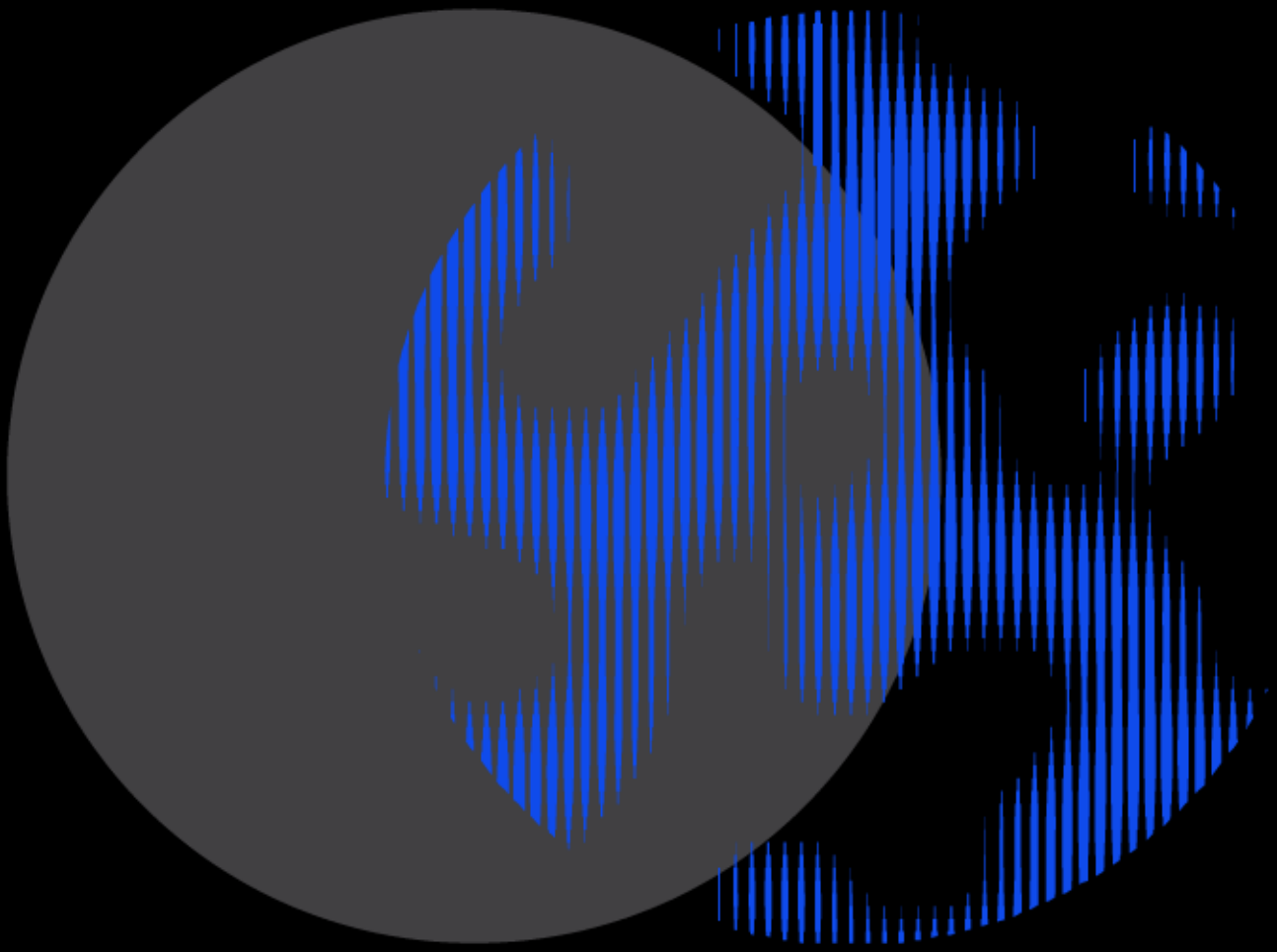
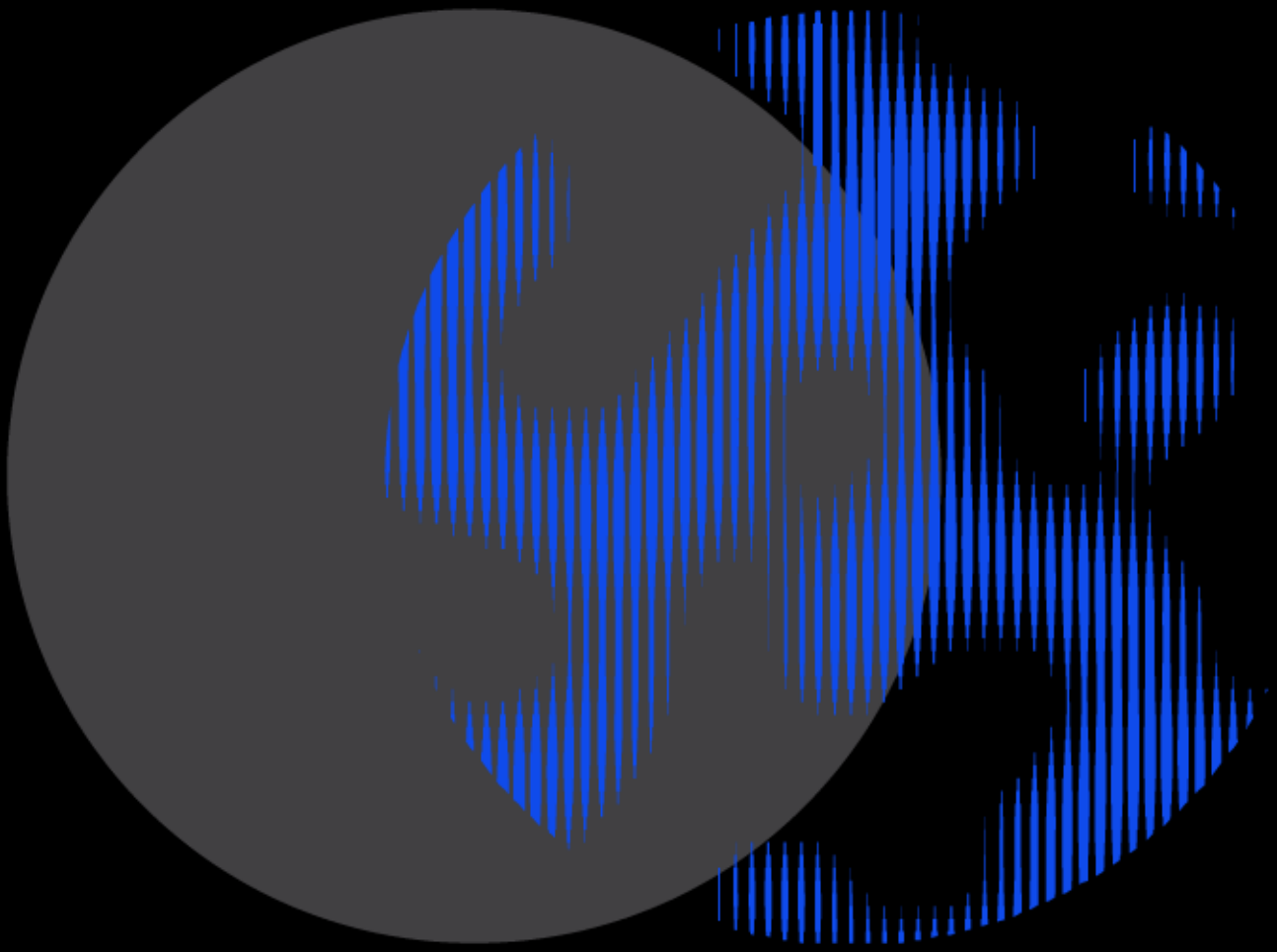
Human Technology Institute



Submission to the Senate Economics Legislation Committee the Digital ID Bill 2023, and the Digital ID (Transitional and Consequential Provisions) Bill 2023

23 January 2024

Human Technology Institute



Submission to the Senate Economics Legislation Committee the Digital ID Bill 2023, and the Digital ID (Transitional and Consequential Provisions) Bill 2023

23 January 2024

About the Human Technology Institute

The Human Technology Institute (HTI) is building a future that applies human values to new technology. HTI embodies the strategic vision of the University of Technology Sydney (UTS) to be a leading public university of technology, recognised for its global impact specifically in the responsible development, use and regulation of technology. HTI is an authoritative voice in Australia and internationally on human-centred technology. HTI works with communities and organisations to develop skills, tools and policy that ensure new and emerging technologies are safe, fair and inclusive and do not replicate and entrench existing inequalities.

