Chapter 2
Concluded matters

2.1 The committee considers responses to matters raised previously by the committee.

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

Bills

Identity Verification Services Bill 2023

Identity Verification Services (Consequential Amendments) Bill 2023[2]

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

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

2 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Identity Verification Services Bill 2023, *Report 12 of 2023*; [2023] AUPJCHR 116.

2.3 The committee requested a response from the Attorney-General in relation to the bills in *Report 11 of 2023*.[3]

Background

2.4 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).[4] 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 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.[5]

2.5 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.[6] 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

---

3 Parliamentary Joint Committee on Human Rights, *Report 11 of 2023* (18 October 2023), pp. 15-41.

4 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.

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

6 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.

circumscribed. The committee reiterated its comments when the bills were reintroduced in the subsequent Parliament in 2019.[7]

2.6 It is noted that the identity verification facilities and services (described below in paragraphs [2.7] to [2.13]) 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.[8] 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 financial year.[9] This bill seeks to provide a legislative framework to support the continued operation of these identity verification services.[10]

Identity verification facilities and services

2.7 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.[11] 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.[12] These identity verification facilities and associated services are detailed below.

2.8 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

---

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

8 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?*.

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

10 Explanatory memorandum, p. 3.

11 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.

12 Identity Verification Services Bill 2023, clause 25.

Verification Service[13] and Face Verification Service,[14] which are 1:1 matching services, and the Face Identification Service, which is a 1:many matching service.[15] 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.[16] Each identity verification service is explained in turn.

2.9 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 passport).[17] 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.[18] The comparison must be carried out in accordance with the conditions and any limitations provided for under the participation agreement (see below at paragraph [2.12]).[19] 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'.[20]

2.10 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

---

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

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

15 Identity Verification Services Bill 2023, clause 5.

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

17 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.

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

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

20 Explanatory memorandum, pp. 38–39.

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).[21] 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[22] of an individual or a biometric template derived from such an image;[23] 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 licence or passport.[24] 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.[25] 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.[26]

2.11 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.[27] 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

---

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

22 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)'.

23 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].

24 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.

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

26 Identity Verification Services Bill 2023, clause 5.

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

government authority for the purpose of the comparison and the authority is a party to a participation agreement).[28]

2.12 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.[29] 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.[30] 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 suspended or terminated.[31] 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).[32]

2.13 The Driver Licence database is a database of identification information as well as a system for biometric comparison of facial images.[33] 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.[34] 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.[35] Hosting agreements govern the Driver Licence database and the collection, use and disclosure of identification information in the database.[36] A hosting agreement is an agreement between the department and each state or territory authority that supplies identification information to the department

---

28 Identity Verification Services Bill 2023, clause 18.

29 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.

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

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

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

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

34 Identity Verification Services Bill 2023, clause 5.

35 Explanatory memorandum, [131].

36 Identity Verification Services Bill 2023, clause 13.

for inclusion in the database.[37] 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.[38] 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).[39]

2.14 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.[40] 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 identity verification services or supporting facilities; or developing, operating or maintaining the Driver Licence database.[41]

2.15 The bill also sets out when protected information can be recorded, disclosed or accessed by entrusted persons.[42] 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.[43] 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.[44] 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.[45] Other circumstances in which an entrusted person would be authorised to make a record of, disclose or access

---

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

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

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

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

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

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

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

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

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

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.[46]

2.16 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.[47] The bill would also permit the automated disclosure of personal information to a person participating in the such services.[48]

Summary of initial assessment

Preliminary international human rights legal advice

Right to privacy

2.17 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.[49]

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.[50] The type of information protected includes

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

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

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

49 Statement of compatibility, pp. 8 and 16.

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

substantive information contained in communications as well as metadata.[51] *Right to social security*

2.18 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.[52] 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.[53] 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.

2.19 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).

2.20 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 unemployment, insufficient family support or unaffordable health care. 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'.[54] 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

---

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

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

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

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

privacy.[55] 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'.[56]

Right to equality and non-discrimination

2.21 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.[57] 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.[58] 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).[59] In this way, the Driver Licence database would allow for a broader range of persons to verify their identity through the identity verification services.[60]

2.22 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.[61] 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 rights).[62] Indirect discrimination occurs where 'a rule or measure that is neutral at face value or without intent to

---

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

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

57 Statement of compatibility, p. 7.

58 Statement of compatibility, p. 7.

59 Statement of compatibility, p. 7.

60 Statement of compatibility, p. 7.

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

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

discriminate' exclusively or disproportionately affects people with a particular protected attribute.[63]

2.23 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'.[64] 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).[65] 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).[66] 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.[67] 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'.[68] 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'.[69]

2.24 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

---

63 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].

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

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

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

67 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].

68 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].

69 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].

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.[70] 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.[71] Where a measure impacts on a particular group disproportionately it establishes prima facie that there may be indirect discrimination.[72]

Right to an effective remedy

2.25 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.[73] 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 data protection bodies.[74]

2.26 The rights to privacy, social security and equality and non-discrimination may generally be subject to permissible limitations where the limitation pursues a

---

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

71 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.

72 *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).

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

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

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), states parties must comply with the fundamental obligation to provide a remedy that is effective.[75]

Committee's initial view

2.27 The committee considered that further information was required to assess the compatibility of the measures with these rights and as such sought the advice of the Attorney-General (as set out in the Attorney-General's response below).

2.28 The full initial analysis is set out in *Report 11 of 2023*.

Acting Attorney-General's response[76]

2.29 The Acting Attorney-General advised:

> **(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**
>
> The identity verification services are a critical tool in protecting governments and industry from the harms of identity crime, and preventing nefarious actor from benefiting from identity theft and fraud.
>
> The importance of the service, in particular the Document Verification Service (DVS), to preventing identity crime is discussed further in a Privacy Impact Assessment undertaken to support the expansion of the DVS for private sector use:
>
> > A significant proportion of identity crime is facilitated by use of stolen, counterfeit or fraudulently obtained identity documents (e.g. documents obtained by using false or stolen information). Available information on the nature and extent of data breaches, together with the cost of fraudulent identity documents, indicates that these documents and/or the information needed to fraudulent manufacture or acquire them are readily available to criminals.
> >
> > The DYS plays an impo1tant role in preventing identity crime by ensuring that the veracity of information on identity documents can be confirmed directly and securely with the document issuing agency. Documents that have been reported stolen, have been cancelled or have expired cannot be successfully verified (returning an 'No' response)

---

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

76 The Attorney-General's response to the committee's inquiries was received on 6 November 2023. This is an extract of the response. The response is available in full on the committee's webpage.

For this reason, the DVS is used to satisfy the identity proofing standard when making a claim for social security payment through Services Australia. The standard involves identity confirmation and verification as provided by section 8 of the *Social Security (Administration) Act 1999* (Cth). In May 2023, almost 90,000 documents were successfully verified by Services Australia through the Document Verification Service for social security payment purposes.

(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

The provision of consent to the collection, use and disclosure of identification information at the initial point of collection by government authorities or creation of an identity document (for example, when an individual applies for a passport) is subject to relevant The IVS Bill requires entities to obtain an individual's consent to the collection, use and disclosure of identification information that relates to the individual, for the purposes of requesting identity verification services, (subclause 9(2)(b)).

When obtaining consent, entities must notify individuals of ce1tain matters (subclause 9(3)). This supports a person to provide informed consent, after considering key matters, including:

- how the entity seeking consent uses identity verification services and how any facial images collected by that entity for the purpose of making a request for services will be used and disposed of (subclause 9(3)(a) and (b)
- whether facial images will be retained for any other purposes (subclause 9(3)(c))
- what legal obligations the entity seeking to collect identification information has in relation to that collection, what rights an individual has and what the consequences of declining to give consent are (subclause 9(3)(d), (e) and (f)), and
- where the individual can get information about making complaints (subclause 9(3)(d)), and where the individual can get information about the operation and management of the approved identification verification facilities (subclause 9(3)(h)).

To clarify, it is not technically possibly or authorised under the IVS Bill for identification information to be stored on the identity verification services. The services do not act as databases. Instead, the services facilitate the comparison of information on a person's identification document against government records held by the issuing agency rather than within the services.

Identity verification through the DYS and Face Verification Service (FVS) is almost instant, with an average response time of under 1 second. The services only provide a response indicating that there is or is not a match, and will not return any identification information as part of the result.

Therefore, the concerns about withdrawal of consent do not arise and the services do not hold any identification information that would need to be removed if consent is withdrawn.

(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)

Consent requirements for the NDLFRS have been agreed with states and territories and are reflected in the Intergovernmental Agreement on Identity Matching Services (IGA):

> When individuals apply for new or renewed driver licences (or any other documents containing facial images to be used in the National Driver Licence Facial Recognition Solution) Road Agencies (or other relevant licensing agency) will take all reasonable steps to notify these applicants that the personal and sensitive information being collected by the Road Agency may be disclosed for the purposes of biometric matching through the National Driver Licence Facial Recognition Solution for law enforcement, national security and other purposes.

Furthermore, subclause l 3(3)(a) requires state and territory authorities that are party to a National Driver Licence Facial Recognition Solution (NDLFRS) hosting agreement to take reasonable steps to inform each individual that their personal information on a driver's licence has been uploaded onto the NDLFRS.

(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

'Reasonable steps' in the context of subparagraph 13(3)(a) and for the purposes of the IGA will vary depending on the nature of operations in each state and territory. States and territories that have uploaded their jurisdictions' data to the NDLFRS have undertaken a privacy impact assessment which, amongst other things, considered existing arrangements for notifying individuals.[77] The Government understands that some jurisdictions have amended privacy statements and provide further advice and guidance on government websites to inform individuals that information on their licence will be uploaded onto the NDLFRS.

---

[77] For example, see Privacy Impact Assessment – VicRoads participation in the National Driver Licence Facial Recognition Solution and Response to the Privacy Impact Assessment of VicRoads' participation in the National Driver Licence Facial Recognition Solution

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

This is not covered by the IVS Bill; which only seeks to regulate the operation of the identity verification services. It does not seek to regulate the use of biometric verification in order to access government services.

To assist the Committee, the following information can be provided.

- Biometric verification is not required to receive a government service from Services Australia, including services provided through Centrelink, obtaining a Medicare Card, and Child Support.
- To receive most Centrelink payments, Services Australia requires individuals to prove who they are by providing documents including an acceptable photo identity document to make a visual comparison of facial features. This facial check is undertaken in person at a service centre or using video chat and is not equivalent to facial biometric verification.
- A strong myGovID includes a biometric verification, currently using an Australian Passport photo, is an option available to individuals wishing to prove who they are to Services Australia, and meets the identity standard for Centrelink payments.

(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

This is not covered by the IVS Bill, which only seeks to regulate the operation of the identity verification services. It does not seek to regulate the use of biometric verification in order to access government services.

To assist the Committee, the following information can be provided.

- Services Australia has alternative methods of identity confirmation for customers who do not want to use a digital identity or consent to a biometric check. This includes avenues to support people who have genuine difficulty proving their identity.
- The alternative identity assessment consists of a series of knowledge based questions, to be answered by the customer, to prove their identity and gain access to a payment or service.
- A person accessing services or payments on the basis of an alternative identity assessment may be asked to verify their identity information periodically. Alternatively, a customer may present to a service centre, with their identity documents, to confirm their identity without use of a biometric check.
- A myGov account linked to a strong digital identity is considered more secure for authentication purposes and will help keep the account

holder's personal information secure, however a myGov account does not require any digital identity (strong or otherwise).

(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

Customers who have not provided consent and successfully undertake the alternative identity assessment have the same level of access to payments and services as customers who have provided consent and met the required identity standard. Declining consent does not restrict access to Centrelink, Medicare or Child Support payments and services.

(h) with respect to informing individuals about data breaches, how will the threshold 'reasonably likely to result in serious harm' 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')

The requirement at subclause 13(3)(c) is intended to align with, and be read in a manner consist with, requirements under the Notifiable Data Breach Scheme under Part IIIC of the *Privacy Act 1988* (Cth).

The Notifiable Data Breach Scheme requires an organisation or agency to notify affected individuals and the Office of the Australian Information Commissioner about an eligible data breach. An eligible data breach occurs when there is unauthorised access or disclosure of personal information, or a loss of that information, and this is likely to result in serious harm to one or more individuals. The reason that an organisation or agency would be required to report a data breach is that they have not been able to prevent the likely risk of serious harm with remedial action. This threshold was established in 2018 in an attempt to balance the need to know against unnecessary notifications to individuals that might raise the risk of notification fatigue.

Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's position. Similar to the Privacy Act, 'reasonable' and 'reasonably' are not defined in the IVS Bill and the term bears the ordinary meaning. What is reasonable can be influenced by current standards and practices. 'Serious harm' is not defined in the Privacy Act or IVS Bill, but in the context of a data breach, may include serious physical, psychological, emotional, financial, or reputational harm.

Similar to the NDB scheme, entities should assess the risk of serious harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the 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

The IVS Bill provides legislative authority for the department to collect, use and disclose identification information that has been communicated to an approved identity verification service, or generated using the NDLFRS. Authority for the department to disclose identification information (subclause 28(1)) is limited to the purposes listed in subclause 27(2). The disclosure of information in these circumstances is appropriate and necessary as it reflects the department's role in facilitating the operation of, and supporting the making of requests for, the identity verification services.

