



## **NSWCCL SUBMISSION**

### **SENATE ECONOMICS AND LEGISLATION COMMITTEE**

### **DIGITAL ID BILL 2023**

**19 January 2024**

## **Acknowledgment**

In the spirit of reconciliation, the NSW Council for Civil Liberties acknowledges the Traditional Custodians of Country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all First Nations peoples across Australia. We recognise that sovereignty was never ceded.

## **About NSW Council for Civil Liberties**

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

## **Contact NSW Council for Civil Liberties**

<http://www.nswccl.org.au>

[office@nswccl.org.au](mailto:office@nswccl.org.au)

Correspondence to: PO Box A1386, Sydney South, NSW 1235

The New South Wales Council for Civil Liberties (NSWCCL) welcomes the opportunity to make a submission to the Senate Economics and Legislation Committee concerning the *Digital ID Bill 2023* (Bill). The companion *Digital ID (Transitional and Consequential Provisions) Bill 2023* will deal with matters arising from the enactment of the Bill and, as such, has not been reviewed in this submission.

NSWCCL contributed to the public consultation on the Digital Identity Legislation Position Paper 2021<sup>1</sup> and made a short submission on the Digital ID Bill (exposure draft) and Digital ID Rules 2023.<sup>2</sup>

NSWCCL endorses the codification of the Australian Government Digital Identity System (AGDIS) which, along with the Document Verification Service and facial verification technology, has not been operating within an effective legal framework. A number of recent high-profile data breaches has highlighted the lack of regulation and enforcement of identity protection in Australia. This has been the impetus for the fast tabling of this legislation.<sup>3</sup> Tackling cybercrime is one of the touted benefits of the AGDIS.

However, the COVID pandemic normalised the mandatory mass collection, use and storage of personal data using contact-tracing apps and as a result<sup>4</sup> NSWCCL has increased concerns generally with ongoing data centralisation and datafication of Australians.

More particularly, recent amendments to the Bill after the consultation period, have not gone far enough in addressing critical issues, such as the safe collection, use, and storage of sensitive data and ensuring that data is not used for other, unintended purposes like law enforcement.

## 1. Introduction to the AGDIS

- 1.1 Individuals can already create a digital identity using MyGovID to access 80 government services, including Medicare, Centrelink and the Australian Tax Office. The AGDIS will operate by linking an individual's MyGov account on the MyGovID app, and providing an existing identity document (such as a passport, driver's licence or birth certificate), to an identity provider.<sup>5</sup>

To prove one's identity to a participating organisation, an individual would log into the organisation's website and select MyGovID as the verification method, log into the MyGovID app and give consent for identity verification with that organisation, without having to share identity documents.<sup>6</sup>

- 1.2 The Bill supports a voluntary, interoperable accreditation scheme for Digital ID service providers, and expansion of the AGDIS outsourcing the process of identity verification to approved Australian businesses. This will be a phased expansion of the AGDIS, initially across government services and then facilitating the reciprocal or shared use of Digital IDs between public and private sector organisations.

---

<sup>1</sup> NSWCCL Submission: Digital Identity Legislation Position Paper 16 July 2021  
[https://www.digitalidentity.gov.au/sites/default/files/2021-08/53\\_nswccl.pdf](https://www.digitalidentity.gov.au/sites/default/files/2021-08/53_nswccl.pdf)

<sup>2</sup> NSWCCL Submission: Digital ID Bill and Digital ID Rules [https://www.digitalidentity.gov.au/sites/default/files/2023-11/nsw\\_council\\_for\\_civil\\_liberties.pdf](https://www.digitalidentity.gov.au/sites/default/files/2023-11/nsw_council_for_civil_liberties.pdf)

<sup>3</sup> See the Medibank, Optus and Latitude data breaches of 2022–23. Kost, E (Aug 04, 2023) *Biggest Data Breaches in Australia [Updated 2023]* <https://www.upguard.com/blog/biggest-data-breaches-australia>

<sup>4</sup> Nabben, K. (Oct 26 2021) *The government wants to expand the 'digital identity' system that lets Australians access services. There are many potential pitfalls* The Conversation <https://theconversation.com/the-government-wants-to-expand-the-digital-identity-system-that-lets-australians-access-services-there-are-many-potential-pitfalls-170550>

<sup>5</sup> At present, access to the MyGovID may be by, either a PIN or biometric information. <https://www.mygovid.gov.au/how-use-it#:~:text=You%20won't%20need%20to,Settings%20in%20your%20myGovID%20app.>

<sup>6</sup> Mealy, E. (Sept 26 2023) *A national digital ID scheme is being proposed. An expert weighs the pros and (many more) cons* The Conversation <https://theconversation.com/a-national-digital-id-scheme-is-being-proposed-an-expert-weighs-the-pros-and-many-more-cons-214144>



The New South Wales Council for Civil Liberties (NSWCCL) welcomes the opportunity to make a submission to the Senate Economics and Legislation Committee concerning the *Digital ID Bill 2023* (Bill). The companion *Digital ID (Transitional and Consequential Provisions) Bill 2023* will deal with matters arising from the enactment of the Bill and, as such, has not been reviewed in this submission.

NSWCCL contributed to the public consultation on the Digital Identity Legislation Position Paper 2021<sup>1</sup> and made a short submission on the Digital ID Bill (exposure draft) and Digital ID Rules 2023.<sup>2</sup>

NSWCCL endorses the codification of the Australian Government Digital Identity System (AGDIS) which, along with the Document Verification Service and facial verification technology, has not been operating within an effective legal framework. A number of recent high-profile data breaches has highlighted the lack of regulation and enforcement of identity protection in Australia. This has been the impetus for the fast tabling of this legislation.<sup>3</sup> Tackling cybercrime is one of the touted benefits of the AGDIS.

However, the COVID pandemic normalised the mandatory mass collection, use and storage of personal data using contact-tracing apps and as a result<sup>4</sup> NSWCCL has increased concerns generally with ongoing data centralisation and datafication of Australians.

More particularly, recent amendments to the Bill after the consultation period, have not gone far enough in addressing critical issues, such as the safe collection, use, and storage of sensitive data and ensuring that data is not used for other, unintended purposes like law enforcement.

## 1. Introduction to the AGDIS

- 1.1 Individuals can already create a digital identity using MyGovID to access 80 government services, including Medicare, Centrelink and the Australian Tax Office. The AGDIS will operate by linking an individual's MyGov account on the MyGovID app, and providing an existing identity document (such as a passport, driver's licence or birth certificate), to an identity provider.<sup>5</sup>

To prove one's identity to a participating organisation, an individual would log into the organisation's website and select MyGovID as the verification method, log into the MyGovID app and give consent for identity verification with that organisation, without having to share identity documents.<sup>6</sup>

- 1.2 The Bill supports a voluntary, interoperable accreditation scheme for Digital ID service providers, and expansion of the AGDIS outsourcing the process of identity verification to approved Australian businesses. This will be a phased expansion of the AGDIS, initially across government services and then facilitating the reciprocal or shared use of Digital IDs between public and private sector organisations.