The work of HTI is informed by a multi-disciplinary approach with expertise in data science, law and governance, policy and human rights.

HTI has conducted research and provided advice relating to the responsible implementation of digital identity systems. HTI has worked collaboratively with Service NSW to provide independent expert advice regarding digital identity in NSW. In December 2023, HTI released a Policy Insights Paper, *Improving governance and training for the use of facial verification technology in NSW Digital ID*, which distils key insights from the process it undertook with Service NSW.[1] In September 2023, HTI made a submission to the Legal and Constitutional Affairs Committee on the Identity Verification Services Bill 2023.[2] In September 2022, HTI published a report outlining a *Model Law for Facial Recognition Technology*, based on an extensive consultation process.[3] This submission draws on all of these outputs.

For more information, contact us at hti@uts.edu.au

Acknowledgement of Country
UTS acknowledges the Gadigal people of the Eora Nation, the Boorooberongal people of the Dharug Nation, the Bidiagal people and the Gamaygal people upon whose ancestral lands our university stands. We would also like to pay respect to the Elders both past and present, acknowledging them as the traditional custodians of knowledge for these lands.

Authors: Sophie Farthing, Lauren Perry, Sarah Sacher, Professor Edward Santow

To discuss this submission, please contact us at hti@uts.edu.au.

[1] Edward Santow, Sophie Farthing and Lauren Perry, 'Improving governance and training for the use of facial verification technology in NSW Digital ID' (James Martin Institute and Human Technology Institute, Policy Insights Paper, December 2023) <https://jmi.org.au/wp-content/uploads/2023/12/JMI-PIP-Improving-governance-and-training-for-the-use-of-facial-verification-technology-in-NSW-Digital-ID.pdf>.
[2] Human Technology Institute, Submission No 4 to the Legal and Constitutional Affairs Legislation Committee, *Inquiry into the Identity Verification Services Bill* (September 2023).
[3] Human Technology Institute, *Facial Recognition Technology: Towards a Model Law* (Report, September 2022).

Contents

Executive summary

The Human Technology Institute (**HTI**) welcomes the opportunity to comment on the Digital ID Bill 2023 (**the Bill**) and the accompanying consequential amendments bill.

An effective digital ID system is one that has strong technical foundations, and an accompanying legal and governance framework that upholds privacy and other human rights. The Bill has elements that would contribute to this positive outcome, including:

- The Bill would extend privacy protections beyond those currently required by the *Privacy Act 1988* (Cth) (**Privacy Act**). Chapter 3 of the Bill contains a number of additional provisions that would provide stronger privacy safeguards – especially in relation to the protection of sensitive information, including biometric information, and the application of consistent privacy protections.[4] This is welcome and necessary in light of the risks to privacy associated with digital ID, and the outdated nature of the Privacy Act.
- The Bill would provide for a number of external oversight mechanisms, including a Digital ID Regulator (the ACCC) to accredit entities and oversee the Australian Government ID System (**AGDIS**); an expanded role for the Information Commissioner (regarding assessment powers in relation to the handling and maintenance of personal information under the Bill, and to provide advice on the operation of the Digital ID Bill to the Digital ID Regulator at their request);[5] a System Administrator for the AGDIS; and an independent Digital ID Data Standard Chair. A Ministerial Digital ID Expert Panel has also been set up to provide independent advice.[6]
- The Bill would provide consequences for non-compliance, including maximum civil penalty rates for privacy breaches and provisions for liability with respect to participation agreements under the AGDIS.[7]
- The Bill would enable choice for individuals since using a digital ID is voluntary, and relying parties must not require a digital ID as a condition of service.[8]
- The Bill has an interoperability requirement for all participants under the AGDIS scheme.[9] This means that accredited entities must provide their accredited services to other entities participating in the system, and relying parties must provide users with a choice of identity service providers when they seek to verify their identity.
- The Bill would require accredited services to be accessible and inclusive, and enables the provision of rules in this regard.[10]

[4] See, for example, requirements for express consent from individuals (cl 45, 46, 48(1)); maximum civil penalties for non-compliance under Chapter 3; extended meaning of personal information (cl 35); specific restrictions on collection, use and disclosure of biometric data (see for example, cl 48, 53); imposing privacy obligations on non-Australian Privacy Principle entities and deeming breaches of additional privacy requirements to be an interference with privacy (cl 36); prohibitions on using information for data profiling or marketing purposes (cl 54, 57); mandatory data breach notification scheme (cl 40, 41).
[5] Cl 42, and also proposed as an amendment to the *Privacy Act 1988* (Cth)– a new s 33C(1)(g).
[6] Department of Social Services, 'Minister Shorten press conference for the launch of the myGov Advisory Group' (Press Conference Transcript, 9 November 2023) <https://ministers.dss.gov.au/transcripts/13051>.
[7] See Chapter 3 civil penalty clauses, and cl 84.
[8] Cl 74.
[9] Cl 79.
[10] Cl 30.

- The Bill would enable the provision of rules for technical service standards and performance testing.[11]
- The Bill would enable the provision of rules for redress mechanisms.[12]

However, some important elements of the Bill need to be improved in order to meet privacy and other human rights requirements. HTI's submission focuses on the need for: legislative consistency with overlapping laws; robust privacy protections within the scheme, and specific regulation of facial recognition technology beyond the scheme; the full realisation of principles of autonomy and consent, as well as accessibility, inclusion and non-discrimination for users; effective redress mechanisms that provide individual remedies and improve accountability; and public access to information and education regarding the scheme.

Need for legislative consistency

The Bill can be seen as only part of the Australian Government's digital identity system, with the other parts of this system governed primarily by the recently-passed *Identity Verification Services Act 2023* (Cth) (**IVS Act**).

The Bill also engages the Privacy Act, with the Government indicating an intent to amend that Act in line with its formal response to the Attorney-General's Department review of the Privacy Act. That review was finalised in 2022, and as yet no proposed amendments to the Privacy Act have been made public. It is essential that these Privacy Act reforms be introduced and passed as soon as possible.

In addition, the states and territories have also taken important steps to introduce their own digital identity systems. Some of these jurisdictions – such as New South Wales – are quite advanced in their work in this area. Others are less advanced.

As a result, Australia's approach to digital identity is reasonably fragmented solely within the federal jurisdiction. That fragmentation increases when one considers also the overlapping state and territory digital identity systems. While a single, unified system of digital ID in Australia is unnecessary to resolve problems arising from this fragmentation, there is a need to adopt an approach that is integrated and coordinated, both within the federal government and across all Australian jurisdictions. Most importantly of all, Australia's digital ID system should be built around the needs of the Australian community.

