Law Council
OF AUSTRALIA

Phase 3 of Australia's Digital Identity legislation

Digital Transformation Agency

28 October 2021

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2021 Executive as at 1 January 2021 are:

[redacted]

The Chief Executive Officer of the Law Council is [redacted].

Acknowledgement

The Law Council is grateful to its Business Law Section's Privacy Law Committee for its contribution to this submission. The Law Council also acknowledges input received from the Queensland Law Society and Law Institute of Victoria.

Introduction

1. The Law Council welcomes the opportunity to provide input to Phase 3 of Australia's Digital Identity consultation, notably the exposure draft of the Trusted Digital Identity Bill 2021 (**the Draft Bill**).

2. The Draft Bill proposes to establish a Trusted Digital Identity Framework (**TDIF**) and an accompanying accreditation and onboarding regime for participants of the TDIF. The TDIF is intended to provide individuals with a simple and convenient method for verifying their identity in online transactions with government and businesses.

3. The Law Council accepts that many paper or card-based services will inevitably undergo digital modernisation in the coming years. However, the establishment of digital identities is a highly sensitive proposal and must be implemented with careful consideration. The Law Council acknowledges that a TDIF provides considerable efficiency gains through the use of a secure and centralised accreditation system, particularly where the collection of information is limited to that which is absolutely necessary and proportionate safeguards are implemented, including the timely deletion of unnecessary information.

4. However, the Law Council considers that participation in the TDIF should be voluntary and that non-digital systems for identity verification must also be maintained. The use of data under the TDIF must also be sufficiently transparent to enable users to provide informed consent, as well as withdraw enduring consent once it has been provided.

5. Finally, the TDIF will undoubtedly have a significant impact on the way citizens interact with the Australian Government and other accredited entities, and the Law Council expresses some concern with the compressed timeframe for consultation on the Draft Bill, particularly as initial considerations for a Digital Identity Framework began in 2015. The Law Council will likely take the opportunity to further engage with the measures prior to or once they progress to Parliament.

Interactions with other reform initiatives

6. Whilst the dominant focus of this submission is privacy, the Law Council wishes to again take the opportunity to call for improved integration and collaboration between other Federal (at least) and State law reform initiatives involving digital identity verification and usage. By way of example the Department of the Prime Minister and Cabinet has the Modernising Document Execution initiative exploring ways to reduce friction in the practices and procedures surrounding the execution and witnessing of legal documents such as statutory declarations and deeds.

7. The new Director Identification Number scheme also appears to be reliant on a person's MyGovID at standard or strong level. In neither of these other initiatives is there a mention of the TDIF and how it might dovetail with the work being done. Similarly, the material for the TDIF does not appear to make mention of the other two initiatives. If it is not already occurring, there is a need for close collaboration between all three initiatives so that synergies can be identified and exploited to achieve significant public utility from integration of resources and effort and initiatives.

Privacy aspects

Personal information

8. The Law Council notes that the definition of 'personal information' at section 9 of the Draft Bill seeks to extend the definition that is currently contained the *Privacy Act 1988* (Cth) (**Privacy Act**). Specifically, the Bill defines 'personal information' as follows (with proposed extension underlined):

> ***personal information:***
>
> *(a) means information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> *(i) whether the information or opinion is true or not; and*
>
> *(ii) whether the information or opinion is recorded in a material form or not; and*
>
> *(iii) <u>whether the individual is alive or dead; and</u>*
>
> *(b) <u>to the extent not already covered by paragraph (a), includes:</u>*
>
> *(i) <u>an attribute of an individual; and</u>*
>
> *(ii) <u>a restricted attribute of an individual; and</u>*
>
> *(iii) <u>biometric information of an individual.</u>*

9. The Law Council considers that this definition should be updated to better reflect the Privacy Act as the primary and authoritative piece of privacy-related legislation. As it is currently defined in the Exposure Draft, the approach fails to communicate consistency across legislative schemes or to provide a reasonable transition period to any new or updated terms which may arise following anticipated reforms to the Privacy Act post its review.