---

<sup>1</sup> NSWCCL Submission: Digital Identity Legislation Position Paper 16 July 2021  
[https://www.digitalidentity.gov.au/sites/default/files/2021-08/53\\_nswccl.pdf](https://www.digitalidentity.gov.au/sites/default/files/2021-08/53_nswccl.pdf)

<sup>2</sup> NSWCCL Submission: Digital ID Bill and Digital ID Rules [https://www.digitalidentity.gov.au/sites/default/files/2023-11/nsw\\_council\\_for\\_civil\\_liberties.pdf](https://www.digitalidentity.gov.au/sites/default/files/2023-11/nsw_council_for_civil_liberties.pdf)

<sup>3</sup> See the Medibank, Optus and Latitude data breaches of 2022–23. Kost, E (Aug 04, 2023) *Biggest Data Breaches in Australia [Updated 2023]* <https://www.upguard.com/blog/biggest-data-breaches-australia>

<sup>4</sup> Nabben, K. (Oct 26 2021) *The government wants to expand the 'digital identity' system that lets Australians access services. There are many potential pitfalls* The Conversation <https://theconversation.com/the-government-wants-to-expand-the-digital-identity-system-that-lets-australians-access-services-there-are-many-potential-pitfalls-170550>

<sup>5</sup> At present, access to the MyGovID may be by, either a PIN or biometric information. <https://www.mygovid.gov.au/how-use-it#:~:text=You%20won't%20need%20to,Settings%20in%20your%20myGovID%20app.>

<sup>6</sup> Mealy, E. (Sept 26 2023) *A national digital ID scheme is being proposed. An expert weighs the pros and (many more) cons* The Conversation <https://theconversation.com/a-national-digital-id-scheme-is-being-proposed-an-expert-weighs-the-pros-and-many-more-cons-214144>

- 1.3 There will initially be three types of Digital ID services that can be accredited: identity service providers (currently myGovID); attribute service providers (providing details like educational or business qualifications); identity exchange providers (Services Australia using myGov). Providers of Digital ID services operating within the AGDIS must be accredited and will be subject to additional regulatory requirements, some of which will also apply to participating relying parties. A relying party uses the AGDIS by accepting proof of identity and needs to be approved to use the service but does not need to be accredited.
- 1.4 Accreditation provides a baseline set of obligations and regulatory oversight that apply to all accredited service providers. Accredited service providers will be required to comply with certain privacy, security, consumer protection, record-keeping, data destruction, and other requirements, e.g. governing cyber and fraud incident reporting, liability and fees. Many of these obligations will be set out in the rules.
- 1.5 Digital ID laws will be overseen by a Digital ID regulator – initially the Australian Competition and Consumer Commission (ACCC). However, multiple agencies and regulators will have roles relating to Digital ID, including the Office of the Australian Information Commissioner (OAIC), in regard to privacy breaches, and Services Australia as the AGDIS System Administrator.
- 1.6 Subject to limited exceptions, it must be voluntary for individuals to use Digital IDs within the AGDIS (particularly when accessing government services).<sup>7</sup>
- 1.7 The Digital ID Rules will provide technical detail about identity verification levels, privacy, security, accessibility and usability and additional privacy safeguards that purport to go beyond those in the Privacy Act 1988.
- 1.8 Amendments made to the Bill after the last round of consultation paper include:
  - 1.8.1 Strengthening the position that Digital IDs are voluntary for individuals who need to access government services. There are exceptions to this requirement which NSWCCCL find unacceptable;
  - 1.8.2 Strengthening safeguards over law enforcement access to personal information held by accredited service providers, so that these agencies may only request access to information with consent, a warrant, or where court proceedings have begun. In the exposure draft entities could also disclose information to law enforcement if a law enforcement body reasonably suspected an offence. NSWCCCL believes that the proposed safeguards are not sufficient. There should be no law enforcement access to information in the digital ID system with or without a warrant. Trust in the Digital ID system should at least be on the same level as the Federal COVIDSafe app, which prohibited access to a law enforcement body;
  - 1.8.3 Significantly increasing penalties for breaches of privacy, as well as other safeguards in the legislation. Penalties are an incentive to ensuring obligations are met by the participants. The availability to service providers of a liability shield for strict compliance with the Digital ID regime, may protect service providers from privacy penalties. NSWCCCL considers that a fee waiver should apply to individuals and that obligation should be set out in the primary legislation;
  - 1.8.4 Ensuring that certain types of information classified as prohibited attributes (such as racial or ethnic origin, religious beliefs or sexual orientation) cannot be collected for use in accredited digital ID services. If this information is received in an unsolicited way, it must be

---

<sup>7</sup> S74 Bill- Clause 74(1) provides that a participating relying party (a relying party approved to participate in the AGDIS) must not require an individual to create or use a digital ID as a condition of receiving a service from the relying party or accessing a service through the relying party.



destroyed as soon as practicable.<sup>8</sup> In the exposure draft, this information was allowed to be collected if there was a reasonable excuse.

## 2. Data Governance

- 2.1 Centralised and federated Digital ID systems generally place control of data in the hands of service providers. These systems also create the risk that a piece of authentication information can be leaked, leading to unauthorised logins to multiple services. Ongoing mandatory mass collection and storage of personal data by centralised oversight authorities has become normalised over many years and particularly during the COVID-19 pandemic. As a result, individuals have become disconnected from their personal information and disempowered from owning it.<sup>9</sup> NSWCCCL supports the return to ownership and governance by individuals of their own personal information and identity.
- 2.2 Alternatives to centralised Digital ID systems exist and have been built through Blockchain and Self-Sovereign Identity using blockchain technology.<sup>10</sup> In fact, the final report of the Senate Select Committee on Australia as a Technology and Financial Centre recommends that Australia embrace technologies such as blockchain and decentralised computing.<sup>11</sup>
- 2.3 The Bill envisages alternative methods of digital ID e.g. in s49(2)(a) of the Bill which includes biometric information "that may be contained in a verifiable credential that is in the control of the individual". However, more detailed work needs to be done in the Bill to ensure that there are no barriers to emerging credentials and IDs controlled by the individual.
- 2.4 Clearly set out in the objects of the Bill<sup>12</sup> is the objective of promoting trust in digital ID services. The focus of the AGDIS must clearly be on ensuring that less data is shared and, when shared, stored in the most secure manner. Recent experience with Government entities, particularly in relation to the MyGovID, has fomented some distrust in the community. In 2020, security researchers warned the public against using MyGovID due to security flaws in its design.<sup>13</sup> The Australian government has also failed to secure information, with data breaches and cybersecurity hacks involving the Australian Tax Office, National Disability Insurance Scheme and Defence Forces.<sup>14</sup>
- 2.5 The priority in terms of data governance should be to determine how the system could be more safely implemented, for example, although requirements to delete or destroy any personal information have been tightened<sup>15</sup>, this does not affect the information that the entity may hold in relation to the individual's deactivated Digital ID.<sup>16</sup>

---

<sup>8</sup> S44 Bill

<sup>9</sup> Nabben op.cit.

