determination 2023* declares New South Wales, Victoria, Queensland, Western Australia, South Australia and the Northern Territory as child protection areas for the purposes of Part 3AA of the Act, meaning that child protection officers in these states and territory may refer individuals to the enhanced income management regime (by providing notice to the Secretary requiring that the person be placed on the regime).[174] It also declares the Department of Health of the Northern Territory as a 'recognised State/Territory authority', meaning that persons may be made subject to the enhanced income management regime by a referral of an officer or employee of this department.[175] Additionally, it specifies 70 per cent as the percentage of a person's welfare payment that is to be the 'qualified portion' (the amount that may be spent on non-excluded goods and services) with respect to

---

172 See Parliamentary Joint Committee on Human Rights, *Social Security (Administration) Amendment (Repeal of Cashless Debit Card and Other Measures) Bill 2022,* Report 3 of 2022 (7 September 2022) pp. 15–26 and *Report 5 of 2022* (20 October 2022) pp. 39–55.

173 See Parliamentary Joint Committee on Human Rights, *Social Security (Administration) Amendment (Income Management Reform) Bill 2023 and related instruments,* Report 4 of 2023 (29 March 2023) pp. 9–25 and *Report 5 of 2023* (9 May 2023) pp. 58–80.

174 Social Security (Administration) (Enhanced Income Management Regime—State Referrals) Determination 2023, Part 2, section 5. The person must also meet the other criteria set out in section 123SCA of the Act.

175 Social Security (Administration) (Enhanced Income Management Regime—State Referrals) Determination 2023, section 6. See *Social Security Administration Act 1999*, sections 123SCJ and 123SCK.

persons required to be subject to the enhanced income management regime as a result of a notice given by a state or territory child protection officer.[176]

1.76 The *Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023* operationalises aspects of the enhanced income management regime as it relates to vulnerable welfare payment recipients, disengaged youth and long-term welfare payment recipients. Under the Act, a person will be subject to the enhanced income management regime if they meet certain eligibility criteria, including that they reside in a specified area, they are a vulnerable welfare payment recipient (as determined by the Secretary) or they are a particular age (for disengaged youth and long-term welfare payment recipients), and they are not an exempt welfare payment recipient.[177] This determination specifies the Northern Territory and areas covered by other instruments, including the Anangu Pitjantjatjara Yankunytjatjara lands and Ngaanyatjarra Lands, as specified areas for the purposes of the eligibility criterion relating to a person's usual place of residence.[178] It also sets out the decision-making principles with which the Secretary must comply in deciding whether to determine that a person is a vulnerable welfare payment recipient for the purposes of subjecting them to the enhanced income management regime.[179] Finally, the instrument specifies classes of persons the Secretary may determine to be exempt welfare payment recipients (such that they cannot be subject to enhanced income management).[180]

1.77 The other instruments specify the Northern Territory for the purposes of eligibility criteria relating to disengaged youth and long-term welfare payment recipients;[181] declare the Northern Territory more generally as a recognised state or territory;[182] and declare New South Wales, Queensland, South Australia and Victoria

---

176 Social Security (Administration) (Enhanced Income Management Regime—State Referrals) Determination 2023, Part 4, section 7. See *Social Security Administration Act 1999*, sections 123SLA and 123SCA.

177 *Social Security Administration Act 1999*, sections 123SCL-123SDF.

178 Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023, section 5. See *Social Security Administration Act 1999*, paragraph 123SCL(1)(a).

179 Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023, sections 6-8. See *Social Security Administration Act 1999*, paragraph 123SCM.

180 Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023, sections 9-12.

181 Social Security (Administration) (Specified Income Management Territory—Northern Territory) Instrument 2023, sections 7 and 8.

182 Social Security (Administration) (Recognised State or Territory—Northern Territory) Determination 2023, section 7. See *Social Security Administration Act 1999*, section 123UFAA.

as child protection states,[183] for the purposes of the income management regime under Part 3B of the Act. The effect of these instruments is that a person will be subject to the income management regime under Part 3B of the Act if their usual place of residence is the Northern Territory and they meet other eligibility criteria relating to disengaged youth[184] and long-term welfare payment recipients,[185] or they are required to be subject to the regime as a result of a referral by a child protection officer in New South Wales, Queensland, South Australia or Victoria or an officer or employee of a Northern Territory authority.

International human rights legal advice

Rights to social security; adequate standard of living; equality and non-discrimination; rights of the child

1.78 As the committee has previously reported on numerous occasions, measures relating to mandatory income management engage multiple human rights.[186] The committee has found that, to the extent that income management ensures a portion of an individual's welfare payment is available to cover essential goods and services,

---

183 Social Security (Administration) (Declared Child Protection State—New South Wales, Queensland, South Australia and Victoria) Determination 2023, section 7.