Subclause 30(3) allows departmental officers and other entrusted persons to disclose protected information where:

- the conduct is authorised by a law of the Commonwealth or of a state or territory, or
- the conduct is in compliance with a requirement under a law of the Commonwealth or of a state or territory.

For example, these exceptions may enable the disclosure of protected information in response to a court where information is requested by subpoena, or in response to a search warrant obtained by a law enforcement agency.

Clauses 31, 32, 33, 34, and 35 of the IVS Bill also permit departmental officers and other entrusted persons to disclose protected information (including identification information) in the following circumstances:

- they were performing their functions or duties or exercising a power related to an approved identity verification facility (for example, this could include a departmental officer disclosing information under a request for a person's own information under the *Freedom of Information Act 1982* or Australian Privacy Principle 12)
- they reasonably believed that it is necessary to prevent a serious or imminent threat to the health or life of a person and the disclosure was made for the purpose of preventing or lessening that threat (for example, this may include circumstances where it is unreasonable or impracticable to obtain the consent of the individual whose health or safety is threatened to the disclosure given the imminence of the threat)
- they were disclosing protected information to an IGIS official for the purpose of the IGIS official exercising a power, or performing a duty, as an IGIS official
- they were disclosing protected information to an Ombudsman official for the purpose of the Ombudsman official exercising a power, or performing a function or duty, as an Ombudsman official

- they had obtained the consent of the person to whom the protection information relates, or
- the protected information that was held in, or generated using the NDLFRS, was supplied by an authority of a state or territory, and that authority has consented to the recording, disclosure, or access.

The IVS Bill also limits the information that is provided in response to a request for identity verification through the identity verification services. In particular, subclause 15(1)(g) and subclause 19(d) ensure that the outcome of a DVS and FVS comparison is communicated to the requesting entity as either a match or not. This ensures that personal information is not communicated back to the entity in response to an identity verification request.

(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

In order for the department to disclose protected information to a law enforcement agency, an exception to the offences in clause 30 must apply. Subclause 30(3) establishes exceptions to these criminal offences where

- the conduct is authorised by a law of the Commonwealth or of a state or territory, or
- the conduct is in compliance with a requirement under a law of the Commonwealth or of a state or territory.

Entrusted persons may rely upon these exceptions to disclose protected information (including identification information) to law enforcement agencies. For example, subclause 30(3)(6) would allow entrusted persons to disclose information to law enforcement officers in response to a search warrant obtained under section 3E of the *Crimes Act 1914* (Cth).

In such circumstances, safeguards and protections will be provided by the relevant law that triggers the exception at subclause 30(3). For example, the approval and execution of a section 3E search warrant is subject to safeguards and limitations in the Crimes Act, ensuring proportionate limitations on the right to privacy.

Subclause 35(2) of the IVS Bill provides that an entrusted person may make a record of, disclose, or access protected information that was held in, or generated using the NDLFRS. This provision may be relied upon to support disclosures to law enforcement agencies. However, such disclosure must be with the consent of the relevant jurisdiction that has responsibility for the data supplied to the NDLFRS. The requirement for consent ensures that any limitation on the right to privacy is proportionate and appropriate.

(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

In relation to the NDLFRS, a range of measures and capabilities have been built into the system that are aimed at minimising the risk and impact of false negative and false positive matches, including: access policies, system design and testing (including biometric matching threshold testing). Relevant states and territories have also been engaged to ensure that the face recognition engine in the NDLFRS is workable and appropriate against their jurisdiction's data sets.

When fulfilling a request for the identity verification services, the matching or comparison of information on an identification document occurs at the data source. For this reason, the Attorney-General's Department continues to work with states and territories to ensure the comparison or matching process aligns with best practices, including those provided by the National Institute of Standards and Technology and advice from other government agencies.

Furthermore, the annual report for the IVS Bill will include information about the accuracy of the systems for biometric comparison of facial images that are operated by the Department, which will be the NDLFRS, or the Department administering the *Australian Passports Act 2005* (Cth), for the purposes of providing identity verification services.

(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

The identification verification facilities operate subject to safeguards, limitations and oversight arrangements to mitigate the risk of data breaches and protect the privacy of Australians. This includes the use of encryption and other arrangements to maintain the security of electronic communications to and from the facilities (clause 25), information held in the NDLFRS (subclause 13(4)), and limitations on the collection of information for the purposes of operating the facilities in the IVS Bill.

The Department has a number of existing measures in place to protect the security of the identity verification services. These include:

- entry into the system (built to PROTECTED standards) is controlled through a Secure Internet Gateway that authorises traffic from approved IP sources and inspects all data traffic to block threats based on real-time intelligence.

- the internal system elements are segregated and communication between environments is prohibited
- all communications and databases are encrypted using ASD Approved Cryptographic Algorithms.
- access to the system is strictly controlled, with all users and administrators required to have individual accounts that undergo strong authentication protocols
- automated real-time security scanning for vulnerabilities to continuously mitigate any emerging threats.

(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

The length of time an individual's data is held in the NDLFRS will be a matter for road agencies in each state and territory.

Information in the NDLFRS is deleted on instruction from the jurisdiction's road agency. Where identification information (a drivers licence) is deleted from a jurisdiction's road agency data, it is also removed from the NDLFRS. Similarly, where an individual is provided with a new licence or photo, the relevant jurisdiction's road agency will update its records with the new identification information, and this information will then be replaced on the NDLFRS.

(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

As stated in the Statement of Compatibility with Human Rights, it is the Government's view that the IVS Bill will have a positive impact on the right to social security by ensuring individuals can more easily and securely verify their identity when seeking access to welfare payments and other benefits. Similarly, the IVS Bill promotes the right to equality and non-discrimination by facilitating the biometric verification of identity using information on licences uploaded on the NDLFRS and, in doing so, support more Australians to securely access critical services.

However, the Government notes the concerns raised by the Committee at paragraph 1. 72. There are a number of safeguards in the IVS Bill and non-legislative policies in-place to promote the rights to social security and equality and non-discrimination, and ensure any perceived limitation is proportionate:

For non-legislative safeguards, see responses to (f) for alternative options for establishing a myGov account and access government services and (k) for safeguards in place to mitigate the risk of data verification errors.

Relevant safeguards in the IVS Bill include:

- the requirement to obtain consent (subclause 9(2)(b) and 3)) which is discussed further in response to (b)
- the requirement for requesting entities to conduct privacy impact assessments[78] in relation to requesting identity verification services (subclause 9(2)(a))
- requesting entities must establish and maintain a mechanism to deal with complaints from individuals whose identification information is held by the entity (subclause 9(2)(d))
- state and territory government authorities must have a means for dealing with complaints by individuals relating to their information on the NDLFRS (subclause 13(3)(d)), and
- other relevant Commonwealth, state and territory complaints handling mechanisms will continue to be available, including those provided by the Commonwealth Ombudsman and the OAIC under section 36 of the Privacy Act.

Concluding comments

International human rights legal advice

Legitimate objective and rational connection

2.30 As noted in the initial analysis, 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, noting the Parliamentary Joint Committee on Human Rights' previous concerns regarding the absence of a federal legislative framework governing the identity verification services,[79] insofar as the bills provide a federal legislative framework to support the operation of the services, the measures appear to be necessary to the extent that they address a legislative gap.[80]

---

78 The IVS Bill defines privacy impact assessment to have the same meaning as in subsection 33D(3) of the Privacy Act. A number of privacy impact assessments have been undertaken for the identity verification services and the NDLFRS, which can be found at www.idmatch.gov.au/privacy-security/privacy-impact-assessments.

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

80 In the inquiry into these bills by the Senate Legal and Constitutional Affairs Committee, several submitters have raised concerns regarding the lack of federal legislative basis for existing identity verification facilities and services and queried their lawfulness. See, e.g. Human Technology Institute, *Submission 4*, p. 6; Digital Rights Watch, *Submission 9*, p. 2; Human Rights Law Centre, *Submission 10*, p. 2; Law Council of Australia, *Submission 12*, p. 1.

2.31 Under international human rights law, it must also be demonstrated that any limitation on a right has a rational connection to (that is, effective to achieve) the stated objective. While the initial analysis noted that the measures may be effective in facilitating the efficient provision of services, further information was sought regarding how the measures would be effective in preventing identity theft and fraud, and social security fraud and misuse of government funds.

2.32 The Acting Attorney-General advised that the identity verification services are a critical tool in protecting governments and industry from the harms of identity crime and preventing identity theft and fraud. For example, the Acting Attorney-General stated that the Document Verification Service ensures the veracity of information on identity documents can be confirmed directly and securely and documents that have been reported stolen, cancelled or expired cannot be successfully verified. With respect to preventing social security fraud and misuse of government funds, the Acting Attorney-General advised that the Document Verification Service is used to verify and confirm identity when individuals are making a claim for social security payments.

2.33 By assisting government agencies and private sector entities to more accurately verify an individual's identity, the measures appear to be rationally connected to the stated objectives of preventing identity theft and fraud, as it is less likely that an individual will be able to use a stolen or fraudulent identity document to access services or benefits that they are not entitled to receive.[81]

2.34 The initial analysis noted the risks of data breaches and misuse of information with respect to large datasets and queried whether the effectiveness of the measures may be undermined by such risks.[82] The Acting Attorney-General stated that the risk

---

81 It is noted that more generally, human rights concerns have been raised in the context of using digital technologies to prevent social security fraud. 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'. See UN Human Rights Council, *Report of the Special Rapporteur on extreme poverty and human rights*, A/74/493 (2019) [64].

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

of data breaches is mitigated by the safeguards and oversight arrangements accompanying the measures. Such measures include: encrypting all communications and databases using ASD Approved Cryptographic Algorithms; controlling access to the services through a secure internet gateway; segregating internal system elements and prohibiting communication between environments; strictly controlling access to the services through strong authentication protocols; and automated real-time security scanning for vulnerabilities and threats to the system. These safeguards appear to mitigate the risk of data breaches and misuse of information, although noting that such risks can never be completely removed.

Proportionality

2.35 With respect to the right to privacy, relevant factors in assessing proportionality include the scope of personal information and the purposes for which the information may be collected, stored, used and shared; and the range of persons authorised to access the information.[83]

2.36 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 [2.9] and [2.10]), which includes an individual's name, address, place or date of birth, age, sex, gender identity or intersex status and facial image.[84] This type of information is particularly sensitive, not only because it includes facial images, which may be used to create biometric templates, but because 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'.[85] Sensitive data should therefore 'enjoy a particularly high level of protection'.[86] As noted above (in paragraph [2.23]), 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).[87]

---

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

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

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

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

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

2.37 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 [2.14]). 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.[88] 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 Licence database to support investigations (as discussed further below at paragraph [2.38]). 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'.[89]

2.38 The bills authorise various persons to access and disclose protected information in certain circumstances, including the department,[90] entrusted persons (which includes APS employees and contractors and employees of foreign governments and public international organisations)[91] and the minister.[92] 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. Use of the Face Identification Service, however, is restricted to officers from a limited group of government agencies, which assists with proportionality.

2.39 As to whom 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

---

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

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

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

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

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

of the official exercising a power, or performing a function or duty.[93] However, other provisions do not specify to whom information may be disclosed.[94] The Acting Attorney-General advised that disclosure of identification information is authorised for specified purposes. For example, departmental officers may disclose protected information for the purposes of performing their functions or duties or exercising a power related to an identity verification facility, such as disclosing information to an individual in response to their request under the *Freedom of Information Act 1982*. The Acting Attorney-General also advised that identification information may be disclosed to law enforcement agencies by entrusted persons if to do so is authorised by, or in compliance with, a Commonwealth, state or territory law, or, with respect to information held in the Driver Licence database, the relevant agency responsible for supplying the information consents to the disclosure. The Acting Attorney-General advised that the safeguards applicable to information disclosed to and used by law enforcement agencies are provided for by the relevant law that authorises the disclosure. For example, if the disclosure of information is in response to a search warrant obtained under the *Crimes Act 1914*, the applicable safeguards are those contained in the *Crimes Act 1914*. With respect to the sharing of information held in the Driver Licence database, the Acting Attorney-General advised that the requirement for consent of the responsible agency ensures that any limitation is proportionate (although, as discussed below, consent of the individual to whom the information relates is not required). While the Acting Attorney-General's response has clarified the circumstances in which personal information may be disclosed to, and used by, law enforcement agencies, questions remain as to the full range of persons who may access and use protected information, noting that some provisions do not specify the authorised recipient of the protected information.