<sup>10</sup> World Economic Forum (Aug 12 2021) *Self-sovereign identity: the future of personal data ownership?*

<https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/>

<sup>11</sup> [https://www.aph.gov.au/Parliamentary\\_Business/Committees/Senate/Financial\\_Technology\\_and\\_Regulatory\\_Technology/AusTechFinCentre/Final\\_report](https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/AusTechFinCentre/Final_report)

<sup>12</sup> S 3 Bill

<sup>13</sup> Saarinen, J (Sept 21 2020) *Researchers say not to use myGovID until login flaw is fixed* IT News

<https://www.itnews.com.au/news/researchers-say-not-to-use-mygovid-until-login-flaw-is-fixed-553601;>

[https://theconversation.com/the-500-million-ato-fraud-highlights-flaws-in-the-mygov-id-system-heres-how-to-keep-your-data-safe-210459;](https://theconversation.com/the-500-million-ato-fraud-highlights-flaws-in-the-mygov-id-system-heres-how-to-keep-your-data-safe-210459) <https://www.news.com.au/technology/online/hacking/australian-defence-force-confirm-data-breach-hack/news-story/c4c0d955be1f8018e0a19ce9233ad2b4>

<sup>14</sup> Mealy- ABC <https://www.abc.net.au/news/2022-11-28/cyber-black-market-shows-medibank-optus-hack-just-the-surface/101700974>

<sup>15</sup> S56 Bill-prohibits an accredited identity exchange provider from retaining specified attributes of individuals. The section ensures that an exchange cannot be a centralised repository of personal information. It prohibits an exchange from retaining core attributes of an individual, namely name, address, date of birth, phone number and email address, which are not retained after the end of the authenticated session.

<sup>16</sup> S 29 Bill

- 2.6 The retention of sensitive information (including digitalised biometric information) for longer than required or unnecessarily creates opportunities for the hacking of personal information. The proposed AGDIS violates the cautionary advice about not linking all of one's personal information, such as tax history and medical history, which can lead to mass analytics, behaviour profiling and targeted advertising. "It potentially creates a "honeypot" of personal data stored in a centralised database that would offer a tempting target for cyber criminals or hostile nations."<sup>17</sup>

Additionally, the proposed scheme is only as secure as one's phone or other personal device. Having a weak password, losing or having a device hacked could lead to data being compromised.<sup>18</sup>

### 3. Biometrics

- 3.1 According to the OAIC's 2023 Community Attitudes Survey, only 49% of Australians are comfortable with the use of their biometric information to verify their identity online. Only a third are comfortable with that information being used when they want to access a service provided by a business.<sup>19</sup>
- 3.2 The use of biometric technology, at any point of authentication, introduces substantial privacy and security risks. NSWCCCL believes that avoiding biometrics altogether, in the current legislative environment, is the best approach. An individual's biometric information cannot be simply replaced or managed if compromised and is particularly difficult to remedy in the case of a data breach. The NSWCCCL therefore urges the government not to use biometrics as a method of authentication but instead offer non-biometric alternatives for verification within the Digital ID system.<sup>20</sup>
- 3.3 Errors in facial recognition technology may result in an individual being denied an essential government service. "Since FRT relies on computer vision, where recognition is always a one-sided visual assessment, there is a danger of misreading or misrecognising a person's identity. This misrecognition and mislabelling by technology can often counter a person's self-identity, especially when it relates to a person's gender identity or race. FRT has been criticised, particularly in its use by law enforcement agencies, for being violative of civil liberties, and for the potential for abuse, propensity for inaccuracies, and improper use."<sup>21</sup>
- 3.4 Should biometric technology be used for verification, even in a limited way, robust testing should be a prerequisite to its adoption in order to interrogate bias, accuracy, and the impact on vulnerable categories of people. What are the options for those who are excluded by biometric technologies because they have failed to be verified by them?
- 3.5 The Bill does contain some special protections against data breach pertaining to biometric information. This includes requiring accredited identity service providers to immediately destroy biometric information it has collected from an individual for the purpose of verifying that individual's identity after the verification is complete under section 48.<sup>22</sup>
- 3.6 However, the Bill also provides for the Minister to make certain rules to allow the disclosure of biometric information when expressly consented to by the individual. Consent is discussed in further detail later in this paper. NSWCCCL agrees with Digital Rights Watch that, at the very least, such a regime would "be appropriate where additional and more onerous protections apply,

---

<sup>17</sup> Nabben op.cit

<sup>18</sup> Mealy op.cit.

<sup>19</sup> The Office of the Australian Information Commissioner, Community Attitudes to Privacy Survey, 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>

<sup>20</sup> Currently a PIN can be used.

<sup>21</sup> UNSW Allens Hub for Technology, Law and Innovation, Digital Identity and Identity verification bills (2 Oct 2023) [https://www.digitalidentity.gov.au/sites/default/files/2023-11/unsw\\_allens\\_hub\\_for\\_technology\\_law\\_and\\_innovation.pdf](https://www.digitalidentity.gov.au/sites/default/files/2023-11/unsw_allens_hub_for_technology_law_and_innovation.pdf)

<sup>22</sup> s 51(1) Bill



including a fair and reasonable requirement and an obligation placed upon accredited entities that the sharing of a biometric credential be in the best interests of the individual.”<sup>23</sup>

3.7 By linking personal identification data across federal and state jurisdictions, as well as the private sector, the federal government has complete oversight of the lives of Australians. There should be no justification for allowing Digital ID data for surveillance. Accordingly, NSWCCCL recommends that law enforcement agencies be explicitly prohibited from accessing Digital ID data held by any accredited entities.

3.8 Notably the Bill permits disclosure of:

3.8.1 a unique identifier for, amongst other things, detecting, reporting, investigating or prosecuting an offence against a law of the Commonwealth, a State or a Territory (S47(4)(e)), and,

3.8.2 biometric information and personal information, if authorised under a warrant (s49(3)(a) and S54(1)(b)(iii) respectively).

3.9 Accredited entities are prohibited from using or disclosing information about an individual’s online activities, such as the individual’s access and use of the Digital ID services provided by the entity<sup>24</sup>, regardless of consent.<sup>25</sup> However, there are exemptions to this prohibition, including:

3.9.1 for “purposes relating to the provision of the entity’s accredited services (including improving the performance or usability of the entity’s information technology systems through which those services are provided)”.<sup>26</sup> Such an exemption, tempts function creep by accredited entities to personalise and commercialise services.

3.9.2 the prohibition on data profiling to track online behaviour, if the use or disclosure is required or authorised under a law of the Commonwealth, a State or Territory.<sup>27</sup> It is not clear whether this provision would include access by authorised warrant.

