Law Council
OF AUSTRALIA

Office of the President

11 October 2023

[redacted]

Digital Identity Bill 2023—Exposure Draft Consultation

1. The Law Council of Australia is pleased to make a submission to the **Department** of Finance in response to its consultation on the exposure draft of the Digital Identity **Bill** 2023 and accompanying **Rules**. The Law Council is grateful for the assistance of the Law Society of New South Wales and the Law Society of South Australia in preparing this submission, in addition to that of its Business Law Section's Privacy Law Committee.

2. The creation of a legislated, economy-wide, digital identification regime is a highly significant and sensitive proposal that requires careful consideration by government. The Law Council supports, in principle, the development of a legislated voluntary accreditation scheme, which would strengthen the existing Trusted Digital Identity Framework (**TDIF**), and gradually expand the Australian Government Digital ID System (**AGDIS**) to include private sector organisations that choose to participate.

3. The Law Council welcomes the Department's consultation on the draft Bill and Rules. Nonetheless, the Law Council is concerned about the very limited timeframe provided for consultation before the anticipated introduction of the Bill into the Parliament, which does not give stakeholders sufficient time to provide considered responses to the technical matters raised in the draft Bill and the accompanying materials.

4. Regrettably, in the brief time available to provide views on the draft Bill and Rules, the Law Council and its membership have not had the opportunity to meaningfully consider the materials provided by the Department, including the specific consultation questions posed. The Law Council's views should, therefore, be considered preliminary.

Context

5. The Law Council has long supported holistic approaches to privacy and data law reform that promote, to the greatest possible extent, consistency and predictability in the relevant legislative frameworks. Consequently, the Bill and Rules should be considered in the broader context of the review of the *Privacy Act 1988* (Cth) (the **Privacy Act Review**), and in conjunction with other related law reform initiatives.

[redacted]

Privacy Act Review

6. Fundamental aspects of the Australian privacy regime have been subject to ongoing consideration by the Commonwealth Government, following the release of the Privacy Act Review **Report** by the Attorney-General's Department in February 2023.[1] The Report contained 116 proposals for reform—a culmination of several years of thorough consultation and review. In late September 2023, the Government formally responded to the Report, agreeing, or agreeing in principle, with the majority of the proposals.[2]

7. There is a significant need for consistency and certainty of key concepts across Australia's digital identity, privacy, and identity verification frameworks. Consequently, as an overarching principle, the Bill should be compatible with the proposals agreed upon by the Government in its response to the Privacy Act Review, particularly in relation to terminology. For instance, the Bill should mirror the Report's proposed definitions for 'collection',[3] 'disclosure'[4] and 'consent'.[5]

8. The expansive definition of 'personal information', proposed under clause 9 of the Bill, would include 'attributes of individuals'. However, extending the meaning of 'personal information' under the Bill may further confuse what is already an uncertain concept, and undermine consistency across the relevant legislative schemes. The Law Council previously raised this concern in response to the exposure draft of the current draft Bill's predecessor, the Trusted Digital Identity Bill 2021.[6] This Bill was not introduced before Parliament was prorogued in April 2022.

9. Notably, the Government's in-principle agreement to the majority of the proposals in Chapter 4 of the Report signifies that further detailed consideration and impact analysis will be required before concrete amendments are made to, for instance, the definitions of 'personal information' and 'sensitive information' in the Privacy Act.

10. In any event, the Bill, if passed, will necessarily require revisions to reflect any new, or updated, terms that may arise, following anticipated reforms to the Privacy Act, as the primary and authoritative piece of privacy-related legislation in Australia.

Related law reform initiatives

11. Apart from the ongoing review of the Privacy Act, the Senate Legal and Constitutional Affairs Legislation **Committee** is currently inquiring into the provisions of the Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023 (the **IVS Bills**).[7] These Bills were introduced into the House of Representatives on 13 September 2023 and were referred to the Committee the following day. Troublingly, the reporting date imposed on the Committee allowed for a truncated consultation period of 12 business days.