2.40 As to the existence of safeguards, the initial analysis outlined 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, which in themselves will contain several safeguards, 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);

---

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

94 See, e.g. Identity Verification Services Bill 2023, clauses 28 and 31.

- 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.[95]

2.41 The above safeguards, as well as the requirement to publish participation agreements and to terminate an entity's ability to access and use a service for non-compliance with an agreement, would generally assist with proportionality. Whether these safeguards are sufficient in all circumstances, however, will depend on how they operate in practice. In particular, the safeguard value of compliance with privacy legislation will depend on the strength of the legislation itself, noting that it is beyond the scope of this analysis to review the adequacy of all state and territory privacy legislation. With respect to the Privacy Act and the APPs, the Parliamentary Joint Committee on Human Rights has previously said that compliance with this legislation is not a complete answer to concerns about interference with the right to privacy for the purposes of international human rights law. This is because the Privacy Act and the APPs contain a number of exceptions to the prohibition on use or disclosure of personal information for a secondary purpose, including where its use or disclosure is authorised under an Australian Law, which may be a broader exception than permitted in international human rights law. The inadequacy of the Privacy Act in protecting privacy and personal information were also revealed in the 2022 review of the Act (the review). The review made several recommendations to strengthen privacy protections, including requiring that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances, which would involve consideration of a range of factors such as the potential adverse impact or harm to the individual, whether any privacy impact is proportionate to the benefit, and whether there are less intrusive means of achieving the same objective.[96] The government's

---

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

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

recent response to the review agreed to a number of recommendations and agreed in principle with others, such as the recommendation with respect to fair and reasonable handling of personal information.[97] It is noted that a number of submitters to the inquiry into these bills by the Senate Legal and Constitutional Affairs Committee raised concerns regarding the reliance on inadequate safeguards in the Privacy Act to protect individuals' right to privacy in relation to these measures and recommended that the Privacy Act be amended in line with the recommendations of the review prior to the passage of these bills.[98]

2.42 In addition to participation agreements, another key safeguard is the Driver Licence database hosting agreement, which requires parties to be subject to privacy legislation and imposes certain requirements on each state or territory party and the department.[99] State or territory parties must take reasonable steps to inform each individual if their identification information is to be included in the database 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 are 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.

2.43 The initial analysis noted that while the safeguards contained in the hosting agreement would generally assist with proportionality, further information was sought as to what constitutes 'reasonable steps' in the context of informing individuals of their inclusion in the database and why consent from the relevant individual is not required for their driver's licence to be included on the database. The Acting Attorney-General advised that consent requirements for the Driver Licence database have been agreed with states and territories and are reflected in the Intergovernmental Agreement on Identity Matching Services. This Agreement provides that when an individual applies for a new or renewed driver licence, the relevant road agency will take all reasonable steps to notify the applicant that their personal and sensitive information will be collected by the agency and may be disclosed for the purposes of biometric matching through the Driver Licence database for law enforcement, national security and other purposes.

---

97 Australian Government, *Government Response: Privacy Act Review Report*, September 2023, p. 27.

98 In the inquiry into these bills by the Senate Legal and Constitutional Affairs Committee, several submitters have raised concerns regarding the lack of federal legislative basis for existing identity verification facilities and services and queried their lawfulness. See, e.g. Human Technology Institute, *Submission 4*, p. 6; Digital Rights Watch, *Submission 9*, p. 2; Human Rights Law Centre, *Submission 10*, p. 2; Law Council of Australia, *Submission 12*, p. 1.

99 Identity Verification Services Bill 2023, clause 13.

2.44 As to what constitutes 'reasonable steps', the Acting Attorney-General advised that it varies depending on the nature of operations in each state and territory. The Acting Attorney-General noted that the states and territories that have uploaded their jurisdictions' data to the Driver Licence database have undertaken privacy impact assessments, which considered arrangements for notifying individuals, and gave the example of the privacy impact assessment with respect to Victoria. However, this privacy impact assessment states that 'VicRoads will need to give thought as what "reasonable steps" would be' in the case of informing individuals about how their information will be used. It states that the current notice given to individuals in Victoria is broadly worded, notifying individuals that their information may be used for other purposes and disclosed to persons and that the individual is required to provide their personal information as failure to do so may result in their driver licence application form not being processed.[100] VicRoads implemented the recommendation to amend its privacy statements to advise applicants of use and disclosure of personal information for biometric facial matching.[101] The Victorian example suggests that 'reasonable steps' involves notifying an applicant by way of a written notice attached to the application form.

2.45 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 Australian population have a driver's licence).[102] 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.[103]

2.46 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'.[104] In the context of the Driver Licence database, individuals do not have the ability to object

---

100 Information Integrity Solutions, *Privacy Impact Assessment – VicRoads participation in the National Driver Licence Facial Recognition Solution*, December 2018, p. 29

101 VicRoads, *Response to the Privacy Impact Assessment of VicRoads' participation in the National Driver Licence Facial Recognition Solution*, July 2019, p. 5.

102 Statement of compatibility, p. 8.

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

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

to the inclusion of their personal data on the database unless they do not wish to proceed with applying for a driver's licence. In practice, this leaves individuals with no choice regarding how their personal information is used, retained and disclosed. Without a requirement for consent or the ability to object, the requirement to inform individuals of the inclusion of their information on the database appears to offer limited safeguard value.

2.47 As to how long an individual's data would be held in the Driver Licence database, the Acting Attorney-General advised that this is a matter for road agencies in each state and territory. Information deleted or updated on the road agency's database will be similarly deleted or updated on the Driver Licence database. If there was no maximum period of time in which a state or territory road agency was authorised to retain the data, it appears possible for an individual's information to be held indefinitely on 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.[105] 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,[106] and that access to data should be strictly limited solely to fighting serious crime and be subject to prior review by a court

105 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].

106 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].

or independent administrative authority.[107] 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.

2.48 In addition to the safeguards contained in participation agreements and the hosting agreements, the initial analysis identified the following safeguards that would likely assist with proportionality with respect to the right to privacy:

- 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;[108]
- 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;[109]
- the department is required to maintain the security of electronic communications, including by encrypting the information, and protecting it from unauthorised interference or access;[110]
- publication of key agreements, including intergovernmental agreement, participation agreement and the Driver Licence database hosting agreement to be published on the department's website;[111]
- an annual assessment of the operation and management of facilities by the Information Commissioner;[112]
- annual reports that must be tabled in Parliament;[113]

---

107 *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.

108 Statement of compatibility, p. 8.

109 Identity Verification Services Bill 2023, clause 14.

110 Identity Verification Services Bill 2023, clause 25.

111 Identity Verification Services Bill 2023, clause 39.

112 Identity Verification Services Bill 2023, clause 40.

113 Identity Verification Services Bill 2023, clause 41.

- oversight by the Commonwealth Ombudsman;[114] and
- review of the Identity Verification Services Bill 2023 within two years of commencement.[115]

Right to social security

2.49 With respect to the right to social security, the initial analysis identified the availability of alternative methods of identity verification as an important safeguard.[116] The Acting Attorney-General advised that Services Australia has alternative methods of identity confirmation for customers who do not want to use a digital identity or consent to a biometric check. This includes avenues to support people who have genuine difficulty proving their identity. The alternative identity assessment consists of a series of knowledge-based questions to be answered by the customer in order to access the payment or service. If this method is used, the customer may be asked to periodically verify their identity, which may be done by presenting at a service centre to confirm identity without using a biometric verification process. The Acting Attorney-General advised that a strong myGov account requires biometric verification and is considered more secure but is not required to access government services, including Centrelink. A general myGov account does not require any digital identity. The Acting Attorney-General further advised that declining to consent to biometric verification does not restrict access to Centrelink, Medicare or child support payments and services, and customers who have verified their identity via an alternative assessment process have the same level of access to payments and services as customers who have a strong myGov account and have consented to biometric verification.

Right to equality and non-discrimination

2.50 With respect to the right to equality and non-discrimination, the initial analysis emphasised the importance of safeguards accompanying the measures to mitigate the risk of data verification errors and discriminatory decisions based on biased or erroneous data. The Acting Attorney-General advised that access policies, system design and testing (including biometric matching threshold testing) minimise the risk and impact of false negative and false positive matches. The Acting Attorney-General stated that the Attorney-General's Department works with states and territories to ensure the comparison or matching process aligns with best practice, and that the annual report for the bill will include information about the accuracy of the systems for biometric comparison of facial images. These safeguards appear to be rather vague, and it is not clear whether they would be sufficient in practice to mitigate the

---

114 Identity Verification Services Bill 2023, clause 34.

115 Identity Verification Services Bill 2023, clause 43.

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

risk of data verification errors, which, as outlined above, could lead to discriminatory decisions and disproportionately impact certain groups.[117]

Right to an effective remedy

2.51 Finally, with respect to the right to an effective remedy, the initial analysis noted that the following safeguards appear to protect this right:

- 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.

2.52 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.[118] However, the adequacy of these complaint mechanisms will depend on how they operate in practice, noting that the 2022 review of the Privacy Act found that existing avenues available to individuals for a claim for breach of privacy under the Act are limited and recommended the Act be amended to allow for a direct right of action with respect to an interference with privacy.[119]

2.53 Regarding the threshold of 'reasonably likely to result in serious harm' in the context of informing individuals about data breaches, the Acting Attorney-General advised that this threshold is intended to align with the requirements under the Notifiable Data Breach Scheme under the Privacy Act. This scheme requires an organisation or agency to notify an affected individual of an eligible data breach, which occurs when there is unauthorised access or disclosure of personal information that is likely to result in serious harm to an individual. The Acting Attorney-General noted that the threshold under the scheme was established in 2018 in an attempt to balance the need to know against unnecessary notifications to individuals that might raise the risk of notification fatigue. As to whether a breach meets the threshold, the Acting Attorney-General advised that this involves an objective assessment, determined from the viewpoint of a reasonable person in the entity's position. The terms 'reasonably' and 'serious harm' are not defined in the legislation and bear their ordinary meanings.

---

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

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

119 Attorney-General's Department, *Privacy Act Review: Report 2022*, February 2023, pp. 272–279.

In the context of a data breach, serious harm may include serious physical, psychological, emotional, financial or reputational harm.

2.54 Noting that the ordinary meaning of 'serious' is significant, important, grave or of great consequence, the threshold of 'serious harm' could be quite high. Additionally, while the threshold is stated to require an objective assessment, many of the factors are inherently subjective, such as whether a data breach is likely to cause serious psychological, emotional or reputational harm to an individual. Without knowing the personal circumstances of the individual, it appears difficult to accurately assess the likely risk of harm. If the threshold of 'serious harm' is applied too narrowly, there is a risk that individuals will not be sufficiently informed about interferences with their right to privacy, thus denying them the opportunity to make a complaint and potentially pursue a remedy for any violation of their rights. Ensuring legislative consistency with the Notifiable Data Breach Scheme under the Privacy Act does not appear to be an adequate justification for potentially restricting individuals' right to an effective remedy.

Conclusion

2.55 In conclusion, while the measures pursue legitimate objectives for the purposes of international human rights law and are likely rationally connected to these objectives, questions remain as to whether the potential interference with the right to privacy would be proportionate in all circumstances. There are a number of important safeguards that would assist to protect the right to privacy, including those contained in participation agreements and the hosting agreements. 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.[120] However, the adequacy of some of the safeguards will depend on how they operate in practice. It is noted that there is a significant reliance on safeguards contained in state and territory legislation, the Privacy Act as well as other legislation authorising use and disclosure of personal information for the purposes of these measures. Without a comprehensive review of this broader legislative framework, it is not possible to conclude whether the safeguards contained in this other legislation are sufficient to protect the right to privacy for the purposes of international human rights law. Further, the absence of individual consent with respect to inclusion of sensitive information, including facial images, on the Driver Licence database as well as the broad purposes for which the information may be used (including secondary purposes by law enforcement), raises particular concerns with respect to the proportionality of this measure. As such, depending on how the measures operate in practice, there appears to be a risk that they may impermissibly limit the right to privacy and it is not clear that an individual would have access to an

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

effective remedy with respect to any violation of rights, as access to a remedy depends on the individual being notified of the breach.

2.56 With respect to the right to social security, the availability of an alternative method of identity verification mitigates the risk that the measures impermissibly limit this right, as individuals who are unable to complete biometric verification do not appear to be restricted from accessing government services and social security payments.

2.57 With respect to the right to equality and non-discrimination, it is not clear that the measures are accompanied by sufficient safeguards to mitigate the risk of data verification errors that may disproportionately impact certain groups and lead to discriminatory decisions. As such, it is not possible to conclude as to the likely compatibility of the measures with this right.

Committee view

2.58 The committee thanks the Acting Attorney-General for this response. 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 remains 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.

2.59 While the committee considers that the measures pursue legitimate objectives and will likely be effective to achieve these objectives, it remains concerned that the measures may not represent a proportionate limit on the right to privacy. The committee considers that the measures are accompanied by numerous important safeguards, but notes that several of these safeguards are contained in other legislation, including state and territory legislation. Without a comprehensive review of the broader legislative framework governing the identity verification facilities and services, it is not possible to conclude whether the safeguards contained in this other legislation are sufficient to protect the right to privacy for the purposes of international human rights law. The committee therefore considers that, depending on how the measures operate in practice, there remains a risk that the measures may impermissibly limit the right to privacy. If this did occur, it is not clear that an individual would have access to an effective remedy with respect to any violation of rights, as access to a remedy depends on the individual being notified of the breach.

2.60 The Acting Attorney-General's response has satisfied the committee that the availability of an alternative method of identity verification mitigates the risk that the measures impermissibly limit the right to social security. With respect to the right to equality and non-discrimination, the committee considers that it is not clear that the measures are accompanied by sufficient safeguards to mitigate the risk of data

verification errors that may disproportionately impact certain groups (on the basis of racial identity) and lead to discriminatory decisions. As such, the committee is unable to conclude as to the likely compatibility of the measures with this right.