NSWCCCL objects to these exemptions. Individuals should have no concerns when using the AGDIS that it may be accessed by law enforcement or for other unauthorised purposes by private enterprise.

#### **4. Voluntary Participation and Equity**

4.1 Equity of access and ownership of one’s digital information must be considered in the context of privilege. The effect on vulnerable members of the community, such as the homeless, refugees, the indigenous population and the disabled community, of not being able to access technology, is profound. A digital identity must not be a precondition to access basic services and rights. Analogue and other accessible digital pathways should be maintained.

4.2 As the AGDIS accesses existing documentation, this will exclude people already without official identification. Individuals who are less digitally literate, without access to digital technology, or with personal objections to Digital ID will also require alternative methods for authentication.

4.3 The Bill provides individuals with the right to voluntarily create and use a digital identity, including the right to deregister and not use a digital identity, at any time.<sup>28</sup> Relying parties need to ensure that use of the AGDIS is not a condition to their supply of a service and that an alternative way to verify identity is available. The interoperability obligation of accredited service providers and

---

<sup>23</sup> Digital Rights Watch (11 Oct 2023) *Submission to the Digital ID Taskforce regarding the Digital ID Bill 2023 exposure draft* [https://www.digitalidentity.gov.au/sites/default/files/2023-12/digital\\_rights\\_watch\\_redacted.pdf](https://www.digitalidentity.gov.au/sites/default/files/2023-12/digital_rights_watch_redacted.pdf)

<sup>24</sup> S53 Bill

<sup>25</sup> S53(2) Bill

<sup>26</sup> S53(3)(a) Bill

<sup>27</sup> S53(3)(c) Bill

<sup>28</sup> S74(1) Bill



relying parties means that there must not be general refusal to provide services to other accredited service providers or relying parties in the AGDIS. NSWCCCL strongly supports simple, accessible, alternatives to accessing services however there is insufficient detail on alternative services in the Bill.

- 4.4 Exceptions to S74 tend to undermine the provision of non-digital alternatives. Exceptions include, where a relying party is a small business, an online-only service, or where the relying party (that is not a Commonwealth service) is providing services, or access to services, in exceptional circumstances. For example, this may apply during an emergency situation such as flood or fire.<sup>29</sup> "Creeping expansion of businesses that superficially satisfy the prescriptive requirements of the law may lead to a slow expansion of the exemption clause. This can, over time, create an ecosystem where despite claims of voluntariness, digital identity becomes both the de facto and de jure DI system, creating anxieties of recognition and sometimes exclusion of people."<sup>30</sup> NSWCCCL sees no justification for, and objects to the exemptions, particularly in an emergency. Further, NSWCCCL has particular concerns about enforcing voluntary participation by accredited and relying service providers.
- 4.5 The Explanatory Memorandum to the Bill explains that "the Bill will not initially provide specific financial or non-financial redress obligations on accredited entities participating in the AGDIS, or on the Regulator. This will be set out in the Digital ID rules."<sup>31</sup> NSWCCCL strongly recommends the detailed provision of redress measures for individuals, within the primary legislation. Individuals should have clear, simple and transparent guidance to remedies for harms suffered, and access to relevant information concerning complaints and conciliation processes. At a minimum, S88 should mandate that a redress framework be developed within a certain, limited timeframe.<sup>32</sup>
- 4.6 Another barrier to equitable access to the AGDIS will be user access fees. Part 6 of the Bill enables rules to be made by the Regulator in relation to fees. NSWCCCL recommends that the Bill prohibits relying parties from passing on fees to individuals and that individuals not be charged to create or deactivate a Digital ID.

### Consent

- 4.7 The Bill provides that the individual in control of their own verifiable credentials must *expressly* consent to any collection, use or disclosure of biometric information contained in such credentials. Various sections in the Bill require an individual's express consent for collection and disclosure, e.g. for biometric information<sup>33</sup>, personal information<sup>34</sup> and for certain attributes<sup>35</sup>. However, obtaining express consent should be far more robust with further obligations to ensure that the consent obtained by entities is both fully informed and voluntary.
- 4.8 Even so, "express consent" will be meaningless in many digital interactions. Opting out of digital interactions is not a realistic option for most individuals. They find that they have to agree to terms of access or risk the suffering of economic disadvantage, discrimination or social exclusion. "[C]onsumers may be informed and understand the inherent privacy risks of providing their personal information but may feel resigned to consenting to the use of their information in order to access online services, as they do not consider there is any alternative. Further, while 'consent' is only a meaningful and effective privacy self-management tool where the individual actually has a choice and can exercise control over their personal information, studies also show that consumers rarely understand and negotiate terms of use in an online environment".<sup>36</sup>

<sup>29</sup> Explanatory Memorandum; S74(5) Bill

<sup>30</sup> UNSW Allens Hub op.cit.

<sup>31</sup> S.88 Bill

<sup>32</sup> Digital Rights Watch op.cit

<sup>33</sup> Ss48 and 49 Bill

<sup>34</sup> S54 Bill

<sup>35</sup> S45 Bill

<sup>36</sup> OAIC 2019 (CCL sub)

- 4.9 The Law Council has suggested, at a minimum, a framework requiring that an accredited entity provide the individual with a clear written or oral statement, explaining the potential consequences of providing consent and any other practical effects or risks associated with the consent. This approach could be adopted in respect of all forms of express consent required under the Bill, including in relation to Ss18 (restricted attributes) and 19 (biometric information).<sup>37</sup> NSWCCCL would go further however and recommends that the government prioritise consumer protections set out in the Australian Consumer Laws with greater obligations on participating businesses. There should also be provision for situations where some collection and disclosure by service providers should not take place even with consent.<sup>38</sup>

## **5. Privacy Act 1988**

- 5.1 The Bill will require Accredited entities to continue to comply with existing privacy protections in the Privacy Act or, for State and Territory entities, their local privacy law. Where a State or Territory entity is not subject to a local privacy law, and wishes to become an accredited provider, the Bill provides for the entity to enter into a binding agreement that would require them to comply with the Australian Privacy Principles.
- 5.2 The Bill provides for Accredited entities to be subject to the notifiable data breach scheme in the Privacy Act or an equivalent State/Territory data breach scheme. Where an entity is not covered by a notifiable data breach scheme, the Bill's provisions extend the Privacy Act's scheme to that entity.
- 5.3 The term Personal Information adopts the current meaning in the Privacy Act and extends to cover any attributes of an individual to the extent the attribute is not otherwise covered by the Privacy Act definition. While most attributes will be personal information, the Bill defines an 'attribute' of an individual to mean information that is associated with the individual, including information that is derived from another attribute. This is broader than information about an individual as used in the Privacy Act, which refers to information 'about' an individual.<sup>39</sup>
- 5.4 Likely changes to the Privacy Act, as a consequence of the adoption of recommendations in the Privacy Act Review Report (PARR)<sup>40</sup>, will result in consequential legislative amendments to ensure the Bill remains consistent with additional requirements in the Privacy Act.<sup>41</sup> Recommendations in the PARR that are relevant to the Bill's operation include personal redress through a statutory tort for invasion of privacy and a direct right of action, a fair and reasonable use test, and stricter controls on overseas data flows.
- 5.5 NSWCCCL does not support the passage of the Bill without the prior enactment of a new privacy regime replacing the current Privacy Act.
- 5.6. NSWCCCL recommends that requirements relating to the conduct of, and reporting on, privacy impact assessments, fraud assessment and security assessments form part of the primary legislation.