184 The criteria for the disengaged youth is that they are an eligible recipient of a particular welfare payment, they are between 15 and 25 years, they usually reside within a specified place, they are not an exempt welfare payment recipient, they do not have an excluded payment nominee, they are not subject to other income management regimes, and they were an eligible recipient of a specific welfare payment for at least 13 of the past 26 weeks. See *Social Security Administration Act 1999*, section 123UCB.

185 The criteria for the long term welfare payment recipient is that they are an eligible recipient of a particular welfare payment, they are at least 25 years but not reached pension age, they usually reside within a specified place, they are not an exempt welfare payment recipient, they do not have an excluded payment nominee, they are not subject to other income management regimes, and they were an eligible recipient of a specific welfare payment for at least 52 of the past 104 weeks. See *Social Security Administration Act 1999*, section 123UCC.

186 See Parliamentary Joint Committee on Human Rights, *Social Security (Administration) Amendment (Income Management Reform) Bill 2023 and related instruments,* *Report 4 of 2023* (29 March 2023) pp. 9–25 and *Report 5 of 2023* (9 May 2023) pp. 58–80; *Social Security (Administration) Amendment (Repeal of Cashless Debit Card and Other Measures) Bill 2022,* *Report 3 of 2022* (7 September 2022) pp. 15–26 and *Report 5 of 2022* (20 October 2022) pp. 39–55; *2016 Review of Strong Futures measures* (16 March 2016) pp. 37–62; *Eleventh Report of 2013: Stronger Futures in the Northern Territory Act 2012 and related legislation* (June 2013) pp. 45–62. The committee has made similar comments regarding measures relating to the Cashless Debit Card program. See, e.g. Parliamentary Joint Committee on Human Rights, *Thirty-first report of the 44th Parliament* (24 November 2015) pp. 21–36; *Report 7 of 2016* (11 October 2016) pp. 58–61; *Report 9 of 2017* (5 September 2017) pp. 34–40; *Report 11 of 2017* (17 October 2017) pp. 126–137; *Report 8 of 2018* (21 August 2018) pp. 37–52; *Report 2 of 2019* (2 April 2019) pp. 146–152; *Report 1 of 2020* (5 February 2020) pp. 132–142; *Report 14 of 2020* (26 November 2020) pp. 38–54; *Report 1 of 2021* (3 February 2021) pp. 83–102; *Report 14 of 2021* (24 November 2021) pp. 14–18.

the income management regime could have the potential to promote rights, including the right to an adequate standard of living and the rights of the child.[187] However, the committee has also found that mandatory income management in Australia engages and limits a number of other human rights, including the rights to a private life,[188] social security,[189] equality and non-discrimination,[190] the rights of the child,[191] and potentially the right to an adequate standard of living (if being subject to mandatory income management caused difficulties in accessing and meeting basic needs).[192]

1.79 Insofar as these instruments operationalise key aspects of the enhanced income management regime under Part 3AA and the income management regime under Part 3B of the Act, including by specifying eligibility criteria for mandatory participation in the regimes and specifying the qualified portion of a participant's welfare payment that is to be, in effect, restricted, these same human rights are

---

187 International Covenant on Economic, Social and Cultural Rights, article 11, and Convention on the Rights of the Child. The statement of compatibility for the two determinations state that they promote the right to an adequate standard of living by restricting individuals from spending a significant portion of their welfare payment to purchase excluded goods and services, such as alcohol, gambling products, pornography and tobacco, which ensures individuals will have sufficient funds available to meet their basic needs such as rent, food and household bills: Social Security (Administration) (Enhanced Income Management Regime—State Referrals) Determination 2023, p. 9; Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023, Explanatory Statement, p. 18. See also Social Security (Administration) (Specified Income Management Territory – Northern Territory) Instrument 2023, Statement of Compatibility, p. 11.

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

189 International Covenant on Economic, Social and Cultural Rights, article 9. The core components of the right to social security are that social security, whether provided in cash or in kind, must be available, adequate, and accessible. See UN Committee on Economic, Social and Cultural Rights*, General Comment No. 19: The Right to Social Security* (2008) [3].

190 International Covenant on Civil and Political Rights, articles 2, 16 and 26 and International Covenant on Economic, Social and Cultural Rights, article 2. It is further protected by the International Convention on the Elimination of All Forms of Racial Discrimination, articles 2 and 5. The relevant protected attributes for the purposes of mandatory income management include race (due to the large number of Aboriginal and Torres Strait Islander persons participating in mandatory income management), place of residence within a state and age (noting that 'disengaged youth', which includes children aged between 15 and 17 years, are a class of participants who are subject to the regimes). As to the disproportionate effect of these measures on groups with these protected attributes, with respect to instruments relating to the Northern Territory, for example, according to the 2021 Census, there are 61,000 people who have identified as Aboriginal and/or Torres Strait Islander living in the Northern Territory (which represents 26.3 per cent of the total population and a larger percentage than in other regions). The data also states that 18.7 per cent of the First Nations population in the Northern Territory are between the ages of 15 and 24. [Northern Territory: Aboriginal and Torres Strait Islander population summary | Australian Bureau of Statistics (abs.gov.au)].