Suggested action

2.61 The committee considers the proportionality of the identity verification framework would be assisted by a comprehensive governmental review of all legislation governing the identity verification facilities and services and National Driver Licence Facial Recognition Solution, particularly state and territory legislation, that considers:

(a) the adequacy of the legislation in protecting the right to privacy, right to equality and non-discrimination and right to an effective remedy;

(b) the length of time an individual's data is held in the Driver Licence database and how long it should be retained;

(c) individual consent with respect to inclusion of sensitive information in such databases;

(d) the breadth of the purposes for which information may be used (including secondary purposes by law enforcement);

(e) if there are sufficient safeguards to mitigate the risk of data verification errors that may disproportionately impact on certain groups;

(f) the full range of persons who may access and use protected information; and

(g) the appropriateness of setting the threshold of 'reasonably likely to result in serious harm' in the context of informing individuals about data breaches.

2.62 The committee recommends that the statement of compatibility be updated to reflect the information provided by the Acting Attorney-General.

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

Legislative instruments

Social Security (Administration) (Public Interest Certificate Guidelines) (DEWR) Determination 2023[121]

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)[122]
Rights	Multiple rights

2.64 The committee requested a response from the minister in relation to the instrument in *Report 11 of 2023*.[123]

Disclosure of personal information in the public interest

2.65 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

121 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Social Security (Administration) (Public Interest Certificate Guidelines) (DEWR) Determination 2023, *Report 12 of 2023*; [2023] AUPJCHR 117.

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

123 Parliamentary Joint Committee on Human Rights, *Report 11 of 2023* (18 October 2023), pp. 52-58.

or class of case. In giving such certificates, the Secretary must act in accordance with guidelines. This legislative instrument sets out those guidelines.[124]

2.66 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 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).[125] 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.[126]

2.67 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;[127]
- the enforcement of a criminal law, or relating to certain offences or threatened offences;[128]
- proceeds of crime orders;[129]
- inquiries relating to a missing or deceased person;[130]
- public housing administration;[131]
- the functions of the Family Responsibilities Commission;[132]

---

124 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].

125 Section 8.

126 Section 6.

127 Section 9.

128 Section 10.

129 Section 11.

130 Sections 12–13.

131 Section 14.

132 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.

- assisting a child protection agency to contact a parent or relative in relation to a child;[133]
- progressing or resolving, where necessary, a matter of relevance to a department that administers any part of the social security or family assistance law;[134] or
- Australian Public Service Code of Conduct investigations.[135]

2.68 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;[136]
- to verify payment qualification;[137] 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.[138]

Summary of initial assessment

Preliminary international human rights legal advice

Multiple rights

2.69 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.

2.70 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.[139] 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.

---

133 Section 17.

134 Section 19.

135 Section 21.

136 Section 24.

137 Section 25.

138 Section 26–27.

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

2.71 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. 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.

2.72 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.[140] The statement of compatibility further states that the measure promotes the rights of the child.[141] 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.

Committee's initial view

2.73 The committee expressed concern that the statement of compatibility accompanying this legislative instrument provides an incomplete and insufficient assessment of the measure, and noted that this was the first opportunity for the committee to consider the compatibility of this measure with human rights in ten years.[142] The committee considered that further information was required to assess the compatibility of this measure with human rights, and sought the advice of the Minister for Employment and Workplace Relations as to the matters set out in the minister's response below.

2.74 The full initial analysis is set out in *Report 11 of 2023*.

---

140 See, Family Responsibilities Commission website.

141 Statement of compatibility, p. 12.

142 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.

Minister's response[143]

2.75 The minister advised:

> **(a) what personal information the department holds and may therefore be disclosed under these grounds**
>
> The Public Interest Certificate Guidelines contained in the Determination (Public Interest Guidelines) defines "information" as follows:
>
> > *information* means information acquired by an officer in the performance of his or her functions or duties, or in the exercise of his or her powers, under the social security law.
>
> This definition is consistent with sub-paragraph (a) of the definition of 'protected information' in the *Social Security Act 1991* (Cth).
>
> The Department of Employment and Workplace Relations is the agency responsible for oversight and administration of employment service programs, including Workforce Australia. The administration of these employment service programs is supported by a network of contracted employment service providers (providers).
>
> In accordance with the *Privacy Act 1988* (Cth), personal information is only collected by the department or providers where it is reasonably necessary for or directly related to the administration of employment service programs, including to provide assistance to individuals participating in those programs, or where otherwise authorised by another legislation, for example, the *Social Security (Administration) Act 1999* (Cth).
>
> Personal information collected by the department or providers may include:
>
> - identifying details, such as name, date or birth and racial/ethnic information;
> - contact details;
> - education history, employment history and activity details;
> - health information; and
> - information relevant to an individual participating in an employment service programs (for example, appointment dates or barriers associated with obtaining employment).
>
> Not all personal information that is requested to be disclosed, is in fact disclosed. The Public Interest Certificate Guidelines specifically provide that only the necessary amount of personal information required to be disclosed, should be disclosed. This has meant that in the majority of cases, only limited information such as individuals' names, dates of birth,

---

143 The minister's response to the committee's inquiries was received on 2 November 2023. This is an extract of the response. The response is available in full on the committee's website.

residential addresses, telephone numbers, rather than the entire files, have been certified for disclosure.

(b) whether each of the grounds for disclosure 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)

The Public Interest Certificate Guidelines include various safeguards to ensure that protected information is only disclosed where the public interest outweighs any limitation on the right to privacy.

All of the purposes for which a Public Interest Certificate can be issued are sufficiently circumscribed in the following ways:

- Section 9 requires it to be established that there is a threat to the life, health or welfare of a person.
- Section 10 only applies to serious criminal offences and civil penalty matters. It does not allow for disclosure in relation to minor criminal offence and civil penalty matters.
- Section 11 is designed to support proceeds of crime regimes so that criminals are not able to retain the proceeds of their criminal activities.
- Sections 12 and 13 require that the decision maker be satisfied that there are no reasonable grounds to believe that the relevant person would object to the disclosure.
- Section 14 is designed to provide a benefit to individuals by supporting those who have applied for, or are tenants in, public housing or other State- or Territory-managed housing.
- Section 15 is designed to provide a benefit to individuals by supporting the work of the Queensland Family Responsibilities Commission in assisting welfare reform communities.
- Section 16 is designed to provide a benefit to individuals by supporting them in receiving reparations to which they may be entitled.
- Section 17 is designed to promote the rights of the child by assisting in contact being made with a parent or relative.
- Section 18 is designed to provide a benefit to individuals by assisting them to obtain concessions for public utilities.
- Section 19 is designed to facilitate the delivery of services by the department and other agencies to income support payment recipients.

- Section 20 is designed to support research and evaluation so that the department can improve the employment services it provides.
- Section 21 is designed to support the investigation of alleged breaches of the Australian Public Service Code of Conduct.
- Section 24 is designed to support the rights of the child by ensuring that they receive appropriate support where they are subject to abuse or violence.
- Section 25 is designed to ensure homeless young persons are able to support themselves if they are not able to live at home.
- Section 26 is designed to assist in the reconciliation between a homeless young person and their parents.
- Section 27 is designed to provide reassurance to parents of a homeless young person whilst not forcing the homeless young person to communicate with their parents if it is against their wishes.

All of the provisions include a requirement that the decision maker be satisfied that the disclosure is necessary for the particular purpose. This serves to limit the disclosure to only that required to meet the particular objective.

Section 23 provides that information about a homeless young person can only be disclosed if that disclosure will not cause them any harm. This ensures that the right to privacy is only limited where there is a benefit to the homeless young person.

The Public Interest Certificate Guidelines include a requirement that the information cannot reasonably be obtained from a source other than the department (sections 8(1)(a) and 23(1)(a)) this ensures that the power can only be used as a last resort and that disclosure can only be authorised where no other less rights restrictive alternative is available.

There are a number of safeguards in place in relation to the disclosure of information under the Public Interest Certificate Guidelines. These include the following:

- While the Privacy Act continues to apply in relation to the handling of protected information that is also personal information as defined in the Privacy Act, the social security law imposes a higher level of protection to such information than is imposed under the Privacy Act. For example, criminal sanctions apply for the unauthorised use or disclosure of information under section 204(1) of the *Social Security (Administration) Act 1999*;
- Public interest certificates made on the basis of the Public Interest Certificate Guidelines are made by the Secretary and her delegates at appropriate levels, and are subject to administrative arrangements which recognise the significance of such decisions;

- In appropriate circumstances, the disclosure of information under the Public Interest Certificate Guidelines may be accompanied by additional measures to further protect the information (e.g. Deeds of confidentiality may be required for recipients of the information); and
- The social security law provides that information provided to a person on the basis of a Public Interest Certificate must be used for the purpose for which it was provided. That recipient is not permitted to further disclose the information to other parties unless the disclosure is for the same purpose or the disclosure is otherwise authorised by law.

(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

The Secretary's authority to issue a public interest certificate is currently exercised by the National Contract Manager for employment services (Senior Executive Service Band 2). This is a senior position and is held by a highly experienced officer. The National Contract Manager is supported by a specialist team of officers and dedicated Provider Leads, who process requests for disclosure. Legal advice is sought in relation to each disclosure request to support them in deciding whether they can be satisfied that all the requirements are met.

Training provided to the specialist team includes:

- mandatory departmental privacy training;
- training on the Privacy Act and information disclosure schemes (delivered by in-house and external lawyers including the Australian Government Solicitor);
- specific Public Interest Certificate training (delivered by an in-house legal team);
- the employment services-specific Information Exchange and Privacy training module (produced by an external legal firm); and
- vicarious trauma training (delivered by an external specialist training provider).

Upon receipt of a request for disclosure, the Secretary or their delegate will consider relevant information available to the department. This includes:

- information held in the department's IT systems regarding the participant, including information provided by Services Australia, such as vulnerability indicators;
- the context in which a request for information is made, or the circumstances leading to the information being requested;

- evidence that obtaining the individual's consent had been attempted (and if not, the reason for not doing so); and
- evidence from the provider regarding their interactions with the individual(s).

(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

The Committee is referred to the response set out in relation to question (c) above.

(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

The Public Interest Certificate Guidelines are compatible with the rights of persons with disabilities under the Convention on the Rights of Persons with Disabilities. There are no particular impacts of the Public Interest Certificate Guidelines on people with disabilities over and above the limitation on the right to privacy that applies to everyone.

Section 6(b) of the Public Interest Certificate Guidelines requires consideration to be given to whether various vulnerabilities, including disability, might limit the information available to the department in relation to an individual's circumstances to inform the decision on issuing a Public Interest Certificate. The decision maker would use the information already available to the department about the individual in determining whether they are unable to give notice of their own circumstances. If it is determined that they may be unable to give notice, this would prompt a more cautious approach to be taken in deciding whether to issue a Public Interest Certificate taking into account the individual's vulnerabilities. This supports the rights of people with disabilities by ensuring that their disability is taken into account in the decision-making process.

(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)

The Statement of Compatibility with Human Rights provided alongside the Public Interest Certificate Guidelines sets out the other rights which are engaged. These include rights under the Convention on the Rights of the Child and the International Convention on Economic, Social and Cultural Rights.

Concluding comments

International human rights legal advice

2.76 The minister advised that the Department of Employment and Workplace Relations (the department), and contracted employment service providers, collect personal information where it is reasonably necessary for, or directly related to, the administration of employment service programs, including to assist participants or where otherwise authorised under other legislation. The minister advised that such personal information may include: identifying details, such as a person's name, date of birth and racial/ethnic information; their contact details; education history, employment history and activity details; health information; and information relevant to an individual participating in an employment service program (for example, appointment dates or barriers associated with obtaining employment). The scope of personal information held by the department is a key factor relevant to the assessment of whether a limitation on the right to privacy is permissible. In this regard, it appears that the department (and contracted employment services providers) hold a wide range of sensitive personal information about individuals.

2.77 Further information was sought as to whether each of the grounds for disclosure[144] would constitute a proportionate limit on the right to privacy. The minister set out some details regarding the purpose for each disclosure power which assists with an assessment of whether each of these bases for disclosure is sufficiently circumscribed. For example, it assists that disclosure pursuant to section 14 is designed to provide a benefit to individuals with respect to public housing. This would appear to indicate that section 14 would not permit the disclosure of personal information where this may disadvantage the individual (for example, to enforce a rental debt). However, in some instances not all circumstances in which information may be disclosed has been included. For example, the minister advised that section 19 is designed to facilitate the delivery of services by the department and other agencies to income support payment recipients. However, section 19 would permit disclosure where necessary to facilitate the progress or resolution of 'a matter of relevance' within the portfolio responsibilities of a department or agency that delivers services or has portfolio responsibilities under the social security law or family assistance law. It is unclear whether, for example, information may be permissibly disclosed on this basis to enforce a social security debt. Further, in some instances the information provided by the minister would appear to simply reflect the words of the provision itself, and so provides no additional explanation as to whether the measure is sufficiently circumscribed. For example, the minister stated that disclosure pursuant to section 9 would require it to be established that there is a threat to the life, health or welfare of a person, but did not explain how this would be established in practice. Further, the minister's response stated that section 21 is designed to support the

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

investigation of alleged breaches of the Australian Public Service Code of Conduct and does not further articulate how and when this ground may be relied on or has been relied on previously.

2.78 With respect to disclosures relating to a young person experiencing homelessness (Part 3 of the guidelines), the minister advised that sections 24-27 are designed to support the rights of the child by ensuring that they receive appropriate support; ensure homeless young persons are able to support themselves; assist in the reconciliation between a homeless young person and their parents; and provide reassurance to parents of a homeless young person while not forcing the homeless young person to communicate with their parents if it is against their wishes. The minister stated that section 23 provides that information about a homeless young person can only be disclosed if that disclosure will not cause them any harm, ensuring that the right to privacy is only limited where there is a benefit to the homeless young person. This may serve as an important constraint, however no information is provided as to how such an assessment is made and whether the views and consent of the young person is sought, such as in relation to whether they wish to reconcile with their parents.