Privacy protections

Some of the privacy provisions in the Bill should be tightened to ensure that protections are robust and reliable.

- The Bill's privacy protections apply only to the extent that an accredited entity is providing an accredited service. To ensure complete coverage, the scope should be extended to activities that are incidental and ancillary to the provision of the service.
- The Bill grants law enforcement bodies unnecessarily broad and deep access to personal information arising from this digital ID scheme. In this way, the Bill intrudes on Australians' privacy rights beyond what may be justified under international human rights law. In addition, the overly-broad access provisions for law enforcement bodies risk contributing to public distrust in the scheme. Law enforcement bodies should be able to access

[11] Cl 80, 81.
[12] Cl 88.

personal information only in highly-restricted circumstances – such as with a judicial warrant in respect of a serious crime, or to investigate serious fraud or cybersecurity incidents directly related to the digital ID scheme itself.

- Data retention periods are not specified in the Bill with respect to non-biometric data. Specific timelines should be provided for the destruction of data so that personal information is not held longer than is necessary.
- The prohibition on data profiling or tracking is welcome, but the wording of the exemptions should be tightened to prevent potential loopholes.

Additionally, the identity architecture of the AGDIS and the existing Trusted Digital Identity Framework (TDIF) are designed as a 'hub and spoke' model which operates in a centralised way. This approach presents several disadvantages, including higher exposure to single points of failure and cybersecurity breaches. Shifting the design of the AGDIS and TDIF architecture to a distributed model (like that which the NSW Government is taking with NSW Digital ID) would ensure the federal Government takes a nationally harmonised approach to digital identity systems as well as improving privacy and data protections for users.

Consent, autonomy and voluntariness

It is welcome that the Bill provides that only individuals who provide express consent will be enrolled in the digital ID scheme. These provisions could be strengthened through the inclusion of a definition and explanation of how consent should be obtained, as well as provision for accessible means of withdrawing consent.

However, reliance on consent has limitations, and further safeguards are needed. The Privacy Act Review recommended the adoption of an objective 'fair and reasonable' test for the processing of personal information, which should be adopted also in this Bill.

The Bill provides that creating and using a digital ID will be voluntary, which gives individuals the choice to opt out. The Bill should also include a guarantee of ongoing equal access to services for those who make this choice. This is necessary to ensure that engaging with digital ID systems is genuinely consent-based, and to prevent exclusion for vulnerable groups. Exemptions to the voluntariness clause also need to be tightened.

Accessibility and non-discrimination

In order to realise the benefits of digital ID, it must be accessible for, inclusive of, and reasonably useable by, all eligible users. The existing provisions relating to the development of accessibility rules and criteria in the Bill could be strengthened – including by explicitly taking into account the human rights of groups that may be adversely affected by the scheme.

Redress

There are serious risks of harm to individuals if the legal requirements in the Bill are not met. While the Bill allows for a potential redress mechanisms to be set up through Digital ID Rules, ideally, a redress mechanism would be enshrined in primary legislation, include provisions for remedies, and provide a simple and accessible avenue for complaints

List of recommendations

Recommendation 1: The Australian Government should adopt a consistent and coordinated approach to federal privacy protections and digital ID. Anticipated amendments to the Privacy Act should be passed as soon as possible, and consequential amendments made to both the IVS Act and Digital ID Bill to address any inconsistencies.

Recommendation 2: Clause 33 of the Bill should be amended to include entities that are 'doing things that are incidental or ancillary' to the provision of accredited services.

Recommendation 3: Clauses 54 and 49 should be amended to enable access to personal information by criminal law enforcement bodies only when:

- a judicial warrant is provided in relation to a serious criminal offence, adopting the definition of 'serious offences' in section 5D of the *Telecommunications Interception and Access Act* (Cth).
- for the purposes of investigating serious criminal fraud and cyber-security incidents directly related to the scheme.
- in circumstances where the personal information is released, on request by the affected individual, directly to the individual, enabling them to choose whether to share it with a law enforcement body.

Recommendation 4: Clauses 136 should be amended to provide a more specific data retention periods with respect to all personal information or, at the very least, to task the ACCC or OAIC with providing guidance on appropriate data retention periods.

Recommendation 5: Clause 53(3)(a) should be amended to provide that data profiling is permitted only to address technical issues, rather than in service provision more broadly.

Recommendation 6: The Bill should be amended to:

- include an explicit process for determining whether a state or territory privacy law meets the requisite level of protection required by the Bill. This assessment should be made by the OAIC
- expressly provide for the Information Commissioner's jurisdiction in respect of privacy protections in the Rules.

Recommendation 7: the Australian Government should take a nationally harmonised approach to digital identity systems by adopting a distributed model, rather than a centralised model.

Recommendation 8: The Bill should define and specify requirements for the provision of express consent; and require the provision of information about the option to withdraw consent, and accessible means of withdrawing consent at any time.

Recommendation 9: The Bill should incorporate the 'fair and reasonable' test, as set out in the Attorney-General Department's Privacy Act Review.

Recommendation 10: To ensure voluntariness is upheld in practice, clause 74 should be amended:

- to include an ongoing guarantee of equal access to services for those who choose to opt out of using a digital ID
- to require the Digital ID Regulator to consider whether granting an exemption would unduly undermine access to services for individuals in the circumstances.

Recommendation 11: To strengthen the development of inclusive and accessible practices, clause 30 should require the following in the development of the Accreditation Rules.

- The human rights of affected groups should be identified and taken into account when developing accessibility and inclusion standards.
- Testing and consultation should be conducted with users from diverse cohorts.
- Training of relevant staff on accessibility issues should be required.
- Support services should be provided for individuals requiring assistance to set up and use digital ID.
- There should be protocols and assistance that enable people to provide alternative forms of identity documents to set up their Digital ID without being disadvantaged within the system
- No fees should be charged directly to individual users by accredited entities or relying parties.

Recommendation 12: Clause 10 should be amended to reflect terminology and definitions in Australia's anti-discrimination legislation; and clause 11 should be amended to include information about disability as a restricted attribute.

Recommendation 13:

- Clause 88 should be amended to require that an accessible redress mechanism for individuals be set up through Digital ID Rules prior to the commencement of the scheme. The redress mechanism should provide for remedies and be adequately resourced.
- The Digital ID Rules should also provide for internal feedback mechanisms and protocols for addressing or escalating complaints, and referring system-level issues to regulators.

Recommendation 14: The Government should introduce legislation to regulate all forms of facial recognition technology, by implementing HTI's model law.

Recommendation 15: Implementation of the Bill should be supported through a robust public education initiative and access to information about privacy assessments, performance outcomes and complaints in relation to the scheme.

Recommendation 16: Clause 162 should be amended to enable an interim review of the legislation after 12 months of operation.

Recommendation 17: Clause 9 of the Digital ID (Transitional and Consequential Provisions) Bill 2023 should be deleted, to restore the requirement to consult on Rules in the six-month period following commencement of the Digital ID Bill.

Background to the Bill

Digital identity technology promises great benefits in terms of user convenience and enhanced security for personal information. There are also benefits for government and business in simpler, more secure systems for proving an individual's identity.

Nevertheless, any digital ID scheme also carries substantial risk, especially if personal information is compromised. The risk of harm is even more significant when biometric information is relied upon to verify an individual's identity, as is the case with the scheme proposed by the Bill. Strong privacy and other rights protections are necessary

to realise the promise of a more secure and effective way of verifying people's identity, and to provide a solid foundation of public trust in the use of digital ID.