191 Convention on the Rights of the Child, articles 2, 3, 16 and 26.

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

engaged and limited.[193] The statements of compatibility accompanying each of the instruments acknowledge, in general terms, that some of these rights are engaged, such as the rights to social security and an adequate standard of living, but fail to identify all rights potentially limited, such as the right to a private life. Limits on these rights may be permissible where a measure seeks to achieve a legitimate objective, is rationally connected to (that is, effective to achieve) that objective, and is proportionate to that objective.

1.80 The stated objectives of the measures relating to the enhanced income management regime are to provide a mechanism to commence and operate the enhanced income management regime and provide participants with access to modern banking technology.[194] The stated objectives of the measures relating to the income management regime include assisting welfare recipients to meet their priority needs and promote and protect the health and development of children.[195] As the committee has previously stated, the general objective of the income management regimes—to combat social harms caused by the use of harmful products—is capable of constituting a legitimate objective.[196] However, it is not evident that facilitating the continued operation of *mandatory* income management under Parts 3AA and 3B of the Act is, for the purposes of international human rights law, necessary and addresses a public or social concern that is pressing and substantial enough to warrant limiting human rights. While facilitating the operation of a regime that provides participants with access to superior technology and improved banking functions is, in itself, an important aim, it remains unclear why this enhanced income management regime must operate on a mandatory basis (or why legislation is required to improve this technology).

1.81 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.

---

193 For a discussion on how each of these rights are engaged and limited, see Parliamentary Joint Committee on Human Rights, *Social Security (Administration) Amendment (Income Management Reform) Bill 2023 and related instruments, Report 4 of 2023* (29 March 2023) pp. 9–25 and *Report 5 of 2023* (9 May 2023) pp. 58–80.

194 Social Security (Administration) (Enhanced Income Management Regime—State Referrals) Determination 2023, statement of compatibility p. 7; Social Security (Administration) (Enhanced Income Management Regime – Commonwealth Referrals and Exemptions) Determination 2023, statement of compatibility p. 16.

195 Social Security (Administration)(Specified Income Management Territory—Northern Territory) Instrument 2023, statement of compatibility p. 10-11; Social Security (Administration) (Recognised State or Territory—Northern Territory) Determination 2023, statement of compatibility p. 9–10; Social Security (Administration) (Declared Child Protection State—New South Wales, Queensland, South Australia and Victoria) Determination 2023, statement of compatibility p. 9–10.

196 See Parliamentary Joint Committee on Human Rights, *Social Security (Administration) Amendment (Income Management Reform) Bill 2023 and related instruments, Report 4 of 2023* (29 March 2023) pp. 9–25 and *Report 5 of 2023* (9 May 2023) pp. 58–80.

The key question is whether the relevant measure is likely to be effective in achieving the objective being sought. Previous evaluations of mandatory income management, including the cashless debit card program, were inconclusive regarding its effectiveness, and whether it has caused or contributed to other harms.[197] Based on earlier evaluations of the income management regime, the committee found in 2016 that the compulsory income management regime did not appear to be an effective approach to addressing issues of budgeting skills and ensuring that an adequate amount of income support payments is spent on priority needs. It noted that while the income management regime may have some benefit for persons who voluntarily participated in the regime, it had limited effectiveness for the vast majority of people who were compelled to participate.[198] There do not appear to be more recent evaluations available with respect to either income management regime.[199] Without more recent evaluations, and noting earlier evaluations of mandatory income management were inconclusive regarding its effectiveness, it is not possible to conclude that the income management regimes under Part 3B and Part 3AA of the Act, which will continue to subject persons to mandatory income management, would be effective to achieve the stated objectives.