2.79 In terms of the persons to whom any information may be disclosed pursuant to these guidelines, the minister stated that social security law provides that information provided to a person on the basis of a public interest certificate must be used for the purpose for which it was provided, and the recipient may not further disclose the information unless that disclosure is for the same purpose, or is otherwise authorised by law. The minister further stated that the guidelines specifically provide that only the necessary amount of personal information required to be disclosed, should be disclosed. The minister stated that this has meant that in most cases, only limited information is certified for disclosure, such as names, dates of birth, residential addresses and telephone numbers, rather than the entire files. This assists with the proportionality of the measure. However, it does not exclude the possibility that in some cases all personal information held in relation to a person may be disclosed. Noting the scope of information that the minister outlined above, there may be a risk that the measure would facilitate a potentially significant interference with a person's privacy.

2.80 As to the presence of safeguards, the minister advised that the *Privacy Act 1988* (Privacy Act) applies in relation to the handling of personal information, once disclosed, as do secrecy provisions set out in the *Social Security (Administration) Act 1999*. These would operate to help to safeguard the information once disclosed, which assists with proportionality (although it is noted this only applies to the information once disclosed, not to the determination to disclose it). The minister also stated that decisions to issue public interest certificates are made by senior officials and are subject to administrative arrangements which recognise the significance of such decisions. In addition, the minister noted that the disclosure of information under the guidelines may be accompanied by additional measures to further protect the

information (e.g. deeds of confidentiality for recipients). This senior oversight and additional measures assist with the proportionality of the measure.

2.81 As to whether any other, less rights restrictive alternatives could achieve the stated objective, the minister stated that the guidelines include a requirement that the information cannot reasonably be obtained from a source other than the department, meaning that the power can only be used as a last resort and disclosure can only be authorised where no other less rights restrictive alternative is available. However, no information is provided as to whether less rights restrictive alternatives for the individual bases for disclosure would be effective (for example, that a decision maker should consider the right to privacy of a person affected by a disclosure certificate or that an individual must be notified in writing each time personal information about them has been disclosed pursuant to this measure).

2.82 As to 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) the minister advised that the authority to issue a public interest certificate is currently exercised by a member of the Senior Executive Service who is supported by a specialist team of officers who process requests for disclosure. The minister stated that legal advice is sought in relation to each disclosure request and noted that the processing team receive training related to privacy obligations, public interest certificates, and vicarious trauma. This training, particularly the privacy training, may assist in ensuring that information is disclosed in appropriate circumstances. However, noting that vicarious trauma training would appear to relate to a risk of trauma to staff themselves rather than to affected individuals it remains unclear if staff would be well-equipped to determine if the disclosure of information may, for example, result in harm to a homeless young person.[145] The minister stated that on receipt of a request for disclosure, the Secretary or their delegate will consider relevant information available to the department, including: information held in the department's systems regarding the participant, including information provided by Services Australia, such as vulnerability indicators; the context in which a request for information is made, or the circumstances leading to the information being requested; evidence that obtaining the individual's consent had been attempted (and if not, the reason for not doing so); and evidence from the provider regarding their interactions with the individual. These factors may assist in the proportionality of the measure, particularly evidence that obtaining the consent of an individual has been attempted or was otherwise not possible, and information relating to vulnerabilities that a person may experience. However, no information has been provided as to if the staff assessing whether to disclose information pursuant to the public interest guidelines would themselves endeavour to contact the affected person at the point at which a decision would be

[145] See paragraph 23(1)(b) of the Social Security (Administration) (Public Interest Certificate Guidelines) (DEWR) Determination 2023.

made. If staff do not contact the affected person, there may, in some circumstances, be a risk that the information these staff rely on may be out of date or be otherwise inaccurate.

2.83 In conclusion, based on the minister's advice it appears likely that in most instances disclosure pursuant to a public interest certificate would constitute a proportionate limit on the right to privacy, noting the presence of relevant safeguards and the restricted circumstances in which information may be disclosed. However, much would depend on whether the right to privacy was fully considered by the decision-maker when disclosing the information.

Rights of people with disability

2.84 In relation to the rights of persons with disability, section 6 requires that in giving a public interest certificate, the Secretary must have regard to 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. The minister stated that in determining whether a person is unable to give notice of their own circumstances a decision maker would use the information already available to the department about the individual. The minister stated that if it is determined that a person may be unable to give notice themselves of their circumstances, this would prompt a more cautious approach to be taken in deciding whether to issue a public interest certificate, taking into account the individual's vulnerabilities. The minister stated that this supports the rights of persons with disability by ensuring that their disability is taken into account in the decision-making process. However, section 8 provides that a public interest certificate may be given if the information to be disclosed cannot reasonably be obtained from a source other than the department.[146] In requiring the decision maker to have regard to a person's disability when considering whether a person may be unable to give notice of their own circumstances, this suggests that the decision maker could consider a person's inability to give such a notice as a reason to grant a certificate to disclose the information on the person's behalf. It does not currently read that the Secretary should have regard to a person's vulnerabilities as a reason for *not* granting the certificate. If this is the intention behind section 6 it should be redrafted to give effect to this intention and to ensure that it is not used as a basis for granting a certificate on behalf of a person with disability.

2.85 In this regard it is noted that the rights of persons with disability include the right to equal recognition before the law. This includes the right to enjoy legal capacity on an equal basis with others in all aspects of life, and in all measures that relate to the exercise of legal capacity, there should be appropriate and effective safeguards to prevent abuse.[147] The UN Committee on the Rights of Persons with Disabilities has made clear that practices that deny the right of people with disabilities to legal

---

146 Paragraph 8(1)(a).

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

capacity in a discriminatory manner, such as substitute decision-making regimes, are contrary to article 12 and must be 'abolished in order to ensure that full legal capacity is restored to persons with disabilities on an equal basis with others'.[148] It is not clear that section 6, as currently drafted, would comply with this requirement, noting that it appears that the Secretary or delegate could take into account a person's disability as a reason to grant a public interest certificate of disclosure without recognising their right to equal recognition before the law.

Engagement of other rights

2.86 Further information was also sought as to 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). The minister stated that the statement of compatibility 'sets out the other rights which are engaged [including] rights under the Convention on the Rights of the Child and the International Convention on Economic, Social and Cultural Rights'. However, further information was sought because the information set out in the statement of compatibility is incomplete and insufficient. As noted, 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.[149] However, because of the limited information in the explanatory materials, the extent of this potential impact was not clear. Further, the statement of compatibility does not identify the ways in which the measure may limit the rights of children, including the rights of children experiencing homelessness, and does not 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. As such, it is not possible to conclude whether any limitation on further human rights, including the rights of the child, would constitute a permissible limitation.

Committee view

2.87 The committee thanks the minister for this response. Based on the information provided by the minister, the committee considers that some of the

---

148 Committee on the Rights of Persons with Disabilities, *General comment No. 1 – Article 12: Equal recognition before the law* (2014) [7]. For a discussion of the academic debate regarding the interpretation and application of article 12, particularly in relation to substitute decision-making, see, eg, Bernadette McSherry and Lisa Waddington, 'Treat with care: the right to informed consent for medical treatment of persons with mental impairments in Australia', *Australian Journal of Human Rights*, vol. 23, issue no. 1, pp. 109–129.

149 The Commission operates in Aurukun, Coen, Doomadgee, Hope Vale and Mossman Gorge in Queensland. For example, in Doomadgee Aboriginal and Torres Strait Islander people make up almost 90 per cent of the population, see ABS 2021 QuickStats Census for Doomadgee.

grounds for disclosure pursuant to a public interest certificate may constitute a proportionate limit on the right to privacy, noting the presence of relevant safeguards and the restricted circumstances in which information may be disclosed. However, the committee notes that a wide range of sensitive personal information could be disclosed pursuant to this certificate and there is no legislative requirement that a decision maker consider the right to privacy before issuing a public interest certificate. As such, the committee is concerned that there may be some risk that this disclosure power could be exercised in circumstances that do not constitute a proportionate limit on the right to privacy.

2.88 In relation to the rights of persons with disability, the committee notes the minister's advice that a decision maker would treat a person's vulnerabilities as a reason for taking a more cautious approach in granting a public interest certificate. The committee welcomes this approach, however, notes that the legislative instrument is not drafted in this way but would allow a decision maker to take into account a person's vulnerabilities, including any disability, as a basis *for* granting a public interest certificate. If a person's disability and purported inability to give notice of their circumstances were to be used as a basis for issuing a certificate, without regard to the person's right to enjoy legal capacity on an equal basis with others, this is likely to be incompatible with the rights of persons with disability.

2.89 The committee also notes that insufficient information has been provided to fully determine whether the measure permissibly limits other rights such as the right to equality and non-discrimination and the rights of the child.

2.90 The committee reiterates its concern that the statement of compatibility accompanying this legislative instrument provides an incomplete and insufficient assessment of the measure. As the committee has consistently advised, 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.[150]

Suggested action

2.91 The committee considers that the proportionality of the measure may be assisted were the instrument amended to:

(a) provide that in giving a public interest certificate the Secretary must have regard to how much the privacy of any person would likely be interfered with by granting the certificate, and whether the grant of the certificate is proportionate to the purpose of the disclosure;

(b) clarify in section 6 that if a person is identified as having particular vulnerabilities, including that they are a person with disability, this

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

prompts a more cautious approach in deciding whether to issue a public interest certificate taking into account their vulnerabilities, and is not a ground that could result in a certificate being granted; and

(c) provide that an individual must be notified in writing each time personal information about them has been disclosed pursuant to a public interest certificate.

2.92 The committee recommends that the statement of compatibility be updated to reflect the information provided by the minister.

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

Social Security (Remote Engagement Program Payment) Determination 2023[151]

FRL No.	F2023L01003
Purpose	This instrument determines the arrangement that is the remote engagement program; the part of that program that is a remote engagement placement; and the rate of payment of a remote engagement program payment
Portfolio	Employment and Workplace Relations
Authorising legislation	*Social Security Act 1991*
Disallowance	15 sitting days after tabling (tabled in the House of Representatives and Senate on 31 July 2023).
Rights	Adequate standard of living; equality and non-discrimination; just and favourable conditions of work; social security; work

2.94 The committee requested a response from the minister in relation to the instrument in *Report 10 of 2023*.[152]

Remote engagement program

2.95 The *Social Security Legislation Amendment (Remote Engagement Program) Act 2021*[153] amended the *Social Security Act 1991* (Social Security Act) to establish a new supplementary payment under the remote engagement program for people in remote areas receiving a qualifying remote income support payment, which includes JobSeeker Payment, Youth Allowance, Parenting Payment and Disability Support Pension (DSP).[154] To qualify for the remote engagement program payment, a person receiving a qualifying remote income support payment must receive employment services from a remote engagement program provider; voluntarily participate in a remote engagement placement for between 15 and 18 hours per week; and satisfy any other qualification requirements determined by the minister by legislative

---

151 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Social Security (Remote Engagement Program Payment) Determination 2023, *Report 11 of 2023*; [2023] AUPJCHR 118.

152 Parliamentary Joint Committee on Human Rights, *Report 10 of 2023* (13 September 2023), pp. 5-18.

153 The Parliamentary Joint Committee on Human Rights considered the Social Security Legislation Amendment (Remote Engagement Program) Bill 2021 in its *Report 11 of 2021* (16 September 2021, pp. 42–53.

154 *Social Security Act 1991*, sections 661A and 661B.

instrument.[155] The minister may, by legislative instrument, determine an arrangement to be the remote engagement program and a part of the remote engagement program to be a remote engagement placement under the program, as well as determine the rate of the remote engagement program payment (being not less than $100 and not more than $190).[156] This instrument determines these matters.

2.96 In particular, the instrument determines the arrangements set out in Part G of Annexure 1 (the Annexure) to the Head Agreement for the Community Development Program 2019-2024 between the Commonwealth and Paupiyala Tjarutja Aboriginal Corporation and the Commonwealth and Ngaanyatjarra Council (Aboriginal Corporation) (the Agreements), as the remote engagement program.[157] The remote engagement program (REP) placements are specified as the REP Placements set out in the Annexure to the Agreements.[158] The Annexure details the REP Trial Services the remote engagement program provider must deliver.[159] Section 7 of the Annexure appears to most directly relate to REP Placements.[160] Paragraph 7.1(b) of the Annexure sets out the features of 'REP Placements', primarily by reference to what REP Placements should and should not be. For example, REP Placements do not create an employment relationship between participants and the provider, are voluntary for REP participants, and participants must participate in the placement for at least 15 hours per week but not more than 8 hours per day.[161] Additionally, the determined rate of payment per fortnight is $190.

Summary of initial assessment

Preliminary international human rights legal advice

Right to adequate standard of living; equality and non-discrimination; just and favourable conditions of work; social security; work

Rights potentially promoted

2.97 To the extent that the measure provides opportunities for job seekers to develop employment skills with the aim of obtaining paid employment, it may promote the right to work. 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

---

155 *Social Security Act 1991*, sections 661A and 661B.

156 *Social Security Act 1991*, subsections 661A(2) and 661E(2).