The Bill would establish a voluntary Accreditation Scheme for entities providing digital ID services.[13] The Bill would also provide a legislative basis for the AGDIS, which facilitates the use of government-issued digital IDs by individuals accessing government services, and would enable its expansion for use by Commonwealth, state and territory governments, and eventually private sector organisations.

Need for legislative consistency

The Bill directly intersects with other legislation – notably the Privacy Act and the recently passed *Identity Verification Services Act 2023* (Cth) (**IVS Act**).

The Privacy Act, in its current form, does not provide sufficient protections in the context of digital ID. Following the Attorney-General's Department's Privacy Act Review (**Privacy Act Review**), the Australian Government indicated an intent to implement a range of reforms to the Privacy Act, which are yet to be made.[14] The Bill deals with the limitations of the Privacy Act by extending privacy protections in the Bill beyond what is required by the Act.

In December 2023, the IVS Act and the *Identity Verification Services (Consequential Amendments) Act 2023* (Cth) were passed by the Australian Parliament. Together they provide a legislative basis for many pre-existing identify verification services. The IVS Act is intrinsically linked with the broader Digital ID Bill as similar services operate under both regimes, with similar associated risks. While the IVS Bill initially adopted an inferior approach to privacy protections, a number of welcome amendments were made prior to its passage into law,[15] which has brought it into closer alignment with the Digital ID Bill.

Ideally, digital ID reforms would have been made through a consistent and coordinated legislative reform process – *after* the Privacy Act amendments were introduced, and *before* identity verification and digital IDs were widely adopted for use by Government. As this was not the reform sequence, it is essential that Privacy Act reforms be passed *as soon as possible* to prevent further fragmentation, inconsistencies, gaps in protections, and unnecessary compliance burdens. Going forward, a coordinated approach across relevant departments and regulators, including those at the state and territory level, must be adopted towards digital ID to ensure the success of the scheme(s).

Future changes to the Privacy Act, in response to the Privacy Act Review, should also be reflected in these Acts, which may require consequential amendments to ensure that they remain consistent with any additional obligations or changed terminology. The reforms proposed by the Privacy Act Review would strengthen both the IVS Act and the Digital ID Bill – for example, through requiring a 'fair and reasonable' test for the collection and use of data.[16] A harmonised approach across all three Acts can also be

[13] Based on the 'Trusted Digital Identity Framework', *Australia's Digital ID System* (Web Page) <https://www.digitalidentity.gov.au/tdif>.
[14] Attorney-General's Department, Government Response: Privacy Act Review Report (Government Response, 28 September 2023).
[15] Amendments included extending the application of the Privacy Act to IVS services, requirements for express consent, alignment with the existing data breach regime, the introduction of use limitations and a ban on data profiling and marketing. See Parliament of Australia, *Identity Verification Services Bill 2023: Schedule of the amendments made by the Senate* (December 2023) <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fsched%2Fr7085_sched_cd2a8998-cfeb-4d24-b856-6bca4061269c%22>.
[16] Attorney-General's Department, *Privacy Act Review Report* (February 2023) Proposals 12.1- 12.3.

achieved through legislative review processes occurring along similar timelines, as outlined further below.

Recommendation 1: The Australian Government should adopt a consistent and coordinated approach to federal privacy protections and digital ID. Anticipated amendments to the Privacy Act should be passed as soon as possible, and consequential amendments made to both the IVS Act and Digital ID Bill to address any inconsistencies.

Privacy protections

As noted above, HTI supports the provision of additional privacy protections in the Bill, beyond the general requirements of the Privacy Act. Those provisions are located primarily in Chapter 3 of the Bill.

However, some of the privacy provisions in Chapter 3 should be tightened to close potential gaps, and ensure that protections are robust and reliable. Strong privacy protections are necessary to comply with Australia's international human rights law obligations. The right to privacy is protected under article 17 of the International Covenant on Civil and Political Rights, and is enshrined in other international human rights instruments that bind Australia.[17] Strong privacy protections will also promote public trust in the federal digital ID ecosystem, thereby increasing the total number of people likely to opt in to the scheme.

Scope of privacy protections

Clause 33 of the Bill provides that Chapter 3 'applies to accredited entities only to the extent the entity is providing its accredited services'. This clause has been adapted since the Exposure Draft provided by the Department of Finance for public consultation. The wording in the Exposure Draft extended coverage to 'entities that are providing accredited services *or doing things that are incidental or ancillary to the provision of those services.*'[18]

The removal of the extension of privacy obligations to 'incidental or ancillary' activities inappropriately reduces the scope of the protections. The current wording would mean that, for example, a data security breach related to the digital ID scheme, which occurred in the course of a company-wide IT update, may not be covered by the privacy obligations in the Bill.

A person affected by a data breach or other privacy infringement will experience the same level of harm regardless of whether it occurred directly in the course of an accredited entity providing an accredited service, or incidental to it. Entities should be expected to exhibit the same degree of caution when handling personal data for incidental purposes.

In order to promote privacy and security of personal information, which are stated objects of the Bill,[19] the scope of clause 33 should extend to 'incidental and ancillary' activities, to match the Exposure Draft wording.

---

[17] *International Covenant on Civil and Political Rights*, art 17; *Universal Declaration of Human Rights*, art 12; *Convention on the Rights of the Child*, art 16. See also Australian Human Rights Commission, *Human Rights and Technology* (Final Report, May 2021).
[18] Department of Finance, *Digital Identity Bill 2023 Consultation* (Exposure Draft September 2023) cl 31(b).
[19] Cl 3(b).

Recommendation 2: Clause 33 of the Bill should be amended to include entities that are 'doing things that are incidental or ancillary' to the provision of accredited services.

Access to personal information for law enforcement purposes

Clause 54 of the Bill provides that personal information, which is not biometric information, can be disclosed to an 'enforcement body' for a number of purposes – including when an accredited entity is satisfied that an enforcement body has 'started proceedings' against a person, either for an offence against a law or 'in relation to breach of a law imposing a penalty or sanction'. Personal information may be disclosed also with the express consent of the individual to which it relates in order to verify their identity or investigate an offence. An 'enforcement body' is stated to have the same meaning as in the Privacy Act, which includes criminal law enforcement agencies and a range of other bodies, such as the Department of Home Affairs and authorities with powers to issue civil penalties or sanctions.[20]

Clause 49(3) limits the disclosure of biometric information to a criminal 'law enforcement agency' when authorised by a warrant, or with the express consent of the individual to which it relates in order to verify their identity or investigate an offence.

Access to *any* personal information from the digital ID scheme for law enforcement purposes should be highly restricted. Access should be limited to the following circumstances:

- Where a judicial warrant is provided in relation to a serious criminal offence. A 'serious offence' should be understood to meet the definition of 'serious offences' in section 5D of *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act). The TIA Act regulates access to communications information by law enforcement bodies via warrants and the definition is transferable to the digital ID context.
- Where access is necessary to investigate serious criminal fraud or cyber-security incidents relating to the scheme. Information obtained through this exception should be used only for matters that are directly relevant to the investigation of such incidents.
- Where the affected individual has provided express consent (or requested) to release personal information to *themselves*. In this scenario, the individual could then make the decision to share it with a law enforcement body.