---

<sup>37</sup> Law Council of Australia (11 Oct 2023) Digital Identity Bill 2023- Exposure Draft Consultation [https://www.digitalidentity.gov.au/sites/default/files/2023-11/law\\_council\\_of\\_australia.pdf](https://www.digitalidentity.gov.au/sites/default/files/2023-11/law_council_of_australia.pdf)

<sup>38</sup> Though the regulator must consider the potential harm that could result from disclosure and the entity's privacy impact assessment.

<sup>39</sup> Explanatory Memorandum

<sup>40</sup> Attorney-General's Department-Privacy Act Review- Report 2023 <https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>

<sup>41</sup> Explanatory Memorandum the Bill

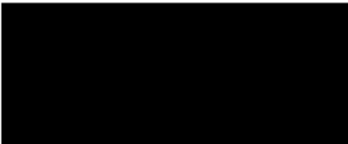


## 6. Human rights framework

- 6.1 AGDIS should be supported by an enforceable human rights framework such as a Bill of Rights. Australia is the only liberal democracy that lacks such a framework.<sup>42</sup> Australia, in its implementation of a Digital ID, must be distinguished from other OECD countries operating these systems for that reason. In Europe, many countries have established digital identity systems, however these systems are built on robust rights-based frameworks that we do not currently enjoy in Australia.<sup>43</sup>
- 6.2 Individuals should be able to obtain a remedy in the event of harm caused by a Digital ID provider which has failed to adhere to the legislation. This would provide another strong incentive for compliance, in addition to civil penalties. This could be achieved by providing consumers using Digital ID a statutory right to compensation in appropriate circumstances (recommended in the PARR). The government should also prioritise the establishment of appropriate and accessible dispute resolution schemes and introduce an unfair trading prohibition in the ACL.
- 6.3 The government commitment to redress, following ID fraud and cyber security incidents, is that it may be included in future versions of the Digital ID Rules, potentially requiring service providers to give notification, information, support, and assistance to those affected by an incident. NSWCCCL objects to such integral provisions being delayed or resigned to the rules.
- 6.4 The Bill does not include express provision to prevent discriminatory uses of a digital ID.<sup>44</sup> The government considers that existing laws provide pathways for individuals to access redress for discrimination. It is acknowledged that due to the reliance on digital technology the Bill may indirectly discriminate against persons for the following reasons:
- 6.4.1 Elderly people may be less likely to have the skills to use or access that technology, and the Bill may indirectly discriminate on the basis of age;
- 6.4.2 Limited telecommunications infrastructure in rural and remote areas of Australia means the Bill may indirectly discriminate on the basis of a person's place of residence or socio-economic factors;
- 6.4.3 Persons of cultural and linguistically diverse backgrounds may be indirectly discriminated against on the basis of ethnicity;
- 6.4.4 Indigenous Australians may also be indirectly disadvantaged because of a range of complex factors. This is also inconsistent with the aims of Article 2 of the UN Declaration on the Rights of Indigenous Peoples that Indigenous peoples are free and equal to all other peoples and individuals and have the right to be free from any kind of discrimination.

This submission was prepared by Michelle Falstein on behalf of the New South Wales Council for Civil Liberties. We hope it is of assistance to the Senate Economics and Legislation Committee.

Yours sincerely,



**Sarah Baker**  
**Secretary**  
**NSW Council for Civil Liberties**

---

<sup>42</sup> <https://humanrights.gov.au/human-rights-act-for-australia>

<sup>43</sup> Digital Rights Watch op.cit.

<sup>44</sup> Statement of Compatibility with Human Rights -Explanatory Memorandum the Bill

**Contacts in relation to this submission:**

**Michelle Falstein**

**Mobile:** [REDACTED]

**Email:** [REDACTED]



- 1.3 There will initially be three types of Digital ID services that can be accredited: identity service providers (currently myGovID); attribute service providers (providing details like educational or business qualifications); identity exchange providers (Services Australia using myGov). Providers of Digital ID services operating within the AGDIS must be accredited and will be subject to additional regulatory requirements, some of which will also apply to participating relying parties. A relying party uses the AGDIS by accepting proof of identity and needs to be approved to use the service but does not need to be accredited.
- 1.4 Accreditation provides a baseline set of obligations and regulatory oversight that apply to all accredited service providers. Accredited service providers will be required to comply with certain privacy, security, consumer protection, record-keeping, data destruction, and other requirements, e.g. governing cyber and fraud incident reporting, liability and fees. Many of these obligations will be set out in the rules.
- 1.5 Digital ID laws will be overseen by a Digital ID regulator – initially the Australian Competition and Consumer Commission (ACCC). However, multiple agencies and regulators will have roles relating to Digital ID, including the Office of the Australian Information Commissioner (OAIC), in regard to privacy breaches, and Services Australia as the AGDIS System Administrator.
- 1.6 Subject to limited exceptions, it must be voluntary for individuals to use Digital IDs within the AGDIS (particularly when accessing government services).<sup>7</sup>
- 1.7 The Digital ID Rules will provide technical detail about identity verification levels, privacy, security, accessibility and usability and additional privacy safeguards that purport to go beyond those in the Privacy Act 1988.
- 1.8 Amendments made to the Bill after the last round of consultation paper include:
  - 1.8.1 Strengthening the position that Digital IDs are voluntary for individuals who need to access government services. There are exceptions to this requirement which NSWCCCL find unacceptable;
  - 1.8.2 Strengthening safeguards over law enforcement access to personal information held by accredited service providers, so that these agencies may only request access to information with consent, a warrant, or where court proceedings have begun. In the exposure draft entities could also disclose information to law enforcement if a law enforcement body reasonably suspected an offence. NSWCCCL believes that the proposed safeguards are not sufficient. There should be no law enforcement access to information in the digital ID system with or without a warrant. Trust in the Digital ID system should at least be on the same level as the Federal COVIDSafe app, which prohibited access to a law enforcement body;
  - 1.8.3 Significantly increasing penalties for breaches of privacy, as well as other safeguards in the legislation. Penalties are an incentive to ensuring obligations are met by the participants. The availability to service providers of a liability shield for strict compliance with the Digital ID regime, may protect service providers from privacy penalties. NSWCCCL considers that a fee waiver should apply to individuals and that obligation should be set out in the primary legislation;
  - 1.8.4 Ensuring that certain types of information classified as prohibited attributes (such as racial or ethnic origin, religious beliefs or sexual orientation) cannot be collected for use in accredited digital ID services. If this information is received in an unsolicited way, it must be

---

<sup>7</sup> S74 Bill- Clause 74(1) provides that a participating relying party (a relying party approved to participate in the AGDIS) must not require an individual to create or use a digital ID as a condition of receiving a service from the relying party or accessing a service through the relying party.

destroyed as soon as practicable.<sup>8</sup> In the exposure draft, this information was allowed to be collected if there was a reasonable excuse.