157 Section 5. Part G of Annexure 1 to the Head Agreement for the Community Development Program 2019-2024 is available on the National Indigenous Australians Agency website.

158 Section 6.

159 Annexure, section 2.

160 It is noted that neither the instrument nor the explanatory materials specify which section of the Annexure specifically relates to a REP Placement. Section 7 of the Annexure appears to be most directly relevant.

161 Paragraph 7.1(b). Section 7 more generally relates to REP Placements and includes responsibilities of providers.

work.[162] The right to work also requires states to provide a system of protection guaranteeing access to employment, including 'technical and vocational guidance and training programs, policies and techniques to achieve steady economic, social and cultural development and productive employment'.[163] This right must be made available in a non-discriminatory way.[164] The statement of compatibility states that the measure, by facilitating the remote engagement program payment, promotes the right to work by strengthening existing incentives for remote jobseekers to actively engage with Commonwealth employment programs, which in turn will improve their skills and assist jobseekers to transition to, and remain in, paid work in the open labour market.[165]

2.98 Insofar as the measure facilitates the payment of a supplementary social security payment, thereby increasing the amount of social security benefits payable to those who participate in the remote engagement program, it may also promote the rights to social security and an adequate standard of living. The statement of compatibility acknowledges this and notes that the additional payment will allow participants to improve their standard of living while building skills and experience to support them to find a job and contribute to their community.[166] 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, particularly the rights to an adequate standard of living and health.[167] Social security benefits must be adequate in amount and duration.[168] States must also have regard to the principles of human dignity and non-discrimination, so as to avoid any adverse effect on the levels of benefits and the form in which they are provided.[169] The right to an adequate standard of living requires Australia to take steps to ensure the availability, adequacy and accessibility of food, clothing, water and housing for all people in Australia, and also imposes on Australia the obligations listed above in relation to the right to social security.[170] Further, under the Convention on the Rights

---

162 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].

163 International Covenant on Economic, Social and Cultural Rights, article 6(2).

164 International Covenant on Economic, Social and Cultural Rights, articles 6 and 2(1).

165 Statement of compatibility, p. 7.

166 Statement of compatibility, p. 7.

167 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).

168 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The Right to Social Security* (2008) [22].

169 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The Right to Social Security* (2008) [22].

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

of the Child, children have the right to benefit from social security and to a standard of living adequate for a child's physical, mental, spiritual, moral and social development.[171] Noting that people receiving the Parenting Payment are eligible to receive the remote engagement program payment, the rights of the child may also be promoted.

2.99 Further, the statement of compatibility states that the measure advances the right to equality and non-discrimination by facilitating the remote engagement program trial, which will explore ways to overcome the barriers faced by remote job seekers in reaching full economic participation and the differences in employment opportunities and consequential disadvantage experienced in parts of remote Australia.[172]

Rights potentially limited

2.100 However, in other ways, the measure may engage and limit the rights to work, social security and an adequate standard of living. In particular, if work performed as part of the remote engagement program placement was characterised as a form of employment for the purposes of international human rights law, the measure may engage and limit the right to just and favourable conditions of work. The right to just and favourable conditions of work includes the right to fair wages and equal renumeration for work of equal value without distinction of any kind; a decent living for the worker and their families; and safe and healthy working conditions.[173] The United Nations (UN) Committee on Economic, Social and Cultural Rights has noted that '[f]or the clear majority of workers, fair wages are above the minimum wage' and 'should be paid in a regular, timely fashion and in full'.[174] It has stated that 'remuneration' encompasses a worker's wage or salary as well as additional direct or indirect allowances in cash or in kind that should be of fair and reasonable amount, such as contributions to health insurance, on-site affordable childcare facilities and housing and food allowances.[175]

2.101 Notwithstanding that the measure does not characterise individuals performing work-like activities under the program as employees or workers, the UN Committee on Economic, Social and Cultural Rights has emphasised that the right to just and favourable conditions of work is a right of everyone, without distinction of any kind, meaning that it applies to all workers in all settings, including unpaid

---

171 Convention on the Rights of the Child, articles 26 and 27.

172 Statement of compatibility, p. 8.

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

174 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 23: on the right to just and favourable conditions of work* (2016) [10].

175 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 23: on the right to just and favourable conditions of work* (2016) [7].

workers.[176] Depending on the nature and hours of work performed by the participant, if such work were to constitute a form of employment for the purposes of international human rights law (even if not characterised in this way under domestic law), there could be a risk that the amount of additional social security payable to the individual (that is, $190 per fortnight for at least 30 hours work) may not amount to fair renumeration, particularly where participants perform work of equal value to work performed by actual employees of the remote engagement program host.[177]

2.102 The measure may also engage and limit the rights to social security and an adequate standard of living if the remote engagement program placement were ended or cancelled and consequently the payment removed from a participant, resulting in a lower overall social security benefit.[178] The right to social security includes the right not to be subject to arbitrary and unreasonable restrictions of existing social security coverage, and states must guarantee the equal enjoyment by all of minimum and adequate protection.[179] The right also requires accessibility, which includes the requirement that qualifying conditions for benefits must be reasonable, proportionate and transparent.[180] The UN Committee on Economic, Social and Cultural Rights has applied similar criteria to the removal of social security benefits, stating:

---

176 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 23: on the right to just and favourable conditions of work* (2016) [5]. At [47] on p. 13, the committee observed that excessive use of unpaid internships and training programs is not in line with the right to just and favourable conditions of work.

177 It is noted that if a participant worked the minimum 15 hours per week, the remote engagement program payment would amount to $6.30 per hour. The current national minimum wage is $23.23 per hour. See Fair Work Ombudsman, *Minimum wages increase from 1 July 2023* (18 August 2023).

178 It is noted that concerns have been raised, including by the Parliamentary Joint Committee on Human Rights, that some of the qualifying payments for the remote engagement program, such as the Jobseeker income support payment, may not in themselves be sufficient for a person to meet their basic needs. In April 2023, Australia's Interim Economic Inclusion Advisory Committee advised that the JobSeeker payment is not sufficient for a person to meet their basic needs. See Interim Economic Inclusion Advisory Committee, 2023–24 Report to the Australian Government. The Committee described the JobSeeker payment rate as 'seriously inadequate' when compared with pensions and other income poverty measures (p. 3). See also Parliamentary Joint Committee on Human Rights, Social Security (Tables for the Assessment of Work-related Impairment for Disability Support Pension) Determination 2023 [F2023L00188], *Reports 4 of 2023* (29 March 2023) and *5 of 2023* (9 May 2023).

179 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The Right to Social Security (2008)* [4] and [9].

180 UN Economic, Social and Cultural Rights Committee, *General Comment No. 19: The Right to Social Security (2008)* [24].

> The withdrawal, reduction or suspension of benefits should be circumscribed, based on grounds that are reasonable, subject to due process, and provided for in national law.[181]

2.103 The UN Committee on Economic, Social and Cultural Rights has further stated that '[u]nder no circumstances should an individual be deprived of a benefit on discriminatory grounds or of the minimum essential level of benefits'.[182]

2.104 In addition, as the remote engagement program determined by the instrument involves two Aboriginal corporations, which provide services in the Ngaanyatjarra Lands in Western Australia, the measure has a disproportionate impact on First Nations people living in remote areas and so engages the right to equality and non-discrimination on the basis of race and place of residence.[183] 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.[184] 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 rights).[185] Indirect discrimination occurs

---

181 UN Economic, Social and Cultural Rights Committee, *General Comment No. 19: The Right to Social Security (2008)* [24].

182 UN Committee on Economic, Social and Cultural Rights, General Comment No. 19: The Right to Social Security (2008) [78]. This approach has also been echoed in the European context. The European Committee of Social Rights has stated that the European Social Charter requires that 'reducing or suspending social assistance benefits can only be in conformity with the Charter if it does not deprive the person of his/her means of subsistence'. See European Committee of Social Rights Conclusions, decision of 06 December 2017, Norway, 2013/def/NOR/13/1/EN. See also Magdalena Sepúlveda Carmona, Carly Nyst and Heidi Hautala, 'The Human Rights Approach to Social Protection' (Report, Ministry for Foreign Affairs of Finland) 1 June 2012, p. 49.

183 The majority of the population of the Ngaanyatjarra Lands are Aboriginal and/or Torres Strait Islander. See Australian Bureau of Statistics, Ngaanyatjarra-Giles and Ngaanyatjarraku (2016) and the Ngaanyatjarra Land School, *The Ngaanyatjarra People*. The Ngaanyatjarra Lands is currently a Community Development Program (CDP) region. It is noted that the CDP has previously been criticised for its discriminatory impact on First Nations people. The former Special Rapporteur on the rights of indigenous peoples has observed that the requirements of the CDP are 'discriminatory, being substantially more onerous than those that apply to predominantly non-indigenous jobseekers', namely those not in remote areas: UN Human Rights Council, *Report of the Special Rapporteur on the rights of indigenous peoples on her visit to Australia*, A/HRC/36/46/Add.2 (2017) [58].

184 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. See also UN Committee on Economic, Social and Cultural Rights, *General Comment 20: non-discrimination in economic, social and cultural rights* (2009) [7].

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

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 (including race and place of residence).[186] Differential treatment (including the differential effect of a measure that is neutral on its face) will not constitute unlawful discrimination if the differential treatment is based on reasonable and objective criteria.[187]

2.105 The above rights may be subject to permissible limitations where the limitation pursues a legitimate objective (one which, where an economic, social and cultural right is in question, is solely for the purpose of promoting the general welfare in a democratic society),[188] is rationally connected to that objective and is a proportionate means of achieving that objective.

Committee's initial view

2.106 The committee considered that to the extent that the measure provides opportunities for job seekers to develop employment skills and facilitates the payment of a supplementary social security payment, this promotes the rights to work, social security, an adequate standard of living, and equality and non-discrimination.

2.107 However, the committee noted that these rights may also be limited, depending on how the program operates in practice (including if a person's placement were to be ended or cancelled). The committee sought the advice of the Minister of Indigenous Affairs, as to the matters set out in the minister's response below.

2.108 The full initial analysis is set out in *Report 10 of 2023*.

Minister's response[189]

2.109 The minister advised:

---

186 *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]. Regarding place of residence, see *Lindgren et al v Sweden*, UN Human Rights Committee Communications Nos. 298/1988 and 299/1988 (1991).

187 UN Human Rights Committee, *General Comment 18: Non-Discrimination* (1989) [13] and UN Committee on Economic, Social and Cultural Rights, *General Comment 20: non-discrimination in economic, social and cultural rights* (2009) [13]. See also *Althammer v Austria*, UN Human Rights Committee Communication No. 998/01 (2003) [10.2].

188 International Covenant on Economic, Social and Cultural Rights, article 4.

189 The minister's response to the committee's inquiries was received on 23 October 2023. This is an extract of the response. The response is available in full on the committee's website.

I note this instrument was informed by the outcomes of co-design with the Ngaanyatjarra people. The engagement of stakeholders from the Ngaanyatjarra Lands in the design of the Remote Engagement Program (REP) Trial originally arose from a Commonwealth commitment made as part of settling a class-action lawsuit brought by the Community Development Program (CDP) Participants in 2019 and settled by the previous Government in 2021.

When we formed Government in 2022, we committed to replace the CDP with a new program with real jobs, proper wages and decent conditions developed in partnership with First Nations people. The trial in the Ngaanyatjarra lands continues in line with the commitment to the community and will inform the design of the new program. I note that accessing the REP payment is voluntary and time limited. It will cease on 30 June 2024.

(a) what are the types of circumstances in which a placement may be cancelled (and thus the payment removed)?

The REP Placement may be cancelled or ended:

- at the request of the REP Host or REP Participant
- if the REP Participant is no longer eligible (e.g. is no longer receiving a qualifying income support payment)
- if the REP Participant is not compliant with the terms of the REP Placement Agreement
- if the REP Host is not compliant with the terms of the REP Placement Agreement, or if the Provider believes the REP Participant would be endangered or placed in an unlawful situation as a result of the REP Placement
- for other reasons, such as the REP Participant gaining employment with the REP Host or if directed by the Department.

In the event of a REP Placement ending due to non-compliance by the REP Host, Providers should aim to arrange another REP Placement for a REP Participant. Providers can also choose to arrange another REP Placement where the REP Participant or REP Host has requested to end an existing placement. A request from the Department to end a REP Placement would only occur in extraordinary and unforeseen circumstances, such as a risk to the REP Participant, the REP Host, or the Provider.

(b) noting that the work performed by a participant may constitute a form of employment for the purposes of international human rights law, is the rate of remote engagement program payment (that is, $190 per fortnight for at least 15 hours work) compatible with the right to fair remuneration (noting participants could work up to 8 hours per day);

The REP Trial has been designed to offer participants the opportunity to participate in a placement to gain experience and develop skills.

Participation in the REP Trial is not employment. The REP Payment is an incentive to encourage participation in the REP Trial, not remuneration. As outlined in the CDP Head Agreement Annexure 1, Part G - REP Trial Services (niaa.gov.au/sites/default/files/part-g-annexure-1-headagreement-cdp-2019-2024.pdf), the REP Payment provides an incentive for Eligible Participants to participate in placements designed to build their skills that will support them to find and maintain employment. Under the terms of the REP Placement Agreement, REP Participants cannot be employees of REP Host organisations.

The REP Payment is paid in addition to a REP Participant's primary income support payment and other supplements.