Anything beyond this is too broad and risks creating distrust – in much the same way as occurred with the My Health Record scheme,[21] and COVID tracing apps.[22]

The stated objects of the Bill would be undermined without strict use limitations in this context. Providing assistance to law enforcement is not one of the purposes of this legislation, and weakens privacy protections that give the Bill a clear and bounded operation.[23] If Australians believe that the digital ID scheme will be used significantly to chase fines, small debts and for other law enforcement purposes, rather than as a way

[20] *Privacy Act 1988* (Cth) s 6.
[21] Paul Karp, 'Police can access My Health Record without court order, parliamentary library warns', *The Guardian* (online, 5 July 2018) <https://www.theguardian.com/australia-news/2018/jul/25/police-can-access-my-health-record-without-court-order-parliamentary-library-warns>.
[22] Graeme Greenleaf and Katharine Kemp, 'Police access to COVID check-in data is an affront to our privacy. We need stronger and more consistent rules in place' *The Conversation,* 7 September 2021 <https://theconversation.com/police-access-to-covid-check-in-data-is-an-affront-to-our-privacy-we-need-stronger-and-more-consistent-rules-in-place-167360>; Max Koslowski, 'Attorney-General to ban police from accessing coronavirus app metadata', *Sydney Morning Herald* (online, 22 April 2020) <https://www.smh.com.au/politics/federal/attorney-general-to-ban-police-from-accessing-coronavirus-app-metadata-20200422-p54m6e.html>.
[23] Cl 3.

of improving how government and the private sector delivers services, then it's likely that millions of Australians, who would otherwise be open to participating, will not have the level of trust needed to adopt a digital ID.

Recommendation 3: Clauses 54 and 49 should be amended to enable access to personal information by criminal law enforcement bodies only when:

- **a judicial warrant is provided in relation to a serious criminal offence, adopting the definition of 'serious offences' in section 5D of the *Telecommunications Interception and Access Act* (Cth).**
- **for the purposes of investigating serious criminal fraud and cyber-security incidents directly related to the scheme.**
- **in circumstances where the personal information is released, on request by the affected individual, directly to the individual, enabling them to choose whether to share it with a law enforcement body.**

Data retention and destruction of data

There are several clauses in the Bill that relate to data retention. With respect to biometric data, there is provision for the immediate destruction of data post-verification (clause 51), which is necessary and welcome.

Clause 29 provides that a digital ID must be deactivated upon request 'as soon as practicable after receiving the request'. Clause 136 provides for the destruction and de-identification of personal information more generally, but does not mention withdrawal of consent or specify a data retention period.

The Bill should be strengthened by specifying clear data retention periods in clause 136 for all forms of personal information, beyond biometric information. Australian Privacy Principle (APP) 11 states that 'where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified.'[24] A provision along these lines could offer a balanced approach: one that makes clear that personal information should not be retained indefinitely, but without specifying a one-size-fits-all retention period. In any event, it would also be helpful if the Bill tasked the ACCC or OAIC to provide guidance on retention periods.

In its submission to the Exposure Draft of the Bill, the OAIC noted that without specified data retention periods, 'there is an increased risk that an individual's personal information will be held for longer than is necessary and become compromised in the event of a data security incident'. The OAIC observed that the Australian Government has recognised data retention risks by agreeing in principle with the Privacy Review recommendation to 'undertake a review of all legal provisions that require retention of personal information' to determine if they are appropriate.[25] The Bill should therefore be tightened to better address data retention risks, and the Committee should recommend maximum data retention periods for inclusion in the Bill.

Recommendation 4: Clauses 136 should be amended to provide a more specific data retention periods with respect to all personal information or, at the very least, to task the ACCC or OAIC with providing guidance on appropriate data retention periods.

---

[24] OAIC, *Australian Privacy Principles Guidelines* (online) Chapter 11, 'APP 11 Security of Personal Information' <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information>.

[25] Office of the Australian Information Commissioner, Submission to the Department of Finance, *Digital Identity Bill 2023 Consultation* (October 2023).

Prohibition on data profiling

The prohibition on data profiling or tracking, and the prohibition on personal information being used or disclosed for marketing purposes are welcome inclusions in the Bill (cl 53, 55). Clause 53(3) provides some exemptions to the data profiling prohibition, including where the use or disclosure is 'for purposes relating to the provision of the entity's accredited service (*including* improving the performance or usability of the entity's information technology systems through which those services are provided).'

To ensure that this clause is not interpreted overly broadly (for example, enabling personalisation or targeting for a range of business purposes), the wording should be tightened so that it allows data profiling *only* for the improvement of technical issues relating to performance or usability.

Recommendation 5: Clause 53(3)(a) should be amended to provide that data profiling is permitted only to address technical issues, rather than in service provision more broadly.

Clarity regarding role of the Information Commissioner in regulating privacy matters, and coverage of the Privacy Act

There are two regulators with roles under the digital ID scheme – the Digital ID Regulator (ACCC) and the Information Commissioner. Both regulators will need to coordinate in order to effectively regulate the scheme. The OAIC must have sufficient powers and certainty to regulate all the privacy-related aspects of the scheme. There are some elements of the Bill that can be improved in this regard.

The Bill specifies criteria that a state or territory privacy law must meet in order for state or territory accredited entities to do an act or engage in a practice with respect to personal information under the digital ID scheme.[26] This includes a requirement that the law offer a level of protection of personal information comparable to that provided by the Australian Privacy Principles. State and territory entities will also be covered by the Notifiable Data Breach scheme in the Privacy Act, unless they are covered by a comparable state or territory scheme.[27]

As noted by the OAIC in its submission to the Exposure Draft of the Bill, the Bill lacks a process for 'formally assessing equivalency of state and territory privacy laws and does not specify who will be responsible for the assessment'.[28] HTI endorses the OAIC's recommendation that the Bill incorporate an express mechanism for determining whether a state or territory law meets the relevant criteria.[29] The OAIC would be best placed to make this assessment.

Additionally, the Accreditation Rules, which will be administered by the ACCC, involves oversight over matters related to the handling of personal information. The privacy aspects of the Rules should be within the remit of the Information Commissioner to enforce, but it is not clear in the Bill that this is the case. HTI endorses the OAIC's recommendation that the Information Commissioner be provided with explicit power to enforce privacy protections in the Rules.

[26] Cl 36(2)(b).
[27] Cl 40(2)(b).
[28] Office of the Australian Information Commissioner, Submission to the Department of Finance, *Digital Identity Bill 2023 Consultation* (October 2023).
[29] Office of the Australian Information Commissioner, Submission to the Department of Finance, *Digital Identity Bill 2023 Consultation* (October 2023).

Clause 36 of the Bill sets out criteria for non-APP entities to ensure that they are covered by legislation equivalent to the Privacy Act or that there is a non-APP agreement in place, so that Privacy Act obligations apply.

An alternative approach could be for accredited entities to be explicitly made subject to the Privacy Act without the need for additional steps. Section 6E(1)(d) of the Privacy Act extends Privacy Act coverage to small businesses accredited under section 56CA(1) of the *Competition and Consumer Act 2010* (Cth). This approach could be adopted in relation to accredited entities under the digital ID scheme.

Recommendation 6: The Bill should be amended to:

- **include an explicit process for determining whether a state or territory privacy law meets the requisite level of protection required by the Bill. This assessment should be made by the OAIC**
- **expressly provide for the Information Commissioner's jurisdiction in respect of privacy protections in the Rules.**

A note on decentralised digital identity architectures

The AGDIS and TDIF adopt a centralised 'hub and spoke' model. This means that identity authentication and attribute-sharing processes take place on the government server side, rather than on the customer side. There are two main critiques of this kind of centralised approach to digital identity systems:

1. **Data security risks:** As the name suggests, centralised identity architectures rely on a central system and are therefore more at risk of a single point of failure or security breach.
2. **Agency and ownership:** centralised models place control of users' personal information and identity exchanges into the hands of the provider (the Government), rather than the individual.