1.82 With respect to the proportionality of measures relating to mandatory income management, the committee has previously stated that while there are some safeguards within Parts 3AA and 3B of the Act, such as the ability to exempt certain welfare payment recipients from the regimes,[200] it is not clear these safeguards are

---

197 A summary of the evaluations of the Cashless Debit Card program is set out in Parliamentary Joint Committee on Human Rights, *Report 14 of 2020* (26 November 2020) pp. 38–54; *Report 1 of 2021* (3 February 2021) pp. 83–102. Studies have been conducted examining other specific elements of the cashless welfare trial, including its effects on: Indigenous mobility; homelessness; and perceptions of shame attached with use of the card. See, *Australian Journal of Social Issues*, vol. 55, no. 1, 2020. In particular: Eve Vincent et al, '"Moved on"? An exploratory study of the Cashless Debit Card and Indigenous mobility', pp. 27–39; Shelley Bielefeld et al, 'Compulsory income management: Combatting or compounding the underlying causes of homelessness?', pp. 61–72; Cameo Dalley, 'The "White Card" is grey: Surveillance, endurance and the Cashless Debit Card', pp. 51–60; and Elizabeth Watt, 'Is the BasicsCard "shaming" Aboriginal people? Exploring the differing responses to welfare quarantining in Cape York', pp. 40–50. See also Luke Greenacre et al, 'Income Management of Government payments on Welfare: The Australian Cashless Debit Card', *Australian Social Work* (2020) pp. 1–14.

198 Parliamentary Joint Committee on Human Rights, *2016 Review of Strong Futures measures* (16 March 2016), p. 52.

199 The explanatory statements accompanying each of the instruments do not refer to any recent evaluations of the income management regimes under Part 3B or Part 3AA of the Act. The explanatory statements refer to the 'mixed results' of previous evaluations of the CDC program and note that future evaluations will focus on the experience of participants coming off the programs and effectiveness of support services.

200 See Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023, Part 3.

sufficient. The committee has also noted the insufficient flexibility to consider individual circumstances, the potentially significant interference with human rights and the availability of less rights restrictive ways of achieving the stated objectives.[201] This analysis remains relevant to these instruments.

1.83 The decision-making principles (set out in one of these determinations),[202] with which the Secretary must comply in deciding whether to determine that a person is a vulnerable welfare payment recipient for the purposes of subjecting them to the enhanced income management regime, may offer some safeguard value. The Secretary is required to consider certain matters, including whether the person is experiencing an indicator of vulnerability and, if so, whether being subject to the enhanced income management regime would be an appropriate response to that indicator, and whether the person is applying appropriate resources to meet some or all of their relevant priority needs.[203] In considering these matters, the Secretary must have regard to certain matters, including the personal circumstances of the individual and any services available to the individual.[204] Additionally, the Secretary is not required to make a determination that a person is a vulnerable welfare payment recipient if to do so would place the person's mental, physical or emotional wellbeing at risk.[205] These decision-making principles provide for some flexibility to consider individual circumstances with respect to whether a person should be determined to be a 'vulnerable welfare payment recipient'. However, this flexibility does not extend to other classes of persons who may be subject to mandatory income management. Concerns therefore remain that the eligibility criteria applicable to the income management regimes are insufficiently individualised.

1.84 The statements of compatibility accompanying the instruments do not identify any additional safeguards that may assist with proportionality. As such, concerns remain that the measures relating to mandatory income management are not proportionate. Accordingly, these instruments risk impermissibly limiting the rights to social security, privacy, equality and non-discrimination and the rights of the child, as well as potentially the right to an adequate standard of living, if participants experience difficulties in meeting basic needs.

---

201 Parliamentary Joint Committee on Human Rights, *Social Security (Administration) Amendment (Income Management Reform) Bill 2023 and related instruments, Report 4 of 2023* (29 March 2023) pp. 9–25 and *Report 5 of 2023* (9 May 2023) pp. 58–80.

202 Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023, Division 2.

203 Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023, subsection 7(1).

204 Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023, subsection 7(6).

205 Social Security (Administration) (Enhanced Income Management Regime—Commonwealth Referrals and Exemptions) Determination 2023, subsection 8(2).

Committee view

1.85 The committee notes that the instruments operationalise key aspects of the enhanced income management regime under Part 3AA of the Act and the income management regime under Part 3B of the Act. The committee considers the instruments that facilitate the operation of the enhanced income management regime, which offers participants superior technology and improved banking functions, to be positive measures.

1.86 However, the committee also notes that in operationalising key aspects of the income management regimes, including by specifying eligibility criteria for mandatory participation in the regimes and specifying the qualified portion of a participant's welfare payment that is to be, in effect, restricted, the instruments engage and limit a number of human rights, including the rights to a private life, social security, equality and non-discrimination, the rights of the child, and potentially the right to an adequate standard of living (if being subject to mandatory income management caused difficulties in accessing and meeting basic needs).

1.87 For many years, the committee has raised concerns regarding the compatibility of compulsory income management with multiple human rights. In particular, by subjecting an individual to mandatory income management and restricting how they may spend a portion of their social security payment, the measure limits the rights to social security and a private life, and possibly the right to an adequate standard of living. Due to the disproportionate impact on certain groups with protected attributes, including Aboriginal and Torres Strait Islander peoples and children, the measures engage and limit the right to equality and non-discrimination and the rights of the child.