10. Noting this position, the Law Council queries whether it is appropriate to extend the accepted definition of 'personal information' at this time, given that a broader review is currently being undertaken into the Privacy Act, which is likely to include detailed consideration of the adequacy and scope of the existing definition. The creation of a further definition as proposed by the Draft Bill may serve to confuse what is already an uncertain area, with the Consumer Data Right scheme referencing personal information by what relates to the individual, while judicial consideration has been given to the point of difference between what information is 'about' an individual and what 'relates' to an individual.[1]

11. A further issue is the decision to extend the definition of 'personal information' to individuals 'alive or dead' in the Draft Bill, noting that this appears to be a significant departure from the current law and practice. The law Council would suggest removal of this extension.

[1] See *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4.

Biometric information of an individual

12. In a similar vein to the above points, the Law Council notes that the Draft Bill refers to 'biometric data' in materially different terms to the Privacy Act, where reference to biometric data and biometric templates forms part of the definition of 'sensitive information' in section 6.

13. The Law Council recommends that the Draft Bill aligns the definition of biometric data to how that term is defined by the Privacy Act. This alignment will help ensure that the law in this area develops in a consistent manner, noting that this area has been subject to substantial regulatory attention and guidance.[2]

Profiling

14. The Law Council is conscious that the TDIF presents a real risk to individual privacy if organisations and government agencies are able to consider and connect different data points and single identifier attributes within the centralised framework. Greater clarity is needed to ensure that issues relating to profiling are addressed given that the regime, by its nature, relies on forms of data matching and profiling.

15. The term 'profiling' is not defined in the Draft Bill nor the Privacy Act. The General Data Protection Regulation (**GDPR**) in Europe provides that profiling consists of:

> *… any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*[3]

16. Large scale profiling is considered a high-risk data process[4] requiring additional governance and protections. For example, under the GDPR, a high-risk process such as profiling would trigger a requirement to conduct a Data Protection Impact Assessment in line with Article 35 of the GDPR. Similar issues arise under the United Kingdom's data protection regime.[5]

17. In light of the concerns regarding the potential for profiling activities arising from the measures proposed under the Draft Bill, the Law Council submits that consideration should be given to incorporating a clear definition of profiling, in line with the approach adopted under the GDPR.

---

[2] See, Iso Amba Kak, ed., "Regulating Biometrics: Global Approaches and Urgent Questions" *AI Now Institute*, September 1 2020 and Guidance by the Office of the Victorian Information Commissioner on *Privacy and Data Protection Act 2014.* See also the definition the Genera Data Protection Regulation (Article 4), which defines biometric data expressly as "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of individuals*".

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Recital 71.

[4] See, Article 29 Data Protection Working Party, '*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (4 April 2017) <https://ec.europa.eu/newsroom/article29/items/611236>.

[5] See, Information Commissioner's Office (UK) '*Guide to the UK General Data Protection Regulation (UK GDPR)*' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>.

Consent

18. The Law Council notes that individuals must expressly consent to the disclosure of attributes to relying parties under section 73 of the Draft Bill. There is some concern that consent may not always be appropriately informed and voluntary, where the individual is not aware of the different data access points or uses for the information.

19. It is unclear to the Law Council how new use cases under TDIF will be consented to, and how that consent will remain current and valid or otherwise genuine and freely given.

20. The Law Council considers that consideration should be given to the inclusion of a specific legislative mechanism enabling an individual to opt-out of the system after they have created a digital identity,[6] and suggests there is a potential need for clarity on the process for withdrawing enduring consent.

Retention and disposal of personal information

21. The Law Council understands that there is no defined safeguard relating to the retention and/or disposal of personal information by an identity provider, or direct connection to the Australian Privacy Principles on this matter under the proposed TDIF.