[1] Attorney-General's Department, Privacy Act Review Report 2022 (February 2023) <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.
[2] Government Response to the Privacy Act Review Report (September 2023) <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>.
[3] Ibid [Proposal 4.3].
[4] Ibid [Proposal 23.6].
[5] Ibid [Proposal 11.1].
[6] Law Council of Australia, Phase 3 of Australia's Digital Identity legislation (Submission to the Digital Transformation Agency, 28 October 2021) <https://lawcouncil.au/resources/submissions/phase-3-of-australias-digital-identity-legislation>.
[7] Australian Government, 2023 Digital ID Bill and Rules submissions (Web Page, September 2023) <https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions>.

12. The Committee is also inquiring into the provisions of the Statutory Declarations Amendment Bill 2023,[8] introduced into the Parliament on 7 September 2023. The Bill proposes to enable Commonwealth statutory declarations to be executed through a digital verification process, through the use of an approved online platform that verifies the digital identity of the declarant through an approved identity service.[9]

13. Notably, the IVS Bills seek to establish new primary legislation to provide a legal framework for the operation of the Commonwealth's identity verification services, allowing government agencies and industry to match biometric information (such as a photograph or biographic information) with an existing government record.

14. While the Law Council appreciates that the IVS Bills and the Digital ID Bill differ in terms of their objects and scope, both proposals appear to raise substantially similar issues concerning digital identity verification and usage. In particular, the Bills relate to accredited identity service providers, such as *myGovID*, which employs identity verification services, with similar risks associated with the implementation of such services.

15. While these reform processes are clearly linked, this Bill and the IVS Bills are misaligned in terms of privacy protection and oversight. From a public policy perspective, the Bill appears to adopt a superior approach compared to the IVS Bills, by, for example:

    - introducing 'additional privacy safeguards' in Chapter 3, Part 2, Division 2;
    - providing the Information Commissioner with an advisory role in relation to the operation of the Bill, at the request of the Minister, pursuant to clause 40;
    - the establishment of independent regulation of Digital ID in Chapter 5, Part 2;
    - providing for clear record keeping, destruction and de-identification requirements in Chapter 8, Part 3; and
    - requiring the Minister to consult with the public and the Information Commissioner before making or amending any rules, per clause 159.

16. While the Government clearly intends for these two legislative proposals to work in tandem, it is currently unclear how, and to what extent, they might interact. The Law Council would appreciate guidance from the Government on this matter. Proceeding with these misaligned proposals, if passed, will increase the cost of compliance for government and business, as there will be multiple inconsistent schemes operating in an overlapping area of activity.

17. In considering the similarities between the two proposals, both thematically and in terms of concurrent timeframes for stakeholder engagement, the Law Council calls for improved coordination and integration of privacy-related, federal law reform initiatives across government. This approach would promote consistency in the law and enable correlations between the various proposals to be fully realised.

18. The Law Council acknowledges that technology typically moves much faster than the law, and that, as a result, the fragmentation of reforms is, at times, unavoidable. Nonetheless, at a minimum, the Law Council seeks a roadmap for the harmonisation of

[8] Senate Legal and Constitutional Affairs Committee, Statutory Declarations Amendment Bill 2023 [Provisions], Web Page (September 2023) <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/StatutoryDeclarations23>.
[9] Statutory Declarations Amendment Bill 2023 (Cth), sch 1, pt 1, item 3 (cl 9A).

Australia's privacy and data laws, to ensure the development of a national privacy framework that is consistent, clear and accessible.[10]

Proposed privacy safeguards and compliance

Additional privacy safeguards

19. Chapter 3, Part 2, Division 2 of the Bill intends to expand upon the safeguards and protections provided under the Privacy Act, which must be followed by accredited Digital ID services under that proposed arrangement. While the inclusion of additional safeguards is welcome, given the clear deficiencies of the Privacy Act, it is difficult to assess the appropriateness and likely effects of such measures, given the uncertain legal climate in anticipation of wholesale reforms to Australia's privacy legislation.

20. Given these current complexities, reform of the Privacy Act should be advanced as a matter of priority. It will be important to maintain the momentum from the Government's response to the Privacy Act Review to avoid uncertainty and unintended consequences created by a fragmented approach to reform, to which the draft Bill and Rules are contributing.