1.88 The committee notes that while the general objective of income management is important, that is, to combat social harms caused by the use of harmful products, it is not clear that continuing to operate *mandatory* income management is, for the purposes of international human rights law, a necessary measure that addresses a pressing and substantial concern. The committee considers that, in the absence of adequate safeguards and sufficient flexibility to consider individual circumstances, and in light of the potentially significant interference with human rights that may result from compulsory participation in income management, the legislative instruments risk impermissibly limiting the rights to social security, privacy, equality and non-discrimination and the rights of the child as well as potentially the right to an adequate standard of living if participants experience difficulties in meeting basic needs.

1.89 The committee notes that it will consider these instruments more comprehensively as part of its review of compulsory enhanced income management

and compulsory income management for compatibility with human rights.[206] The committee is required to complete the first review and report to the Parliament by 4 September 2024.

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

[206] In 2023, the committee was given the function (under section 243AA of the *Social Security (Administration) Act 1999*) to review compulsory enhanced income management and compulsory income management for compatibility with human rights and report to the Parliament. The committee must complete the first review by 4 September 2024, and subsequent reviews must be completed within three years thereafter.

Social Security (Administration) (Public Interest Certificate Guidelines) (DEWR) Determination 2023[207]

FRL No.	F2023L01229
Purpose	This legislative instrument establishes guidelines to assist the Secretary of the Department of Employment and Workplace Relations, or their delegate, in exercising their power under the *Social Security (Administration) Act 1999* to disclose information acquired in the performance of functions or duties, or exercise of powers, where necessary in the public interest
Portfolio	Employment and Workplace Relations
Authorising legislation	*Social Security (Administration) Act 1999*
Disallowance	15 sitting days after tabling (tabled in the House of Representatives on 14 September 2023 and in the Senate on 16 October 2023). Notice of motion to disallow must be given on the second sitting day in 2024 in the House and by 28 November 2023 in the Senate)[208]
Rights	Multiple rights

Disclosure of personal information in the public interest

1.91 The *Social Security (Administration) Act 1999* makes it an offence for a person to, for example, make an unauthorised record of, use or disclose protected information or produce certain documents to a court. However, the Secretary may do so if they certify that it is necessary to do so in the public interest in a particular case or class of case. In giving such certificates, the Secretary must act in accordance with guidelines. This legislative instrument sets out those guidelines.[209]

1.92 The Secretary may give a public interest certificate for the disclosure of information if it cannot be reasonably obtained from a source other than the department; they are satisfied that the disclosure is for a purpose mentioned; and the

---

207 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Social Security (Administration) (Public Interest Certificate Guidelines) (DEWR) Determination 2023 [F2023L01229], *Report 11 of 2023*; [2023] AUPJCHR 108.

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

209 This power is set out in subsection 208(1)(a) of the *Social Security (Administration) Act 1999*, providing that the Secretary may certify that the disclosure of information is in the public interest. This legislative instrument revokes and replaces the previous such determination: Social Security (Administration) (Public Interest Certificate Guidelines) (DEEWR) Determination 2013 [F2013L01553].

disclosure will be made either to a person specified or a person who the Secretary is satisfied has a sufficient interest in the information (meaning they are either a relevant minister or have a genuine and legitimate interest in the information).[210] In giving such a certificate, the Secretary must have regard to any situation in which the person to whom the information relates is, or may be subject to, physical, psychological or emotional abuse; and whether the person in such a situation may be unable to give notice of his or her circumstances because of their age; disability; or social, cultural, family or other reasons.[211]

1.93 The guidelines provide that the Secretary may disclose information for a range of purposes, including those related to:

- threats to a person's life, health or welfare;[212]
- the enforcement of a criminal law, or relating to certain offences or threatened offences;[213]
- proceeds of crime orders;[214]
- inquiries relating to a missing or deceased person;[215]
- public housing administration;[216]
- the functions of the Family Responsibilities Commission;[217]
- assisting a child protection agency to contact a parent or relative in relation to a child;[218]
- progressing or resolving, where necessary, a matter of relevance to a department that administers any part of the social security or family assistance law;[219] or
- Australian Public Service Code of Conduct investigations.[220]

---

210 Section 8.

211 Section 6.

212 Section 9.

213 Section 10.

214 Section 11.

215 Sections 12–13.

216 Section 14.

217 Section 15. This is a Queensland statutory body established pursuant to the *Family Responsibilities Commission Act 2008* (QLD). The primary objective of the Commission is to hold conferences with community members to encourage persons to engage in 'socially responsible standards of behaviour' while promoting the interests, rights and wellbeing of children and other vulnerable persons living in the community.