## 2. Data Governance

- 2.1 Centralised and federated Digital ID systems generally place control of data in the hands of service providers. These systems also create the risk that a piece of authentication information can be leaked, leading to unauthorised logins to multiple services. Ongoing mandatory mass collection and storage of personal data by centralised oversight authorities has become normalised over many years and particularly during the COVID-19 pandemic. As a result, individuals have become disconnected from their personal information and disempowered from owning it.<sup>9</sup> NSWCCCL supports the return to ownership and governance by individuals of their own personal information and identity.
- 2.2 Alternatives to centralised Digital ID systems exist and have been built through Blockchain and Self-Sovereign Identity using blockchain technology.<sup>10</sup> In fact, the final report of the Senate Select Committee on Australia as a Technology and Financial Centre recommends that Australia embrace technologies such as blockchain and decentralised computing.<sup>11</sup>
- 2.3 The Bill envisages alternative methods of digital ID e.g. in s49(2)(a) of the Bill which includes biometric information "that may be contained in a verifiable credential that is in the control of the individual". However, more detailed work needs to be done in the Bill to ensure that there are no barriers to emerging credentials and IDs controlled by the individual.
- 2.4 Clearly set out in the objects of the Bill<sup>12</sup> is the objective of promoting trust in digital ID services. The focus of the AGDIS must clearly be on ensuring that less data is shared and, when shared, stored in the most secure manner. Recent experience with Government entities, particularly in relation to the MyGovID, has fomented some distrust in the community. In 2020, security researchers warned the public against using MyGovID due to security flaws in its design.<sup>13</sup> The Australian government has also failed to secure information, with data breaches and cybersecurity hacks involving the Australian Tax Office, National Disability Insurance Scheme and Defence Forces.<sup>14</sup>
- 2.5 The priority in terms of data governance should be to determine how the system could be more safely implemented, for example, although requirements to delete or destroy any personal information have been tightened<sup>15</sup>, this does not affect the information that the entity may hold in relation to the individual's deactivated Digital ID.<sup>16</sup>

---

<sup>8</sup> S44 Bill

<sup>9</sup> Nabben op.cit.

<sup>10</sup> World Economic Forum (Aug 12 2021) *Self-sovereign identity: the future of personal data ownership?*

<https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/>

<sup>11</sup> [https://www.aph.gov.au/Parliamentary\\_Business/Committees/Senate/Financial\\_Technology\\_and\\_Regulatory\\_Technology/AusTechFinCentre/Final\\_report](https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/AusTechFinCentre/Final_report)

<sup>12</sup> S 3 Bill

<sup>13</sup> Saarinen, J (Sept 21 2020) *Researchers say not to use myGovID until login flaw is fixed* IT News

<https://www.itnews.com.au/news/researchers-say-not-to-use-mygovid-until-login-flaw-is-fixed-553601;>

[https://theconversation.com/the-500-million-ato-fraud-highlights-flaws-in-the-mygov-id-system-heres-how-to-keep-your-data-safe-210459;](https://theconversation.com/the-500-million-ato-fraud-highlights-flaws-in-the-mygov-id-system-heres-how-to-keep-your-data-safe-210459) <https://www.news.com.au/technology/online/hacking/australian-defence-force-confirm-data-breach-hack/news-story/c4c0d955be1f8018e0a19ce9233ad2b4>

<sup>14</sup> Mealy- ABC <https://www.abc.net.au/news/2022-11-28/cyber-black-market-shows-medibank-optus-hack-just-the-surface/101700974>

<sup>15</sup> S56 Bill-prohibits an accredited identity exchange provider from retaining specified attributes of individuals. The section ensures that an exchange cannot be a centralised repository of personal information. It prohibits an exchange from retaining core attributes of an individual, namely name, address, date of birth, phone number and email address, which are not retained after the end of the authenticated session.

<sup>16</sup> S 29 Bill



- 2.6 The retention of sensitive information (including digitalised biometric information) for longer than required or unnecessarily creates opportunities for the hacking of personal information. The proposed AGDIS violates the cautionary advice about not linking all of one's personal information, such as tax history and medical history, which can lead to mass analytics, behaviour profiling and targeted advertising. "It potentially creates a "honeypot" of personal data stored in a centralised database that would offer a tempting target for cyber criminals or hostile nations."<sup>17</sup>

Additionally, the proposed scheme is only as secure as one's phone or other personal device. Having a weak password, losing or having a device hacked could lead to data being compromised.<sup>18</sup>

### 3. Biometrics

- 3.1 According to the OAIC's 2023 Community Attitudes Survey, only 49% of Australians are comfortable with the use of their biometric information to verify their identity online. Only a third are comfortable with that information being used when they want to access a service provided by a business.<sup>19</sup>
- 3.2 The use of biometric technology, at any point of authentication, introduces substantial privacy and security risks. NSWCCCL believes that avoiding biometrics altogether, in the current legislative environment, is the best approach. An individual's biometric information cannot be simply replaced or managed if compromised and is particularly difficult to remedy in the case of a data breach. The NSWCCCL therefore urges the government not to use biometrics as a method of authentication but instead offer non-biometric alternatives for verification within the Digital ID system.<sup>20</sup>
- 3.3 Errors in facial recognition technology may result in an individual being denied an essential government service. "Since FRT relies on computer vision, where recognition is always a one-sided visual assessment, there is a danger of misreading or misrecognising a person's identity. This misrecognition and mislabelling by technology can often counter a person's self-identity, especially when it relates to a person's gender identity or race. FRT has been criticised, particularly in its use by law enforcement agencies, for being violative of civil liberties, and for the potential for abuse, propensity for inaccuracies, and improper use."<sup>21</sup>
- 3.4 Should biometric technology be used for verification, even in a limited way, robust testing should be a prerequisite to its adoption in order to interrogate bias, accuracy, and the impact on vulnerable categories of people. What are the options for those who are excluded by biometric technologies because they have failed to be verified by them?
- 3.5 The Bill does contain some special protections against data breach pertaining to biometric information. This includes requiring accredited identity service providers to immediately destroy biometric information it has collected from an individual for the purpose of verifying that individual's identity after the verification is complete under section 48.<sup>22</sup>
- 3.6 However, the Bill also provides for the Minister to make certain rules to allow the disclosure of biometric information when expressly consented to by the individual. Consent is discussed in further detail later in this paper. NSWCCCL agrees with Digital Rights Watch that, at the very least, such a regime would "be appropriate where additional and more onerous protections apply,

---

<sup>17</sup> Nabben op.cit

<sup>18</sup> Mealy op.cit.