Clause 7.1 of Annexure 1, Part G provides that REP Placements:

- are voluntary;
- do not include paid employment and do not, in themselves, create an employment relationship between the REP Participant and the REP Host or Provider;
- must not be approved if a REP Host has downsized its workforce in the previous 12 months before the commencement of REP Trial Services (i.e. through redundancies or termination) and the proposed REP Placement/s involve the same tasks as those performed by former employees;
- must not be used as a stop-gap measure while a REP Host is undertaking recruitment exercises, or as a way of meeting ad-hoc needs in lieu of creating paid employment positions;
- must not, in whole or in part, involve work which would otherwise have been undertaken by a paid worker if the REP Placement had not taken place; and
- must be ended where the REP Participant commences paid employment with the REP Host.

A REP Placement must not replace jobs or a paid worker. REP Placements must also be tailored to the needs of the REP Participant.

(c) how is the measure effective to achieve the stated objectives and in particular, noting the mixed findings of the CDP regarding its effectiveness in achieving employment outcomes for participants, how is the remote engagement program different from the CDP such that it is more likely to achieve the stated objectives;

The Remote Engagement Program Trial uses a co-design approach to trial ideas that could be considered in the design of a new remote employment program to replace the CDP. The REP Trial aims to test ideas and understand barriers to employment in remote areas. Under the Social Security Act payments cannot be made after 30 June 2024. It complements other trials currently under way, including the new community projects approach in

CDP and the New Jobs Program Trial which commenced on 18 September 2023.

The outcomes of these trials will help to provide an evidence base for what works and what does not work in remote employment services. The REP Trial is trialling a new supplementary payment in the social security system as an incentive for eligible jobseekers to attend a placement designed to build their skills that will support them to find and maintain employment and contribute to their community. The REP Trial is unique in its integration with the income support system. No other CDP trials or projects currently underway offer the delivery of incentives via the income support system to gain experience and develop skills.

(d) whether communities were consulted about the proposed measure in this instrument, as opposed to the broader policy underpinning the remote engagement program, and if so, what were the outcomes of those consultations;

The REP Trial was a concept that emerged from ongoing engagement with stakeholders from the Ngaanyatjarra Lands in Western Australia as part of settling a class-action lawsuit brought by CDP Participants in 2019 and settled by the previous Government in 2021.

A Ngaanyatjarra Lands Co-Design Group, comprising community and Ngaanyatjarra Council (Aboriginal Corporation) (NCAC) representatives, was established in March 2022 and met in March and May 2022 to determine the details of the REP Trial, including the rate of the REP Payment.

At the May 2022 Co-Design Group meeting, the Board of Ngaanyatjarra Council asked NCAC to bring forward design options for a trial program. The Board of Ngaanyatjarra Council endorsed the REP Placements in November 2022.

The Paupiyala-Tjarutja Aboriginal Corporation, the governing body for the Spinifex people and the CDP provider in Tjuntjuntjara within CDP Region 3, expressed an interest in being involved in the REP Trial on 28 September 2022 and were subsequently invited to participate.

Additionally, Providers must engage broadly with communities to identify their priorities for the REP Trial, including their preferred REP Host organisations and preferred activities to be undertaken as part of REP Placements.

(e) whether review is available for certain decisions made in relation to this measure, such as where a person's placement is cancelled, and their payment is removed;

REP Participants have several options to request a review of decisions relating to their REP Placement, including: internal review by the Provider; formal review by Services Australia; and review by the Administrative Appeals Tribunal. Before agreeing to be a REP Participant, REP Participants

will be provided with information about making a complaint or appealing a decision.

In the event of non-compliance by a REP Participant, Providers must consider alternatives to ending the REP Placement Agreement and outline factors that must be taken into consideration before making a decision to end the placement, including:

- reasons for the non-compliance, including whether the REP Participant was fully able to comply with the requirements of the REP Placement Agreement;
- the severity and impact of the non-compliance (for example, a REP Participant engaging in unsafe practices despite appropriate guidance and training compared with failure to notify in advance of a single absence);
- whether the REP Participant was adequately warned of the consequences of non-compliance;
- the frequency or repeated nature of the non-compliance; and
- how other REP Participants have been treated by the Provider in similar situations.

Providers must support REP Participants over the course of their REP Placement and act as an advocate for the REP Participant. When making a decision to end a REP Placement, REP Providers must make lawful decisions; observe natural justice; evidence, facts and findings; explanation of reasons and documenting decisions.

(f) what other safeguards accompany the measure.

Safeguards for REP Participants under this measure include:

- Participation in a REP Placement is voluntary.
- The REP Participant can end the REP Placement at any time and for any reason.
- Providers must use a case management approach, whereby adjustments are made for the differing needs and strengths of each Eligible Participant.
- Providers must conduct an assessment of individuals before they commence in a REP Placement.
- Before commencing a REP Placement, Providers must discuss the Eligible Job Seeker's skills, aspirations, and the nature of REP Placement the Eligible Job Seeker would like to participate in.
- Participation in REP Placements cannot be used to replace real jobs at a REP Host.

- Before signing the REP Placement Agreement, REP Participants must be informed of the REP Trial arrangements that will impact on them, and providers must:
    - provide the REP Participant with a copy of the Fact Sheets for REP Participants and the REP Placement Agreement, including the Privacy Collection Notice;
    - explain the content of the Fact Sheets for REP Participants and the REP Placement Agreement, including the Privacy Collection Notice;
    - explain the impact of the REP Payment on the REP Participant's income and potential impact on benefits, including:
        - the REP Payment is taxable;
        - the REP Payment does not need to be reported to Centrelink;
    - the REP Payment forms part of the person's taxable income, and may affect the REP Participant's entitlements from State Government authorities or other organisations to whom changes in income must be reported;
    - explain that in order to receive the REP Payment, the REP Participant must attend a REP Placement for at least 15 hours every week in their payment fortnight;
    - tell the REP Participant that participation is voluntary and they can end their REP Placement at any time and for any reason;
    - ensure the REP Participant understands the duration, conditions and participation requirements of the REP Placement and the REP Payment.
- Providers must assess job seeker eligibility and suitability for a REP Placement, and support the REP Participant in their REP Placement to ensure the REP Participant has the best chance to successfully participate in the REP Placement and gain the desired skills and experience.
- A three way REP Placement Agreement is signed by the Provider, REP Participant and REP Host that ensures the REP Participant's safety and the provision of appropriate tasks and supervision.
- Contractual requirements to engage with communities in the implementation of the REP Trial.

Concluding comments

International human rights legal advice

2.110 While the initial analysis noted that facilitating a program seeking to build skills and support employment opportunities, and enabling the payment of a supplementary social security benefit, is capable of constituting a legitimate objective, questions arose as to whether the measure is an effective and proportionate means to achieve this stated objective.

2.111 Regarding the effectiveness of the remote engagement program, the minister advised that the REP uses 'a co-design approach to trial ideas that could be considered in the design of a new remote employment program to replace the CDP', and trials a new supplementary payment in the social security system as an incentive for eligible jobseekers to 'attend a placement designed to build their skills that will support them to find and maintain employment and contribute to their community'. The minister stated that the trial aims to test ideas and understand barriers to employment in remote areas until 30 June 2024, and complements other trials currently under way. The minister further stated that 'the outcomes of these trials will help to provide an evidence base for what works and what does not work in remote employment services'. The minister stated that the REP differs from the CDP in that the REP relates to the delivery of incentives via the income support system to gain experience and develop skills (rather than part of a mutual obligation on program participants as a precondition to receiving jobseeker payments).

2.112 As noted in the preliminary analysis, as this program is evidently in the trial phase, and is intended to develop an evidence base for future programs, it is not yet clear whether it is effective to achieve the stated objective. While in general terms providing participants with an opportunity to build employment-related skills could assist to achieve the objective of helping participants to secure employment, where there are minimal or no prospects of local employment (a relevant consideration in the Ngaanyatjarra Lands), it remains unclear whether the measure would be effective to achieve the stated objective in such circumstances.[190] In this regard, it is noted that the primary difference between CDP and REP appear to be that participation in REP is voluntary and does not impact a person's primary social welfare payment, whereas CDP was initially involuntary and constituted a mutual obligation tied to receipt of a

---

190 In its evaluation of the Community Development Program, which is intended to be replaced by the Remote Engagement Program, the Department of the Prime Minister and Cabinet stated that many CDP participants face moderate to extreme barriers to employment based on the Job Seeker Classification Instrument, reflecting the high share of CDP participants living in very remote areas with limited labour market opportunities – the majority of whom are Aboriginal or Torres Strait Islander people. See *The Community Development Program: Evaluation of Participation and Employment Outcomes* (2018) pp. iv, 63, 67–78.

person's primary welfare payment.[191] It remains unclear whether this difference has an impact on the achievement of the stated objectives of the REP, which are framed in similar terms to those underpinning the CDP (namely, to improve employment outcomes in remote communities by increasing participation in work-like activities, improving employability and increasing sustainable work transitions among CDP participants).[192] It appears that without addressing the underlying causes of unemployment or job insecurity in remote areas, such as limited labour market opportunities, it is not clear that the REP alone would necessarily be effective to achieve the broader objective of securing employment for REP participants.

2.113 The operational detail of the measure is relevant in assessing proportionality, including the types of circumstances in which a placement may be cancelled (and thus the payment removed). In this regard, the minister advised that a placement may be cancelled for a number of reasons, including if the participant is no longer eligible (for example where they are no longer receiving a qualifying income support payment), or where either the participant or the host are not complying with the terms of the placement agreement. A placement may also be cancelled at the request of the REP host or REP participant or if directed by the department. The minister advised that a request from the department to end a placement would only occur in extraordinary and unforeseen circumstances, such as a risk to the participant, host or provider. As noted above, the UN Economic, Social and Cultural Rights Committee has stated that the 'withdrawal, reduction or suspension of benefits should be circumscribed, based on grounds that are reasonable, subject to due process, and provided for in national law'.[193] While some of the grounds appear to be sufficiently circumscribed and provided for in law, such as where a participant is no longer eligible or not compliant with the terms of the placement agreement, other grounds are broadly framed. For example, it is not clear whether ending a placement at the request of the REP host would necessarily be reasonable in all circumstances, as there does not appear to be any limit on the bases on which the REP host may request to end a placement. The minister advised that where a host has requested to end a placement, the REP provider

---

191 Participation in CDP activities appears to have been voluntary since May 2021 when a number of mutual obligations were removed, see NIAA 2021, 'Changes to Mutual Obligations Requirements for Community Development Program (CDP)'.

192 Department of the Prime Minister and Cabinet, *The Community Development Program: Evaluation of Participation and Employment Outcomes* (2018) pp. iv. Regarding evaluations of the CDP, see Australian National Audit Office (ANAO), *The Design and Implementation of the Community Development Programme* (2017) [4.38]–[4.45]. At [4.42], the ANAO noted that 'the proportion of participants placed in at least one job was almost unchanged but there was a small increase in the total number of job placements (mostly casual jobs), particularly Indigenous jobseekers'.

193 UN Economic, Social and Cultural Rights Committee, *General Comment No. 19: The Right to Social Security (2008)* [24].

can choose to arrange another placement. However, this is a discretionary safeguard and may have limited value in practice if there are no other placements available.

2.114 Another relevant factor in assessing proportionality is whether communities were genuinely consulted about the proposed measure in this instrument, as opposed to the broader policy underpinning the remote engagement program. In this regard, the minister advised that the REP emerged from ongoing engagement with stakeholders from the Ngaanyatjarra Lands in Western Australia as part of settling a class-action lawsuit brought by CDP Participants in 2019, settled in 2021. The minister stated that a co-design group was established in March 2022, met in March and May 2022 to determine the details of the trial and rate of payment, and that in May the Board of Ngaanyatjarra Council asked the Ngaanyatjarra Council (Aboriginal Corporation) to bring forward design options for a trial program, endorsing the REP Placements in November 2022. The Paupiyala-Tjarutja Aboriginal Corporation expressed interest in being involved in the REP in September 2022 and were subsequently invited to participate. The minister further noted that providers must engage broadly with communities to identify their priorities for the REP, including their preferred REP host organisations and preferred activities to be undertaken as part of REP Placements.

2.115 As noted in the initial analysis, co-designing the program with communities that are to be affected by the measure is an important aim. Indeed, as part of its obligations in relation to respecting the right to self-determination, Australia has an obligation under customary international law to consult with indigenous peoples in relation to actions which may affect them.[194] The right of indigenous peoples to be consulted is a critical component of free, prior and informed consent.[195] The minister's response suggests that communities were consulted regarding various aspects of the REP, including with respect to early design options. This engagement with the community assists with proportionality. However, it remains unclear whether such consultation contained all the constituent elements of 'free, prior and informed consent' for the purposes of international human rights law. In particular, while the minister stated that the Ngaanyatjarra Lands Co-Design Group determined the details of the REP, including the rate of pay, it is noted that under the Social Security Act, the rate of pay must be between $100 and $190. Given these legislative limits on the rate of pay, it is not clear that the rate of pay could be said to be genuinely co-designed, noting that the obligation to consult under international human rights law includes the right of indigenous peoples to 'influence the outcome of decision-making processes

194 See Parliamentary Joint Committee on Human Rights, *Report 4 of 2017* (9 May 2017) p.122–123; *Report 15 of 2021* (9 December 2021) pp. 9–26.