218 Section 17.

219 Section 19.

220 Section 21.

1.94 Part 3 of the guidelines separately provide that the secretary may disclose information relating to a child experiencing homelessness in receipt of a relevant social security payment, including:

- where the person has been subjected to violence or abuse;[221]
- to verify payment qualification;[222] or
- for purposes relating to facilitating a reconciliation with the child's parents or to provide assurance to the child's parents that they have been in contact with the department.[223]

Preliminary international human rights legal advice

Multiple rights

1.95 By permitting the disclosure of personal information in circumstances where the person in question may be at some risk of harm, or is a young person who is not living with their parents, the measure may promote several rights, including the rights to life, health, social security and an adequate standard of living, and protection of the family. The right to life imposes an obligation on the state to protect people from being killed by others or identified risks.[224] The right to health is the right to enjoy the highest attainable standard of physical and mental health.[225] The right to social security recognises the importance of adequate social benefits in reducing the effects of poverty and plays an important role in realising many other economic, social and cultural rights, in particular the right to an adequate standard of living and the right to health.[226] The right to an adequate standard of living requires state parties to take steps to ensure the availability, adequacy and accessibility of food, clothing, water and housing for all people in Australia.[227] The right to respect for the family requires the state not to arbitrarily or unlawfully interfere in family life and to adopt measures to

221 Section 24.

222 Section 25.

223 Section 26–27.

224 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.

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

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

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

protect the family.[228] The statement of compatibility briefly states that the measure promotes the right to an adequate standard of living and the rights of the child.[229]

1.96 However, by permitting the disclosure of personal information, this measure also engages and limits the right to privacy. The right to privacy includes respect for informational privacy, including the right to respect for private and confidential information, particularly the storing, use and sharing of such information.[230] 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.

1.97 The statement of compatibility briefly identifies that the guidelines engage the right to privacy. It states that the guidelines 'promote, or are reasonably proportionate to achieving human rights objectives', and sets out a series of dot points with respect to permissible grounds for disclosure.[231] However, it does not analyse the compatibility of each of the grounds for disclosure with the right to privacy. For example, it states that the disclosure of information relating to a proceeds of crime order 'is proportionate to the objectives of that legislation and consistent with the legitimate human rights purposes of the criminal law'.[232] The statement of compatibility does not identify key factors relevant to an assessment of whether a limitation on the right to privacy is permissible. In particular, it does not identify what personal information the department holds and may therefore be disclosed under these grounds. Further, it does not identify whether each of the grounds for disclosure would be a proportionate limit on the right to privacy (having regard to whether the measure is sufficiently circumscribed, 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). In this regard, subsection 208(1) of the Act empowers the Secretary to issue a public interest certificate permitting the disclosure of personal information in relation to a class of cases, not merely one individual.[233] This raises questions as to whether the measure is appropriately circumscribed. It is also unclear whether officers administering this measure would have training or specialised experience in assessing relevant factors, such as whether a young person has experienced violence or abuse, or whether there is a threat to the life of a person.

---

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

229 Statement of compatibility, pp. 12–13.

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

231 Statement of compatibility, pp. 11–12.

232 Statement of compatibility, p. 11.

233 *Social Security (Administration) Act 1999*, subsection 208(1).

1.98 Further, the measure requires that in giving a public interest certificate, the Secretary must have regard to any situation in which the person to whom the information relates is, or may be, subject to physical, psychological or emotional abuse; and whether the person in such a situation may be unable to give notice of his or her circumstances because of their age, disability or for social or other reasons. Consideration of whether a person may be unable to give notice of a change in their circumstances due to age, disability or other factors engages and may limit the right to equality and non-discrimination, and the rights of persons with disability. The right to equality and non-discrimination provides that everyone is entitled to enjoy their rights without discrimination of any kind and that all people are equal before the law and entitled without discrimination to equal and non-discriminatory protection of the law.[234] International human rights law further recognises that persons with disability have a right to equal recognition before the law, and have a right to exercise their legal capacity to make decisions.[235] It is not clear how the Secretary (or their delegate) would determine that a person (including a person with disability) is unable to provide updates on their own circumstances, what training they would have in relation to assessing such factors, and when this would constitute a sufficient basis on which to disclose their personal information without their consent.

1.99 Further, a number of the grounds on which disclosure of personal information may be permitted, are broad, and may engage and limit further human rights. For example, facilitating the disclosure of personal information for the purposes of the functions of the Queensland Family Responsibilities Commission would appear likely, in practice, to have a disproportionate impact on Aboriginal and Torres Strait Islander persons, because the Commission operates largely in Aboriginal and Torres Strait Islander communities in Queensland.[236] However, because of the limited information in the explanatory materials, this is not clear.