<sup>19</sup> The Office of the Australian Information Commissioner, Community Attitudes to Privacy Survey, 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>

<sup>20</sup> Currently a PIN can be used.

<sup>21</sup> UNSW Allens Hub for Technology, Law and Innovation, Digital Identity and Identity verification bills (2 Oct 2023) [https://www.digitalidentity.gov.au/sites/default/files/2023-11/unsw\\_allens\\_hub\\_for\\_technology\\_law\\_and\\_innovation.pdf](https://www.digitalidentity.gov.au/sites/default/files/2023-11/unsw_allens_hub_for_technology_law_and_innovation.pdf)

<sup>22</sup> s 51(1) Bill

including a fair and reasonable requirement and an obligation placed upon accredited entities that the sharing of a biometric credential be in the best interests of the individual.”<sup>23</sup>

3.7 By linking personal identification data across federal and state jurisdictions, as well as the private sector, the federal government has complete oversight of the lives of Australians. There should be no justification for allowing Digital ID data for surveillance. Accordingly, NSWCCCL recommends that law enforcement agencies be explicitly prohibited from accessing Digital ID data held by any accredited entities.

3.8 Notably the Bill permits disclosure of:

3.8.1 a unique identifier for, amongst other things, detecting, reporting, investigating or prosecuting an offence against a law of the Commonwealth, a State or a Territory (S47(4)(e)), and,

3.8.2 biometric information and personal information, if authorised under a warrant (s49(3)(a) and S54(1)(b)(iii) respectively).

3.9 Accredited entities are prohibited from using or disclosing information about an individual’s online activities, such as the individual’s access and use of the Digital ID services provided by the entity<sup>24</sup>, regardless of consent.<sup>25</sup> However, there are exemptions to this prohibition, including:

3.9.1 for “purposes relating to the provision of the entity’s accredited services (including improving the performance or usability of the entity’s information technology systems through which those services are provided)”.<sup>26</sup> Such an exemption, tempts function creep by accredited entities to personalise and commercialise services.

3.9.2 the prohibition on data profiling to track online behaviour, if the use or disclosure is required or authorised under a law of the Commonwealth, a State or Territory.<sup>27</sup> It is not clear whether this provision would include access by authorised warrant.

NSWCCCL objects to these exemptions. Individuals should have no concerns when using the AGDIS that it may be accessed by law enforcement or for other unauthorised purposes by private enterprise.

#### **4. Voluntary Participation and Equity**

4.1 Equity of access and ownership of one’s digital information must be considered in the context of privilege. The effect on vulnerable members of the community, such as the homeless, refugees, the indigenous population and the disabled community, of not being able to access technology, is profound. A digital identity must not be a precondition to access basic services and rights. Analogue and other accessible digital pathways should be maintained.

4.2 As the AGDIS accesses existing documentation, this will exclude people already without official identification. Individuals who are less digitally literate, without access to digital technology, or with personal objections to Digital ID will also require alternative methods for authentication.

4.3 The Bill provides individuals with the right to voluntarily create and use a digital identity, including the right to deregister and not use a digital identity, at any time.<sup>28</sup> Relying parties need to ensure that use of the AGDIS is not a condition to their supply of a service and that an alternative way to verify identity is available. The interoperability obligation of accredited service providers and

---

<sup>23</sup> Digital Rights Watch (11 Oct 2023) *Submission to the Digital ID Taskforce regarding the Digital ID Bill 2023 exposure draft* [https://www.digitalidentity.gov.au/sites/default/files/2023-12/digital\\_rights\\_watch\\_redacted.pdf](https://www.digitalidentity.gov.au/sites/default/files/2023-12/digital_rights_watch_redacted.pdf)

<sup>24</sup> S53 Bill

<sup>25</sup> S53(2) Bill

<sup>26</sup> S53(3)(a) Bill

<sup>27</sup> S53(3)(c) Bill

<sup>28</sup> S74(1) Bill



relying parties means that there must not be general refusal to provide services to other accredited service providers or relying parties in the AGDIS. NSWCCCL strongly supports simple, accessible, alternatives to accessing services however there is insufficient detail on alternative services in the Bill.

- 4.4 Exceptions to S74 tend to undermine the provision of non-digital alternatives. Exceptions include, where a relying party is a small business, an online-only service, or where the relying party (that is not a Commonwealth service) is providing services, or access to services, in exceptional circumstances. For example, this may apply during an emergency situation such as flood or fire.<sup>29</sup> "Creeping expansion of businesses that superficially satisfy the prescriptive requirements of the law may lead to a slow expansion of the exemption clause. This can, over time, create an ecosystem where despite claims of voluntariness, digital identity becomes both the de facto and de jure DI system, creating anxieties of recognition and sometimes exclusion of people."<sup>30</sup> NSWCCCL sees no justification for, and objects to the exemptions, particularly in an emergency. Further, NSWCCCL has particular concerns about enforcing voluntary participation by accredited and relying service providers.
- 4.5 The Explanatory Memorandum to the Bill explains that "the Bill will not initially provide specific financial or non-financial redress obligations on accredited entities participating in the AGDIS, or on the Regulator. This will be set out in the Digital ID rules."<sup>31</sup> NSWCCCL strongly recommends the detailed provision of redress measures for individuals, within the primary legislation. Individuals should have clear, simple and transparent guidance to remedies for harms suffered, and access to relevant information concerning complaints and conciliation processes. At a minimum, S88 should mandate that a redress framework be developed within a certain, limited timeframe.<sup>32</sup>
- 4.6 Another barrier to equitable access to the AGDIS will be user access fees. Part 6 of the Bill enables rules to be made by the Regulator in relation to fees. NSWCCCL recommends that the Bill prohibits relying parties from passing on fees to individuals and that individuals not be charged to create or deactivate a Digital ID.

### *Consent*

- 4.7 The Bill provides that the individual in control of their own verifiable credentials must *expressly* consent to any collection, use or disclosure of biometric information contained in such credentials. Various sections in the Bill require an individual's express consent for collection and disclosure, e.g. for biometric information<sup>33</sup>, personal information<sup>34</sup> and for certain attributes<sup>35</sup>. However, obtaining express consent should be far more robust with further obligations to ensure that the consent obtained by entities is both fully informed and voluntary.
- 4.8 Even so, "express consent" will be meaningless in many digital interactions. Opting out of digital interactions is not a realistic option for most individuals. They find that they have to agree to terms of access or risk the suffering of economic disadvantage, discrimination or social exclusion. "[C]onsumers may be informed and understand the inherent privacy risks of providing their personal information but may feel resigned to consenting to the use of their information in order to access online services, as they do not consider there is any alternative. Further, while 'consent' is only a meaningful and effective privacy self-management tool where the individual actually has a choice and can exercise control over their personal information, studies also show that consumers rarely understand and negotiate terms of use in an online environment".<sup>36</sup>

<sup>29</sup> Explanatory Memorandum; S74(5) Bill

<sup>30</sup> UNSW Allens Hub op.cit.