195 United Nations Human Rights Council, *Free, prior and informed consent: a human rights-based approach - Study of the Expert Mechanism on the Rights of Indigenous Peoples*, A/HRC/39/62 (2018) [14].

affecting them, not a mere right to be involved in such processes or merely to have their views heard'.[196]

2.116 Further information was sought as to whether the rate of remote engagement program payment is compatible with the right to fair remuneration, noting that the rate of $190 per fortnight for 30 hours work equates to $6.33 per hour, if a person worked the minimum hours required.[197] The minister stated that the REP is not employment, but rather has been designed to offer participants the opportunity to participate in a placement to gain experience and develop skills. The minister stated that the payment is an incentive to encourage participation, not remuneration, and the REP Placement must not replace jobs or a paid worker. Further, the minister stated that under the terms of the REP Placement Agreement, REP Participants cannot be employees of REP Host organisations. The minister also referred to clause 7.1 of the Annexure, which provides that REP Placements:

- are voluntary;
- do not include paid employment and do not create an employment relationship between the participant and host or provider;
- must not be approved if a host has downsized its workforce in the previous 12 months and the proposed placement involves the same tasks as those performed by former employees;
- must not be used as a stop-gap measure while a host is undertaking recruitment exercises, or as a way of meeting ad-hoc needs in lieu of creating employment positions;
- must not, in whole or in part, involve work that would otherwise have been undertaken by a paid worker; and
- must end if a participant commences paid employment with the host.

2.117 Clause 7.1 of the Annexure appears to set some parameters around the type of work and tasks that may be performed by a participant. This may mitigate the risk

---

196 UN Human Rights Council, *Free, prior and informed consent: a human rights-based approach - Study of the Expert Mechanism on the Rights of Indigenous Peoples*, A/HRC/39/62 (2018) [15]-[16]. The UN Human Rights Council further advised that the obligation to 'consult with indigenous peoples should consist of a qualitative process of dialogue and negotiation, with consent as the objective' and that consultation involves 'a process of dialogue and negotiation over the course of a project, from planning to implementation and follow-up'. In the context of special measures, the UN Committee on the Elimination of Racial Discrimination has stated that special measures should be 'designed and implemented on the basis of prior consultation with affected communities and the active participation of such communities'. See United Nations Committee on the Elimination of Racial Discrimination, *General Recommendation No. 32* (2009) [16]–[18].

197 By contrast, the current national minimum wage is $23.23 per hour. See Fair Work Ombudsman, *Minimum wages increase from 1 July 2023* (18 August 2023).

of participants performing work and tasks that would otherwise be undertaken by an employee of the host organisation. However, while it is evident that the work-like activities performed by participants as part of their placements do not constitute employment under domestic law, depending on the nature and hours of work performed by a participant, there appears to be a possibility that such work may nonetheless constitute a form of employment for the purposes of international human rights law. This is because the right to just and favourable conditions of work applies to all workers in all settings, including unpaid workers.[198] Indeed, the UN Committee on Economic, Social and Cultural Rights has observed that excessive use of unpaid internships and training programmes is not in line with the right to just and favourable conditions of work.[199] Further, the right to fair and equal remuneration relates to the *value* of work performed as opposed to the specific job or tasks performed. As observed by the UN Committee on Economic, Social and Cultural Rights, '[s]ince the focus should be on the "value" of the work, evaluation factors should include skills, responsibilities and effort required by the worker, as well as working conditions'.[200] Remuneration must also provide a decent living for workers and their families and must be sufficient to meet basic needs such as health care, education and housing.[201]

2.118 As the focus should be on the value of the work performed, even if a participant performs different tasks to those ordinarily performed by an employee, if the tasks nonetheless contribute to the overall work of the host organisation it is not clear why, in such circumstances, the participant should not be remunerated fairly and equally for such work. Additionally, it is not clear that the work-like activities performed by participants would, in practice, be that dissimilar to tasks being performed by employees, particularly noting that many organisations in the Ngaanyatjarra Lands are community organisations that may not be adequately funded or resourced and thus may be unable to employ a sufficient level of staff to meet the organisation's ongoing or ad-hoc needs. It may therefore be difficult in practice to ensure that participants are not undertaking tasks that could be performed by employees if the organisation had adequate funds to employ more people.[202] There therefore appears to be a risk that in some circumstances, the work-like activities

---

198 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 23: on the right to just and favourable conditions of work* (2016) [5].

199 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 23: on the right to just and favourable conditions of work* (2016) [47(b)].

200 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 23: on the right to just and favourable conditions of work* (2016) [12].

201 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 23: on the right to just and favourable conditions of work* (2016) [18].

202 The most common occupations in Ngaanyatjarraku are community and personal service workers in the industries of local government administration, education and other allied health services. See Australian Bureau of Statistics, Ngaanyatjarra-Giles and Ngaanyatjarraku (2016).

performed by a participant could constitute a form of employment for the purposes of international human rights law and, in such cases, the rate of payment (that is, $190 per fortnight for at least 30 hours work or a maximum of $6.33 per hour) would unlikely be sufficient to amount to fair remuneration, particularly where participants perform work of equal value to work performed by actual employees of the host organisation.[203] While it is acknowledged that the REP payment is in addition to a participant's qualifying social security payment, were the participant to be paid the minimum wage for the hours worked as part of the program, they would receive a higher fortnightly income amount than that offered by the REP.[204] For example, a single participant receiving the Jobseeker Payment plus the REP payment would receive a total social security payment of $939.20 per fortnight. Were they to be paid the minimum wage for their participant in the REP (that is, $23.23 per hour for a minimum of 30 hours of work per fortnight), they would receive a total amount of $1,128.56.[205] If they were to work more than 30 hours per fortnight the difference would be even greater (noting that the REP payment would not increase once 30 hours per fortnight has been reached).

2.119 As to whether the measure is accompanied by effective safeguards, including the availability of review, the minister advised that there are several review options available, including internal review by the provider; formal review by Services Australia; and review by the Administrative Appeals Tribunal. Additionally, participants will be informed about how to make a complaint and appeal a decision. The minister advised that if a participant does not comply with the REP Placement Agreement, the REP Provider must consider alternatives to ending the placement and must take into account certain factors before making a decision to end the placement. Relevant factors include the reasons for non-compliance, the severity and impact of the non-compliance, and the frequency or repeated nature of the non-compliance. The minister stated that when deciding to end a placement, providers must make lawful decisions, observe natural justice, have sufficient evidence, clearly explain the

---

203 It is noted that if a participant worked the minimum 15 hours per week, the remote engagement program payment would amount to $6.30 per hour. The current national minimum wage is $23.23 per hour. See Fair Work Ombudsman, *Minimum wages increase from 1 July 2023* (18 August 2023).

204 The rate of each qualifying social security payment varies depending on the payment type and the individual circumstances of the participant. For example, a single person with no children is eligible to receive $749.20 as a Jobseeker Payment.

205 This includes $696.90 for the 30 hours worked (at a rate of $23.23) plus a reduced Jobseeker Payment of $431.66 (noting that a person may earn up to $150 without a payment reduction and then any income over $150 means that the payment is reduced by 50 cents for each dollar between $150 and $256 then 60 cents for each dollar over $256). See Services Australia, *Income test* and *How much you can get* (20 September 2023). This example is based on a single person with no children whose maximum fortnightly Jobseeker Payment is $749.20.

reasons for the decision and document the decision. It appears that there are several review options available to participants, which assists with proportionality.

2.120 As to the existence of other safeguards, the minister stated that the placement is voluntary and a participant can end it at any time; providers must conduct an assessment of individuals before they commence a placement and discuss the participant's skills, aspirations and the nature of the placement to ensure a suitable match; providers must use a case management approach, making adjustments according to the different needs and strengths of participants; participants must be provided with information about the placement, including the minimum hours required to participate and the tax implications of the supplementary payment; and a three way REP Placement Agreement is signed by the participant, host and provider. The minister also emphasised that the REP is time limited and will cease on 30 June 2024. The voluntary and time limited nature of the REP as well as the obligation on providers to tailor the placement to suit the needs of the participant and deliver the program in a culturally appropriate manner assists with proportionality, particularly with respect to the right to equality and non-discrimination insofar as it may ensure placements are inclusive.[206] However, these safeguards have limited value with respect to the right to fair and equal renumeration. Additionally, while the overall measure is time limited, it is not clear whether the placements themselves are time limited, as the duration of each placement will be set out in the REP Placement Agreement. If a person were to participate in a placement for the duration of the entire program (that is, from potentially mid 2023 until 30 June 2024), the potential interference with rights is more significant and thus less proportionate.

2.121 In conclusion, while the measure pursues a legitimate objective, it is not yet clear whether it will be effective to achieve the stated objective of securing employment, noting that the REP is still in its trial phase and evaluations are yet to be undertaken. The measure is accompanied by some safeguards that assist with proportionality, including the availability of review, the voluntary and time limited nature of the program and the requirement that placements are tailored to the needs and skills of participants. However, it is not clear that all grounds on which a placement may be ended (and thus the supplementary payment removed) would, in practice, be reasonable. In particular, there does not appear to be any limit on the bases on which a REP host may request to end a placement. There appears to be a risk that removing the supplementary payment on unreasonable grounds may constitute a retrogressive measure and, in such circumstances, the measure may impermissibly limit the rights to social security and an adequate standard of living. However, were the supplementary payment to be removed only in circumstances that are reasonable, subject to due process, and provided for in law (as required by international human rights law), noting the safeguards set out above, the measure would likely be compatible with these rights.

---

206 Annexure, subsection 5.1.

2.122 With respect to the right to just and favourable conditions of work, despite the program's classification as a non-employment relationship under domestic law, depending on the nature and hours of work undertaken by a participant, it may nonetheless be considered employment for the purposes of international human rights law. In such cases, concerns remain that the rate of $190 per fortnight for 30 hours work (which equates to $6.33 per hour), is insufficient to amount to fair and equal remuneration for the purposes of the right to just and favourable conditions of work. As such, it has not been demonstrated that the measure would, in all circumstances, constitute a proportionate limitation on the rights to just and favourable conditions of work. If the measure were to impermissibly limit the above rights, it would also likely constitute unlawful discrimination, particularly with respect to Aboriginal and Torres Strait Islander peoples, as the differential treatment could not be said to be based on reasonable and objective criteria.

Committee view

2.123 The committee thanks the minister for this response. The committee notes the intention behind the remote engagement program is to replace the CDP with a new program with 'real jobs, proper wages and decent conditions – developed in partnership with First Nations peoples'.[207] The committee considers that to the extent that the measure provides opportunities for job seekers to develop employment skills and facilitates the payment of a supplementary social security payment, this promotes the rights to work, social security, an adequate standard of living, and equality and non-discrimination.

2.124 However, the committee notes that these rights may also be limited, including if a person's placement were to be ended or cancelled. The committee considers that the measure pursues the legitimate objective of seeking to build skills and support employment opportunities and enabling the payment of a supplementary social security benefit. The committee notes that as the program is still in its trial phase and has thus not been subject to evaluation, it is not possible to conclude on its likely effectiveness to achieve the stated objective. With respect to proportionality, the committee considers that the measure is accompanied by some important safeguards, such as the availability of review, the voluntary and time limited nature of the measure and the obligation on providers to tailor placements to the needs of participants. However, the committee remains concerned that a placement may be ended in circumstances that may not always be reasonable, noting that there does not appear to be any limit on the bases on which a REP host may request to end a placement. The committee considers that were the supplementary payment to be removed on unreasonable grounds, it may constitute a retrogressive measure such that it risks impermissibly limiting the rights to social security and an adequate standard of living. The committee also considers, however, that were the supplementary payment to be

[207] Explanatory statement, p. 1.

removed only in circumstances that are reasonable, subject to due process, and provided for in law, the measure would likely be compatible with these rights.

2.125 The committee also remains concerned that if the placement were to constitute a form of employment for the purposes of international human rights law, the rate of pay for a minimum 15 hours per week (which would amount to $6.33 per hour, which is significantly less than the minimum wage of $23.23 per hour), is insufficient to amount to fair and equal remuneration. While the committee notes that the remote engagement program payment is in addition to the participant's other social security entitlements, were the participant to be paid the minimum wage for the hours worked as part of the program, they would receive a higher fortnightly income amount than that offered by the REP. As such, if the placement were to constitute a form of employment for the purposes of international human rights law, the committee considers that the measure may not, in all circumstances, constitute a proportionate limitation on the right to just and favourable conditions of work. Further, if the measure impermissibly limits the above rights, the committee considers that it would also likely constitute unlawful discrimination, particularly with respect to Aboriginal and Torres Strait Islander peoples, as it is not clear that the differential treatment is based on reasonable and objective criteria.

Suggested action

2.126 The committee considers the proportionality of this measure may be assisted by:

(a) amending the Social Security Act to remove the maximum rate of pay for the remote engagement program payment, thereby allowing the rate of pay to be greater than $190 and determined through genuine co-design;[208]

(b) circumscribing with greater clarity the grounds on which a REP Placement may be ended, including the circumstances in which a REP host may cancel a placement; and

(c) specifying the duration of the REP Placement in legislation, noting that the longer the placement the more likely it would be considered to be a form of employment.

2.127 The committee recommends that the statement of compatibility be updated to reflect the information provided by the minister.

[208] *Social Security Act 1991*, subsection 661E(3).

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

Mr Josh Burns MP

Chair