1.100 The statement of compatibility further states that the measure promotes the rights of the child.[237] However, it does not identify that the disclosure of personal information about a child may also limit their rights, or explain how it balances the rights of the child to special protection (for example) with their right to privacy, such as in circumstances where an older child has expressed a wish that their family should not be given their personal information.

---

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

235 Convention on the Rights of Persons with Disabilities, article 12.

236 See, Family Responsibilities Commission website.

237 Statement of compatibility, p. 12.

Committee view

1.101 The committee notes that permitting the disclosure of personal social security information in a range of circumstances engages and may promote multiple rights, but it may also limit a number of rights including: the right to privacy; rights of the child; and the rights of people with disability.

1.102 The committee is concerned that the statement of compatibility accompanying this legislative instrument provides an incomplete and insufficient assessment of the measure. Where legislation limits human rights, the committee expects that the statement of compatibility will provide a detailed, reasoned and evidence-based assessment of each measure that limits rights.[238] The committee further notes that this measure revokes and replaces the earlier 2013 version of this measure, and that consequently this provides the first opportunity for the committee to consider the compatibility of this measure with human rights in ten years.[239]

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

(a) what personal information the department holds and may therefore be disclosed under these grounds;

(b) whether each of the grounds for disclosure[240] would constitute a proportionate limit on the right to privacy (including whether each measure is sufficiently circumscribed, 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);

(c) whether officers administering this measure would have training or specialised experience in assessing relevant factors, such as whether a young person has experienced violence or abuse, or whether there is a threat to the life of a person;

(d) how the Secretary would determine that a person is unable to provide updates on their own circumstances, and what training they would have in relation to assessing such factors;

---

238 For further guidance, see Parliamentary Joint Committee on Human Rights, *Guidance Note 1: Expectations for statements of compatibility*.

239 In this regard, the committee notes that the statement of compatibility accompanying the 2013 version of this measure was also incomplete, providing only an assessment of elements of the measure which were, at that time, new inclusions. See, Social Security (Administration) (Public Interest Certificate Guidelines) (DEEWR) Determination 2013 [F2013L01553], statement of compatibility.

240 In sections 9–21 and Part 3 of the legislative instrument.

(e) whether the measure is compatible with the rights of people with disability to equality before the law, including how the Secretary would determine that a person with disability is unable to give notice of their own change in circumstances; and

(f) whether the disclosure of personal information may, in circumstances provided for in this measure, engage and limit further human rights (for example, the rights of the child).

Telecommunications (Interception and Access — Independent Commission Against Corruption of South Australia) Declaration 2023[241]

FRL No.	F2023L01128
Purpose	Declares the Independent Commission Against Corruption of South Australia as an interception agency for the purposes of the *Telecommunications (Interception and Access) Act 1979*
Portfolio	Attorney-General
Authorising legislation	*Telecommunications (Interception and Access) Act 1979*
Disallowance	15 sitting days after tabling (tabled in the House of Representatives and the Senate on 4 September 2023. Notice of motion to disallow must be given by 16 November 2023 in the House and by 9 November 2023 in the Senate)[242]
Right	Privacy

Declaration as an interception agency

1.104 This legislative instrument declares the Independent Commission Against Corruption of South Australia (ICAC SA) an interception agency for the purposes of the *Telecommunications (Interception and Access) Act 1979* (the Act).[243]

1.105 This means that the ICAC SA may apply for telecommunication interception warrants under Part 2-5 of the Act.[244] These warrants permit interception of communications passing over a telecommunications systems (including listening to or recording, by any means, such a communication without the knowledge of the person

241 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Telecommunications (Interception and Access — Independent Commission Against Corruption of South Australia) Declaration 2023, *Report 11 of 2023*; [2023] AUPJCHR 109.

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

243 Pursuant to section 34 of the Act. The Independent Commission Against Corruption South Australia was formerly known as the 'Independent Commissioner Against Corruption South Australia' and was previously declared to be an interception agency pursuant to the Telecommunications (Interception and Access—Independent Commissioner Against Corruption of South Australia) Declaration 2013 [F2013L01146]. Item 4 of this legislative instrument revokes that earlier declaration.

244 *Telecommunications (Interception and Access) Act 1979,* section 39. A court or the Administrative Appeals Tribunal may authorise a telecommunications interception warrant. Most applications must be made in writing, but urgent applications may be made by telephone (see, section 40).

making the communication).[245] An issuing judge or tribunal member may grant a warrant where they are satisfied that information that would be likely to be obtained would be likely to assist in connection with the investigation by the agency of a serious offence.[246]

International human rights legal advice

Right to privacy

1.106 Authorising the ICAC SA to apply for and execute telecommunications interception warrants, which allow the covert interception of private communications, engages and limits the right to privacy.