In contrast to the Commonwealth's centralised identity architecture, the NSW Government's Digital ID and Verifiable Credentials system is based on a distributed model. There are several compelling useability and rights-based benefits of this model, including:

- stronger privacy safeguards and user agency through data minimisation and personal identity information being stored on each user's device, rather than a centralised server. This also reduces susceptibility to, and scalability of, cyberattacks
- the ability for the system to work offline and online
- no single point of failure between providers.

This decentralised identity architecture is considered better practice and mirrors the approach taken by the European Union's Digital Identity Wallet.

While the Australian Government has committed to ensuring interoperability across Australian jurisdictions via 'seamless Commonwealth, state and territory digital identity systems', affirmed in Principle 1 of the 2023 National Strategy for Identity Resilience, HTI recommends that the Australian Government also take a nationally harmonised approach to digital identity systems by moving towards a distributed model.

Recommendation 7: the Australian Government should take a nationally harmonised approach to digital identity systems by adopting a distributed model, rather than a centralised model.

Consent and autonomy

Express consent

HTI welcomes the centrality of express consent to the digital ID scheme. For example, the Bill would require an individual's express consent for the disclosure of an attribute or restricted attribute of the individual to the relying party (clauses 45 and 46); collection, use or disclosure of biometric information (clause 48(1)); and use or disclosure of personal information to conduct testing in relation to the AGDIS (clause 82).

The provisions requiring express consent could be strengthened by including a definition of express consent, and an explanation of how it should be obtained. Key requirements are outlined in the *Australian Privacy Principles Guidelines*.[30] Among other things, consent for Digital ID should be explicit, opt-in, current and specific. Clear, accurate information should be provided to individuals about how their information is being collected and used, and specific information should be provided about the use of biometrics.

The Bill would enable individuals who have consented to the Digital ID Scheme to deactivate their Digital ID upon request.[31] It is important for individuals to be able to *easily* adjust their preferences with respect to disclosure of personal information and withdrawal of consent. There should be a provision in the Bill requiring proactive provision of information about the option to withdraw consent at any time, and an accessible means of doing so.

Consent should not be the only criterion on which to base decisions regarding the use, collection and disclosure of personal information. The potential for harm associated with the sensitivity of information and the scope that can be collected means that a higher standard is required. The limitations of relying on consent has been well-recognised,[32] and the Privacy Act Review recommended the adoption of an objective 'fair and reasonable' test for the processing of personal information, to which the Government has agreed in principle.[33] This test should be included in the Bill, ahead of anticipated reforms to the Privacy Act.

Recommendation 8: The Bill should define and specify requirements for the provision of express consent; and require the provision of information about the option to withdraw consent, and accessible means of withdrawing consent at any time.

Recommendation 9: The Bill should incorporate the 'fair and reasonable' test, as set out in the Attorney-General Department's Privacy Act Review.

---

[30] OAIC, *Australian Privacy Principles Guidelines* (December 2022) 9 – 13.
[31] Cl 29.
[32] See, e.g., Neil Richards and Woodrow Hartzog, 'The pathologies of digital consent', *Washington University Law Review*, 96 (2019) 1461; Future of Privacy Forum and Asian Business Law Institute, *Australia: Status of consent for processing personal data* (Jurisdiction Report, June 2022) <https://fpf.org/wp-content/uploads/2022/06/20220628-ABLI-FPF-Consent-Project-Australia-Jurisdiction-Report.pdf>.
[33] Attorney-General's Department, *Government Response: Privacy Act Review Report* (Government Response, 28 September 2023) 8.

Voluntariness

Consent is only meaningful when people are not unreasonably disadvantaged if they opt to use traditional methods of proving their identity; in other words, they must retain equal entitlements and access to the same services and products. Clause 74 provides that creating and using a digital ID is voluntary – participating relying parties 'must not, as a condition of providing a service or access to a service, require an individual to create or use a digital ID.' Clause 74 is an essential requirement to ensure that people's rights are respected in relation to the scheme.

However, the Statement of Compatibility with Human Rights states, with respect to disability rights, that 'clause 74 of the Bill is a potential limitation on the rights of people with disability if they choose not to create a digital ID' because 'the Bill does not guarantee the same level of access, or that access must be as effective as the use of a Digital ID to services that are currently in existence prior to the implementation of the framework.'[34]

This is a concerning statement. Equal access to services regardless of the *means* of proving one's identity is necessary to ensure that engaging with digital ID is genuinely voluntary and consent-based, particularly with respect to essential government services where people have no other choice of service. In other words, if people, including those with disability, choose not to use a digital ID to access services, the government must ensure that the option of alternate methods of identity verification (such as face-to-face interactions at a service centre) remain in place into the future and do not become unreasonably burdensome to users. If the ongoing quality of these service are not guaranteed, there is a risk that people may end up feeling coerced into adopting a digital ID to engage with government, even if they do not want to.

Without this guarantee, indirect discrimination and exclusion may result for groups that face barriers to using digital ID, such as people with disability, older people, a disproportionate number of First Nations people, people from remote areas and digitally excluded groups – as discussed further in the next section. While efforts to make digital ID accessible and inclusive are commendable, it must also be recognised that there will always be a cohort for whom digital ID is not accessible or usable, who are already facing exclusion and marginalisation – which can be exacerbated through this scheme if it is not truly voluntary. This is particularly the case for large swathes of the country that do not have reliable access to the internet, a phone or mobile data.[35] There will also be many people who wish to opt out due to a lack of trust or comfort with the use of biometrics – they should not face disadvantages as a result of this choice. This is illustrated by the OAIC's 2023 *Community Attitudes Survey,* which found that only 49% of Australians are comfortable with one-to-one uses of biometric information.[36]

For the above reasons, clause 74 should be amended to include an explicit guarantee of *equal* access to services for those who opt out of digital ID.

The Digital ID Regulator may grant exemptions to the voluntariness clause. It is welcome that Commonwealth entities are not subject to exemptions (clause 74(6)), and that exemptions can only be granted upon requests. However, the available grounds

[34] Statement of Compatibility, Digital ID Bill 2023 (Cth) [40].
[35] See Australian Digital Inclusion Index, ***Measuring Australia's Digital Divide*** (Report, 2023) <https://www.digitalinclusionindex.org.au/>.
[36] Comfort levels drop further in relation to one-to-many uses of biometrics, which is not proposed by the Bil:. OAIC, ***Australian Community Attitudes to Privacy Survey 2023*** (Report, August 2023) <https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023>.

for exemptions for non-Commonwealth relying parties are fairly broad. They include (at clause 74(5)):

- The relying party provides services or access to services only online
- The relying party is providing services or access to services in exceptional circumstances.

In order to prevent unfairness, grounds for exemptions could be tightened. For example, in relation to the second category, the Bill does not specify what is meant by 'exceptional circumstances', though the Explanatory Memorandum states that this may include 'flood or fire'.[37]

As noted by the ACT Human Rights Commission in their submission to the Exposure Draft, there is potential for the scheme to be 'voluntary' in theory, but 'in practice, individuals who do not wish to use Digital ID may be excluded from accessing accredited services that either rely on or require the use of Digital ID where an exemption has been granted.'[38] A natural disaster is precisely the kind of situation where people may need flexibility and access to alternatives – for example they may lose access to their internet or phone. Care should be taken to ensure that the exemptions do not result in exclusion or tiered service delivery in 'emergency' situations or in circumstances where there is a lack of choice between service providers – for example in remote communities. These points can be dealt with by requiring the Digital ID Regulator to consider whether granting an exemption would unduly undermine access to services for individuals in the relevant circumstances.