<sup>31</sup> S.88 Bill

<sup>32</sup> Digital Rights Watch op.cit

<sup>33</sup> Ss48 and 49 Bill

<sup>34</sup> S54 Bill

<sup>35</sup> S45 Bill

<sup>36</sup> OAIC 2019 (CCL sub)



- 4.9 The Law Council has suggested, at a minimum, a framework requiring that an accredited entity provide the individual with a clear written or oral statement, explaining the potential consequences of providing consent and any other practical effects or risks associated with the consent. This approach could be adopted in respect of all forms of express consent required under the Bill, including in relation to Ss18 (restricted attributes) and 19 (biometric information).<sup>37</sup> NSWCCCL would go further however and recommends that the government prioritise consumer protections set out in the Australian Consumer Laws with greater obligations on participating businesses. There should also be provision for situations where some collection and disclosure by service providers should not take place even with consent.<sup>38</sup>

## **5. Privacy Act 1988**

- 5.1 The Bill will require Accredited entities to continue to comply with existing privacy protections in the Privacy Act or, for State and Territory entities, their local privacy law. Where a State or Territory entity is not subject to a local privacy law, and wishes to become an accredited provider, the Bill provides for the entity to enter into a binding agreement that would require them to comply with the Australian Privacy Principles.
- 5.2 The Bill provides for Accredited entities to be subject to the notifiable data breach scheme in the Privacy Act or an equivalent State/Territory data breach scheme. Where an entity is not covered by a notifiable data breach scheme, the Bill's provisions extend the Privacy Act's scheme to that entity.
- 5.3 The term Personal Information adopts the current meaning in the Privacy Act and extends to cover any attributes of an individual to the extent the attribute is not otherwise covered by the Privacy Act definition. While most attributes will be personal information, the Bill defines an 'attribute' of an individual to mean information that is associated with the individual, including information that is derived from another attribute. This is broader than information about an individual as used in the Privacy Act, which refers to information 'about' an individual.<sup>39</sup>
- 5.4 Likely changes to the Privacy Act, as a consequence of the adoption of recommendations in the Privacy Act Review Report (PARR)<sup>40</sup>, will result in consequential legislative amendments to ensure the Bill remains consistent with additional requirements in the Privacy Act.<sup>41</sup> Recommendations in the PARR that are relevant to the Bill's operation include personal redress through a statutory tort for invasion of privacy and a direct right of action, a fair and reasonable use test, and stricter controls on overseas data flows.
- 5.5 NSWCCCL does not support the passage of the Bill without the prior enactment of a new privacy regime replacing the current Privacy Act.
- 5.6. NSWCCCL recommends that requirements relating to the conduct of, and reporting on, privacy impact assessments, fraud assessment and security assessments form part of the primary legislation.

---

<sup>37</sup> Law Council of Australia (11 Oct 2023) Digital Identity Bill 2023- Exposure Draft Consultation [https://www.digitalidentity.gov.au/sites/default/files/2023-11/law\\_council\\_of\\_australia.pdf](https://www.digitalidentity.gov.au/sites/default/files/2023-11/law_council_of_australia.pdf)

<sup>38</sup> Though the regulator must consider the potential harm that could result from disclosure and the entity's privacy impact assessment.

<sup>39</sup> Explanatory Memorandum

<sup>40</sup> Attorney-General's Department-Privacy Act Review- Report 2023 <https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>

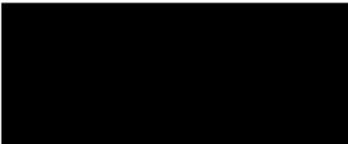
<sup>41</sup> Explanatory Memorandum the Bill

## 6. Human rights framework

- 6.1 AGDIS should be supported by an enforceable human rights framework such as a Bill of Rights. Australia is the only liberal democracy that lacks such a framework.<sup>42</sup> Australia, in its implementation of a Digital ID, must be distinguished from other OECD countries operating these systems for that reason. In Europe, many countries have established digital identity systems, however these systems are built on robust rights-based frameworks that we do not currently enjoy in Australia.<sup>43</sup>
- 6.2 Individuals should be able to obtain a remedy in the event of harm caused by a Digital ID provider which has failed to adhere to the legislation. This would provide another strong incentive for compliance, in addition to civil penalties. This could be achieved by providing consumers using Digital ID a statutory right to compensation in appropriate circumstances (recommended in the PARR). The government should also prioritise the establishment of appropriate and accessible dispute resolution schemes and introduce an unfair trading prohibition in the ACL.
- 6.3 The government commitment to redress, following ID fraud and cyber security incidents, is that it may be included in future versions of the Digital ID Rules, potentially requiring service providers to give notification, information, support, and assistance to those affected by an incident. NSWCCCL objects to such integral provisions being delayed or resigned to the rules.
- 6.4 The Bill does not include express provision to prevent discriminatory uses of a digital ID.<sup>44</sup> The government considers that existing laws provide pathways for individuals to access redress for discrimination. It is acknowledged that due to the reliance on digital technology the Bill may indirectly discriminate against persons for the following reasons:
- 6.4.1 Elderly people may be less likely to have the skills to use or access that technology, and the Bill may indirectly discriminate on the basis of age;
- 6.4.2 Limited telecommunications infrastructure in rural and remote areas of Australia means the Bill may indirectly discriminate on the basis of a person's place of residence or socio-economic factors;
- 6.4.3 Persons of cultural and linguistically diverse backgrounds may be indirectly discriminated against on the basis of ethnicity;
- 6.4.4 Indigenous Australians may also be indirectly disadvantaged because of a range of complex factors. This is also inconsistent with the aims of Article 2 of the UN Declaration on the Rights of Indigenous Peoples that Indigenous peoples are free and equal to all other peoples and individuals and have the right to be free from any kind of discrimination.

This submission was prepared by Michelle Falstein on behalf of the New South Wales Council for Civil Liberties. We hope it is of assistance to the Senate Economics and Legislation Committee.

Yours sincerely,



**Sarah Baker**  
**Secretary**  
**NSW Council for Civil Liberties**

---

<sup>42</sup> <https://humanrights.gov.au/human-rights-act-for-australia>

<sup>43</sup> Digital Rights Watch op.cit.

<sup>44</sup> Statement of Compatibility with Human Rights -Explanatory Memorandum the Bill

**Contacts in relation to this submission:**

**Michelle Falstein**

**Mobile:** [REDACTED]

**Email:** [REDACTED]