1.107 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.[247] It also includes the right to control the dissemination of information about one's private life. The right to privacy may be permissibly limited where the limitation seeks to achieve a legitimate objective, is rationally connected to (that is, effective to achieve) that objective, and is a proportionate means by which to achieve it.

1.108 The statement of compatibility identifies that this measure engages and limits the right to privacy.[248] It states that the measure addresses the investigation and prosecution of serious crime and corruption. This is a legitimate objective for the purposes of international human rights law, and the facilitation of telecommunications interception would appear to be rationally connected to (that is, effective to achieve) that objective.

1.109 A key aspect of whether a limitation on a right is permissible is whether the limitation is proportionate to the objective being sought. In this respect, it is necessary to consider whether: a proposed limitation is sufficiently circumscribed and accompanied by sufficient safeguards; whether any less rights restrictive alternatives

---

245 *Telecommunications (Interception and Access) Act 1979*, section 6. Section 48 also provides that an interception warrant may authorise entry on to physical premises (if it would be impracticable or inappropriate to intercept communications otherwise than by use of equipment installed on those premises).

246 *Telecommunications (Interception and Access) Act 1979*, section 46. 'Serious offence' is defined in section 5D and includes a number of offences.

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

248 Statement of compatibility, p. 4. The statement of compatibility is substantially the same as that which accompanied the Telecommunications (Interception and Access – Law Enforcement Conduct Commission of New South Wales) Declaration 2017 [F2017L00533]. The committee raised privacy concerns in relation to that legislative instrument in connection with concerns regarding the compatibility of the Act itself. See, Parliamentary Joint Committee on Human Rights, *Report 7 of 2017* (8 August 2017), pp. 30-33.

could achieve the same stated objective; and whether there is the possibility of oversight and the availability of review.

1.110 The statement of compatibility states that interception of telecommunications will only be available to the ICAC SA in relation to the investigation of serious offences, and only where a judge or tribunal member has issued a warrant.[249] This assists in the assessment of whether the warrant regime is itself sufficiently circumscribed. However, it does not provide a complete answer as to whether Chapter 2 of the Act (dealing with interception of communications) constitutes a proportionate limit on the right to privacy. In this regard, the statement of compatibility states that any information collected by the ICAC SA may only be used 'for defined purposes and purposes connected with the investigation of serious offences',[250] but does not articulate what those purposes are, meaning the potential breadth of use is not clear. As to how long information may be retained, the statement of compatibility states that communications are destroyed where the chief officer of the agency is satisfied that the record is no longer required for a purpose permitted by the legislation. However, it does not explain what these purposes are, and whether the requirement to destroy records is subject to a mandatory maximum time period, for example. The statement of compatibility also states that persons affected by an interception warrant have relevant judicial avenues through which to challenge the validity of the interception and the use of any intercepted communications. It also states that the ICAC SA is subject to stringent recordkeeping and reporting obligations.[251] However, the safeguard value of these mechanisms is not clear noting, in particular, that judicial avenues for review will be of no use when a person is not made aware that their private communications are subject to interception.

Committee view

1.111 As the committee has noted on numerous occasions, the *Telecommunications (Interception and Access) Act 1979* was enacted prior to the establishment of the committee, and the corresponding requirement that a statement of compatibility with human rights with respect to the Act be drafted.[252] As such, the Act has not, as a whole, been reviewed by the committee for compliance with Australia's human rights obligations. Of those specific powers in the Act that have been reviewed by the committee, the committee notes it has previously raised concerns as to the

249 Statement of compatibility, pp. 4-5.

250 Statement of compatibility, p. 5.

251 These include reporting obligations set out in the *Telecommunications (Interception) Act 2012* (South Australia), which require the regular inspection of records and annual reporting to the Attorney-General.

252 *Human Rights (Parliamentary Scrutiny) Act 2011*, section 8.

compatibility of a number of these powers with human rights, particularly the right to privacy.[253]

1.112 As such, the committee considers that it is not able to conclude that declaring a body to be an interception agency, and thereby able to intercept private communications, constitutes a permissible limit on the right to privacy.

Suggested action

1.113 The committee recommends that a foundational assessment of the human rights compatibility of the *Telecommunications (Interception and Access) Act 1979* be conducted by the Attorney-General's Department.

1.114 The committee draws these human rights concerns to the attention of the Attorney-General and the Parliament.

253 See, for example, Parliamentary Joint Committee on Human Rights, *Report 5 of 2022* (20 October 2022), National Anti-Corruption Commission Bill 2022 and National Anti-Corruption Commission (Consequential and Transitional Provisions) Bill 2022, pp 7-31.