Recommendation 10: To ensure voluntariness is upheld in practice, clause 74 should be amended:

- **to include an ongoing guarantee of equal access to services for those who choose to opt out of using a digital ID**
- **to require the Digital ID Regulator to consider whether granting an exemption would unduly undermine access to services for individuals in the circumstances.**

Accessibility, inclusion, user-centricity and non-discrimination

In order to realise the potential benefits of digital ID, it must be accessible for, and inclusive of, all eligible users. This includes people with disability, older people, people from culturally and linguistically diverse backgrounds (CALD), and people living in regional or remote areas. As discussed above, it is also essential to ensure that there are equal alternatives to the use of digital ID for those who need it, to prevent indirect discrimination.

Clause 30 provides that 'accredited services must be accessible and inclusive'. The Accreditation Rules will address the specific requirements, with clause 30(2) providing a non-exhaustive list of relevant matters – including requirements to comply with accessibility standards or guidelines, requirements relating to user-testing, and requirements relating to device or browser access. Clause 28(2)(a) allows for the Accreditation Rules to outline user experience and inclusion requirements that must be met in order to become and remain an accredited entity. This clause could also usefully

[37] Explanatory Memorandum, Digital ID Bill 2023 (Cth) [327].
[38] ACT Human Rights Commission, Submission to the Department of Finance, *Digital Identity Bill 2023 Consultation* (October 2023).

provide more specific requirements with respect to the development of rules around accessibility and inclusion.

Accessibility and inclusion criteria should explicitly take into account the human rights of groups that may be adversely affected by the scheme. These include the rights of people with disability, children, First Nations people, and those who depend on access to essential services such as social security (noting that digital ID is integrated into the social security system, and the social security cohort includes highly vulnerable people).

This lens is particularly important with respect to facial verification technology, which carries risks of misidentification and bias[39] – indicating a need for rigorous design and ongoing monitoring of digital identity products and services, by reference to non-discrimination and access rights.

Additionally, there should be provision for:

- consultation and testing with individuals from diverse demographic groups
- relevant staff to be trained in the accessibility implications for digital ID to mitigate the risk of adverse outcomes for people in affected groups
- human assistance readily available to enable people to set up and use their digital ID
- protocols and assistance that enable people to provide alternative forms of identity documents to set up their Digital ID without being disadvantaged within the system – noting that certain groups are less likely to have access to official identity documents.[40] Currently, to gain the strongest level of digital ID, a person must have access to a passport, which excludes many Australians.[41]

A further accessibility consideration relates to the charging of fees. The Bill precludes rules being made that would charge an individual a fee to create a digital ID to use in the AGDIS.[42] However, this explicit preclusion does not appear to apply to accredited entities that are not participating in the AGDIS. The charging of fees to individuals could lead to exclusion from private sector digital ID services, and increase data protection risks for those who cannot afford fees, contrary to the intention of the Bill. For these reasons, the Bill should explicitly prevent the charging of fees to individual users by *all* accredited services and relying parties.

Recommendation 11: To strengthen the development of inclusive and accessible practices, clause 30 should require the following in the development of the Accreditation Rules.

- **The human rights of affected groups should be identified and taken into account when developing accessibility and inclusion standards.**
- **Testing and consultation should be conducted with users from diverse cohorts.**
- **Training of relevant staff on accessibility issues should be required.**
- **Support services should be provided for individuals requiring assistance to set up and use digital ID.**

[39] Human Technology Institute, *Facial recognition technology: Towards a model law* (Report, September 2022), 28.
[40] Including First Nations people in remote communities, refugees, people fleeing domestic violence, people who have experienced a natural disaster.
[41] 'How to set up MyGov ID', *MyGov* (Web Page) <https://www.mygovid.gov.au/set-up>.
[42] Cl 144(3).

- **There should be protocols and assistance that enable people to provide alternative forms of identity documents to set up their Digital ID without being disadvantaged within the system**
- **No fees should be charged directly to individual users by accredited entities or relying parties.**

Definition of 'attributes' and 'restricted attributes'

The Bill would extend the meaning of 'personal information' (as understood in the Privacy Act) to include attributes of individuals. This means that information that is associated with an individual and can be derived from another attribute is considered personal information for the purposes of the Bill. Clause 10 provides a non-exhaustive list of attributes, and clause 11 sets out 'restricted attributes' which are particularly sensitive and warrant a higher level of protection.

Accredited entities are prohibited from collecting information related to attributes – such as a person's 'racial or ethnic origin', 'religious beliefs or affiliations', 'philosophical beliefs', and 'sexual orientation or practices'. Although these categories link with protected attributes under Australia's anti-discrimination laws,[43] the Bill does not consistently use terminology adopted in Australia's anti-discrimination framework, nor refer to the relevant laws. This section should be redrafted to align this clause with well-established legal definitions to ensure a consistent approach.

Similarly, restricted attributes include 'health information' among other categories, but do not include information about disability. The Explanatory Memorandum states that while consideration was given to including disability as a restricted attribute, the choice was made to not include it since there is 'not yet an accepted definition of "disability" in Australian law'. However, section 4 of the *Disability Discrimination Act 1992* (Cth) *does* provide an accepted legal definition of disability.

While 'health information' is defined in the Privacy Act[44] to include information related to disability, for the purposes of clarity and completeness, clause 11 should explicitly reference disability as a restricted attribute.

Recommendation 12: Clause 10 should be amended to reflect terminology and definitions in Australia's anti-discrimination legislation; and clause 11 should be amended to include information about disability as a restricted attribute.

Redress for individuals

There are significant risks to individuals associated with misuse and data breaches under the scheme, particularly with respect to biometric data – regardless of the strengths of safeguards and civil penalties in place. Individuals whose privacy or other human rights have been breached by the actions of an accredited entity should have an effective process through which to submit a compliant about the entity's actions, and be provided with redress proportionate to the harm they have suffered.

[43] Federal discrimination laws include: *Racial Discrimination Act 1975* (Cth); *Sex Discrimination Act 1984* (Cth); *Disability Discrimination Act 1992* (Cth); *Age Discrimination Act 2004* (Cth); *Australian Human Rights Commission Act 1986* (Cth); *Fair Work Act 2009* (Cth).
[44] *Privacy Act 1988* (Cth) s 6FA.

Clause 88 of the Bill states that the 'Digital ID rules *may* provide for or in relation to a redress framework' for incidents in relation to the AGDIS scheme. Notably, the Draft Digital ID Rules released for public consultation did not provide for a redress scheme.[45]

The Bill should explicitly provide for a redress scheme, with the details of the redress scheme to be set out in the Digital ID Rules. These details should be made publicly available prior to the passage of the Bill.

A redress mechanism set up by the Bill or Digital ID Rules should include provisions for remedies (including monetary remedies), and provide a simple, practical and accessible avenue for complaints. While clause 88 sets out a range of matters that a redress framework may deal with, this list does not currently include provisions for sufficient remedies or accessibility considerations.

The redress mechanism should allow an individual to submit complaints about the handling of their information by accredited service providers and relying parties (including those not participating in the AGDIS). Ideally, the complaints-handling body should be the same for both the IVS Act and Digital ID Bill schemes, with provision for joined-up complaints. The redress mechanism also needs to be adequately resourced to effectively fulfil its role and enable the timely resolution of matters – noting that the existing complaints mechanisms for most of Australia's information regulators have large backlogs of complaints due to insufficient resourcing.