21. Nonetheless, should the Government proceed with expeditiously introducing this Bill into Parliament, regard should be had to the below remarks regarding the additional privacy safeguards proposed in the Bill.

Prohibited attributes

22. Clause 41 of the draft Bill provides that an accredited entity must not intentionally collect, use or disclose certain attributes of an individual. The Law Council notes that this clause does not prevent *all* collection, use or disclosure of prohibited attributes—it simply prohibits the *intentional* collection, use or disclosure.

23. In the document *Your Guide to the Digital ID Legislation and Rules* (the **Guide**), the Department acknowledges that an accredited entity may *unintentionally* collect prohibited attributes:

> *This is sensitive information about a person, such as a person's racial or ethnic origins, or religious beliefs. Accredited entities may unintentionally collect that information—for example if a person's photo could disclose their religious belief because of their clothing*.[11]

24. The Law Council queries whether 'intentional', an objectively high threshold, is the appropriate test for an entity's state of mind in this context. The use of 'intentional'—which, in its ordinary meaning, refers to a deliberate act—could have broader, unintended consequences. As drafted, proposed clause 41 suggests that:

- among other things, the *reckless* collection, use or disclosure of prohibited attributes is permitted, noting that proposed paragraph 149(3)(b) of the Bill draws a distinction between 'intention', 'knowledge' and 'recklessness'; and
- an entity may somehow use, or disclose, prohibited attributes, as long as such use or disclosure is not intentional.

[10] Law Council of Australia, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Submission to the Senate Legal and Constitutional Affairs Committee, 8 November 2022) <https://lawcouncil.au/resources/submissions/privacy-legislation-amendment-enforcement-and-other-measures-bill-2022> 8.
[11] Department of Finance, *Your Guide to the Digital ID Legislation and Digital ID Rules* (18 September 2023) 12.

25. The scenario contemplated by the Guide (a person's clothing in a photo disclosing their religious belief) is the unavoidable, or incidental, collection of prohibited attributes, rather than the unintentional collection. This is because the prohibited attribute is directly deducible—or immediately observable and inseparable—from other attributes permitted to be collected.

26. To reflect the legislative intent more accurately (as contemplated by the Guide) and ensure greater protection for individuals, further consideration should be given to the appropriateness of the word 'intentional' in the context of proposed clause 41. Alternative wording may be preferable, for example, a clause that:

- expressly prohibits the collection, use or disclosure of prohibited attributes;
- prohibits an accredited entity from intentionally soliciting prohibited attributes; and
- (to accommodate the circumstance contemplated by the Guide) specifically carves out the collection, use or disclosure of prohibited attributes that are 'reasonably unavoidable'. This is only because those prohibited attributes are directly incidental to, or immediately deducible or observable from (and inseparable from), other attributes permitted to be collected, used or disclosed.

27. The Bill should also clarify whether clause 41 only applies to the collection of prohibited attributes by the accredited entity in the context of the draft Bill. That is, whether the information collected by the accredited entity, in its ordinary course of business, is similarly prohibited in general.

28. For example, the Law Council queries whether an accredited entity could still collect sensitive information that comprises prohibited attributes, in respect of its own employees, noting that an employee record is generally considered to be outside the application of the Privacy Act. It is unclear whether this situation would give rise to a contravention of clause 41, noting it is still, technically, the collection of prohibited attributes by an accredited entity.

Consent

29. Clause 42 of the draft Bill provides that an accredited entity must obtain an individual's express consent to the disclosure of certain attributes (e.g., the individual's name, address, data of birth and phone number) to a relying party. However, obtaining express consent should be more robust than merely 'check[ing] a tick box', as suggested in the Guide.[12]

30. Given that the scope of attributes permitted to be disclosed is practically unlimited (save for certain prohibited attributes under clause 41), further obligations, or guardrails, are required to ensure that the consent obtained by entities is both fully informed and voluntary.

[12] Ibid 19.

31. There should be, at a minimum, a framework similar to that envisaged by the Office of the Australian Information Commissioner (**OAIC**) under Australian Privacy Principle (**APP**) 8.2,[13] which requires:

- the APP entity (or, in this case, the accredited entity) to provide the individual with a clear written or oral statement, explaining the potential consequences of providing consent;
- the statement to be made at the time consent is sought, and not to be relied on as assumed prior knowledge of the individual; and
- the statement to explain any other practical effects or risks associated with the consent, of which the accredited entity is aware, or would reasonably be expected to be aware.

32. Ideally, this best practice approach should be adopted in respect of all forms of express consent required under the Bill, including in relation to proposed clause 43 (restricted attributes) and 46 (biometric information).

Biometric information

33. Clause 46 of the draft Bill provides for two situations in which an accredited entity can collect, use or disclose biometric information, outside the realm of law enforcement, as follows:

- for the purpose of verifying the identity of the individual, and/or authenticating the individual to their digital ID, but only if the collection, use or disclosure of biometric information is authorised by the entity's accreditation conditions;[14] and
- if the biometric information is contained in a verifiable credential that is in control of the individual, and the collection, use or disclosure complies with any requirements prescribed by the Digital ID **Accreditation Rules**.[15]

34. The Guide envisages that, in relation to proposed paragraph 45(1)(b), the individual's express consent is obtained before the disclosure of biometric information in a verifiable credential:

> *The Bill will allow for the Minister to make rules, disallowable by Parliament, to allow disclosure of biometric information where the disclosure is to allow an individual in control of their own verifiable credential to expressly consent to share that credential. The Minister must consult with the Information Commissioner before making any rules about biometrics.*
>
> *The technology around verifiable credentials is new, rapidly advancing and requires the ability to make prompt changes to ensure the legislation keeps up with future advancements. An important safeguard for any future rule is that it cannot undermine the protection in the Bill that requires the individual to give their consent to use or disclose the biometric or verifiable credential.*[16]

[13] Office of the Australian Information Commissioner, Chapter 8: APP 8 Cross-border disclosure of personal information (Web Page, 22 July 2019) <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>.
[14] Exposure Draft, Digital ID Bill 2023, sub-cl 46(1).
[15] Ibid sub-cl 46(2).
[16] Department of Finance, *Your Guide to the Digital ID Legislation and Digital ID Rules* (18 September 2023) 20.

35. Although the draft Digital ID Rules and Accreditation Rules have not established detailed rules on the usage of verifiable credentials, neither the Bill nor the Accreditation Rules appear to suggest the position envisaged above by the Guide, where the individual's express consent must be sought for the disclosure of biometric information in a verifiable credential.

36. Paragraph 45(1)(b) provides that express consent of the individual in relation to the collection, use or disclosure of biometric information is only required in respect of:

- a warrant issued by a magistrate, judge or member of a tribunal;[17]
- disclosure to the individual to whom the biometric information relates;[18]
- retention, use or disclosure by an accredited identity service provider for verification or authentication;[19] and
- retention, use or disclosure by an accredited identity service for preventing or investigating fraud.[20]

37. Despite the drafting of proposed sub-clause 46(2), consent should not be presumed only because the individual has control of the verifiable credentials or has provided such verifiable credentials to the accredited entity. Ideally, the Bill's drafting should reflect the explanation in the Guide (quoted above): that is, 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.

Financial penalties

38. The Law Council supports, in principle, strengthening the enforcement mechanisms for the existing TDIF by introducing a civil penalties regime which would apply to accredited service providers.

39. The Bill would enhance enforcement of the accreditation scheme by empowering the Regulator to impose civil penalties for non-compliance with accreditation requirements under proposed Chapter 8, Part 2, Division 2. The Bill also contemplates civil penalties for breaches by accredited entities of the additional privacy safeguards set out in Chapter 3, Part 2, Division 2.

40. The implementation of financial penalties in these circumstances would bolster the accreditation system by providing appropriate deterrents against non-compliance, or undue interference with individuals' privacy by relevant entities.

[17] Exposure Draft, Digital ID Bill 2023, sub-cl 46(3)(a).
[18] Ibid sub-cl 46(5).
[19] Ibid sub-cl 46(6).
[20] Ibid sub-cl 46(8).

[redacted]

[redacted]