Outside of an external redress mechanism, the Digital ID Rules should also provide for internal feedback mechanisms for people to report errors or exclusions related to digital ID, and require the development of protocols for resolving these issues or escalating complaints. There should also be provision for internal complaints to be monitored and assessed to identify any patterns indicating system level issues and referred to the Digital ID Regulator and/or Information Commissioner.

Recommendation 13:

- **Clause 88 should be amended to require that an accessible redress mechanism for individuals be set up through Digital ID Rules prior to the commencement of the scheme. The redress mechanism should provide for remedies and be adequately resourced.**
- **The Digital ID Rules should also provide for internal feedback mechanisms and protocols for addressing or escalating complaints, and referring system-level issues to regulators.**

Need for specific regulation of facial recognition technology

Both the Digital ID Bill and the IVS Act seek to regulate facial recognition technology (FRT) in a limited way by restricting the use of one-to-one and one-to-many facial recognition in the context of the digital identity scheme. However, more broadly, FRT remains largely unregulated in Australia.

There is an increasing number of private sector companies offering one-to-many FRT services that, on their face, severely restrict the right to privacy without adequate human rights justification. Existing Privacy Act provisions only deal with this scenario in a very limited way, and so this activity is largely unregulated. Both the Privacy Act Review and HTI have noted that existing federal law does not sufficiently regulate the use of FRT. The Government's response to the Privacy Act Review explicitly acknowledges the need for further reform in respect of FRT, and states that 'this work

[45] Department of Finance, *Draft Digital ID Rules 2023* (September 2023) <https://www.digitalidentity.gov.au/sites/default/files/2023-09/draft%20Digital%20ID%20Rules%20September%202023_0.pdf>.

should be coordinated with the Government's ongoing work on Digital ID and the National Strategy for Identity Resilience'.[46]

The Committee should call on the Government to make good on its commitment to address the broader issues of FRT reform. HTI has undertaken extensive work in this area, and has outlined a model law for FRT, which has achieved widespread multi-sector support.[47] This model law should be the foundation of broader reform for FRT.

While the need is urgent and important, Parliament has a number of viable options regarding where to locate this broader FRT reform: it could be introduced into the Privacy Act, in a stand-alone FRT statute, in the Digital ID Bill or in another statute. Regardless of whether that broader FRT reform is included in the Digital ID Bill itself, the Committee is well placed to recommend that the Government introduce broader FRT reform as a matter of urgency. Until that broader reform takes place, Australians remain vulnerable to the significant harms associated with misuse and overuse of facial recognition. Moreover, schemes such as the digital ID scheme also remain vulnerable to a catastrophic loss of community trust when a near-inevitable scandal occurs as a result of other organisations misusing FRT.

Recommendation 14: The Government should introduce legislation to regulate all forms of facial recognition technology, by implementing HTI's model law.

Public education and transparency

The Bill contains a number of useful transparency measures, including a public register of accredited entities,[48] the use of trustmarks to indicate that an entity has met accreditation standards,[49] and annual reporting requirements for the Digital ID Regulator and the Information Commissioner.[50] Further transparency measures could include the publication of privacy impact assessments conducted for the purposes of the scheme, public reporting on the outcomes of performance testing, and the number and nature of complaints made by users.

It is important that people are made aware of the risks they undertake when relying on private services that are not accredited by the scheme. Trustmarks and public registers alone are unlikely to be sufficient without further efforts to explain risks to individuals. Proactive public education is crucial in this respect.

There also needs to be public education around how to make a complaint or seek redress, and about individual's rights in relation to the scheme. This is important for securing community trust in the scheme and enabling access to justice.

Additionally, Services Australia should conduct outreach and provide clear information and support to individuals reliant on social security. An explanation should be provided about the benefits and risks of digital ID and an assurance that it is voluntary, and will remain voluntary. Social security recipients should be directed to human assistance if they wish to set up a digital ID, or are having any issues using one.

Recommendation 15: Implementation of the Bill should be supported through a robust public education initiative and access to information about privacy assessments, performance outcomes and complaints in relation to the scheme.

---

[46] Attorney-General's Department, *Government Response: Privacy Act Review Report* (Government Response, 28 September 2023) 10.
[47] Human Technology Institute, *Facial recognition technology: Towards a model law* (Report, September 2022) <https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf>.
[48] Cl 120.
[49] Cl 117.
[50] Cl 154, 155.

Review

Clause 162 provides for the Bill to be reviewed within two years of commencing. The IVS Act will be reviewed after one year. It is prudent for both Acts to be reviewed together, in light of their overlapping applications, and the amended Privacy Act which this Government is committed to introducing into Parliament. As such, it would be preferable to conduct an interim review of the Digital ID Bill after one year to keep it on a similar timeline to the IVS Act.

This review should focus on the operation of the additional privacy protections and associated regulations, as well as the Bill's alignment with the amended Privacy Act. It should also assess the Scheme against accessibility and non-discrimination criteria.

Additionally, many matters have been left to be clarified in the Digital ID Rules or Accreditation Rules, and by the Data Standards Chair, including with respect to a range of:

- privacy measures
- accessibility measures
- performance standards and testing
- redress measures.

These rules require holistic assessment as part of a review process to ensure that they are in place and fit for purpose. This process should also enable consideration as to whether any rules should be included in the primary legislation.

Recommendation 16: Clause 162 should be amended to enable an interim review of the legislation after 12 months of operation.

Requirement to consult on Rules

Clause 169 of the Digital ID Bill requires the Minister to engage in consultations before making or amending Rules under the Bill by legislative instrument. This includes public consultations and consultations with the Information Commissioner on privacy-related Rules. However, clause 9 of the Digital ID (Transitional and Consequential Provisions) Bill 2023 states that this requirement to consult does not apply for a six-month period following commencement of the Bill. While draft versions of the Accreditation Rules and Digital ID Rules were released for public consultation alongside of the Exposure Draft, it is likely that these Rules will undergo some adaptions and require further consideration and input (as has the Bill). Consultation on the updated Rules will be crucial to ensure that they are tested, trusted and fit for purpose. For this reason, clause 9 of the Digital ID (Transitional and Consequential Provisions) Bill 2023 should be removed.

Recommendation 17: Clause 9 of the Digital ID (Transitional and Consequential Provisions) Bill 2023 should be deleted, to restore the requirement to consult on Rules in the six-month period following commencement of the Digital ID Bill.

Interoperability

Clause 79 of the Bill would require entities participating in the AGDIS to ensure interoperability with other digital identity systems. This means that participating accredited entities and participating relying parties would be prevented from refusing to provide services to other participating accredited entities or participating relying parties.

This is an essential feature that will enable individuals to choose their Digital ID provider, and ensure that AGDIS systems work well together. The development of rules in relation to clause 79, as well as with respect to standards and service levels, will assist in enabling technical interoperability between services in practice.

However, clause 79(3)(c)(iv) would allow the Minister to grant an exemption from the interoperability obligation if 'an entity will provide an arrangement to assist individuals who would otherwise be at a disadvantage in accessing the Australian Government Digital ID System.'

It is not clear what is anticipated by this clause, nor is it explained in the explanatory materials. As discussed above, all AGDIS Digital ID services should be accessible to people who are disadvantaged and there are measures that should be taken to strengthen the Bill and rules in this regard. If all services are required to be non-discriminatory, inclusive, and to provide equal access, there would be no apparent need to disturb the interoperability requirement through this provision.

For these reasons, the Committee should request further clarification about how the exemption to interoperability in clause 79(3)(c)(iv) would operate in practice, and consider if universal accessibility requirements would better address any anticipated issues relating to access and interoperability.