22. There also appears to be no outlined interaction with other federal regulations, such as the Protective Security Policy Framework, to oversee components of personal information that may be considered public records.

23. The Law Council suggests that consideration should be given to incorporating additional safeguards regarding the retention and/or disposal of personal information by an identity provider, and clarifying how the framework will interact with other federal regulations and policies relating to this issue. Should such steps already be in place, greater guidance could be provided to clarify obligations prior to the scheme commencing.

Enforcement and breach

24. The Law Council has received specific feedback from the Law Institute of Victoria (**LIV**) that the sanctions for a breach of the Digital Identity legislation may be considered inadequate, given the consequences of a data breach for an individual are far-reaching and it can take a considerable amount of time before the extent of the damage incurred is apparent.

25. The LIV notes that the proposed approach may be disproportionate to the potential damage that can be incurred as a result of a data breach, and consideration should be given to alternative penalties such as a financial penalty tied to the accredited entity's revenue. Further, the LIV has pointed out that it is not unheard of for one arm of the government to sue another government agency, and that despite the indirect cost to the taxpayer, this may be appropriate in terms of public visibility and media comment.

[6] See, Judy Skatssoon, 'DTA finds 'overwhelming' support for digital identity' *Government News* (15 February 2021), <https://www.governmentnews.com.au/dta-finds-overwhelming-support-for-digital-identity/>.

26. Finally, the LIV has noted that the financial liability of participants within the TDIF is limited where participants act in good faith and in compliance with legislative rules. The LIV has submitted that this liability be widened to include class actions and individual claims for loss suffered, given the nuanced and potential lasting impact on individuals. This would act as a further incentive for government agencies and accredited providers to ensure the TDIF is functioning as intended and protected appropriately.

Boutique and Small Law Practices as Relying Parties

27. Within the TDIF, there are a number of participating entities that can be broadly categorised as either an 'accredited entity' or a 'relying party'.[7] An accredited entity is a service provider offering digital service, and includes an attribute service provider, credential service provider, identity exchange, identity service provider and a prescribed entity. A relying party is an entity that consumes or relies on the identity services in the TDIS.

28. To participate in the TDIF, accredited entities are required to be onboarded and accredited, whereas relying parties are only required to be onboarded. The Law Council anticipates that law practices will be 'relying parties' under the Draft Bill, because they will use the system in various verification processes. As such, law practices will need to be onboarded (as opposed to onboarded and accredited).

29. The onboarding requirements are contained in chapter 2 of the Draft Bill and require entities to comply with the applicable technical standards and the Trusted Digital Identity Rules (**TDI Rules**).

30. Section 7 of the TDI Rules prescribe the following requirements when an entity is applying for approval to onboard to the TDIS:

> *(a) the entity must have a written plan for testing (within periods and at intervals specified in the plan) the interoperability of its facility and the trusted digital identity system;*
>
> *(b) the entity must have conducted a cyber security risk assessment in relation to its integration of its facility with the trusted digital identity system;*
>
> *(c) the entity must have adopted written processes and procedures:*
>
> *(i) to investigate digital identity fraud incidents in relation to its facility, including incidents notified to it by the Oversight Authority; and*
>
> *(ii) to ensure its compliance with section 44 of the Act;*
>
> *(iii) to prevent, identify and investigate unauthorised access, including by the entity's personnel and contractors, to digital identity information under the entity's control;*
>
> *(d) the entity must have effective procedures to ensure that it complies with the reportable incident requirements;*

[7] Digital Transformation Agency, *Your guide to the Digital Identity legislation* (October 2021) 13.

(e) *the entity must have adopted a business continuity plan that addresses at least the following:*

(i) *disaster recovery procedures;*

(ii) *continuity procedures for critical functions of its digital identity facility;*

(iii) *regular reviews of the plan, but at least once a year;*

(iv) *procedures for notifying the Oversight Authority of changes to the plan and results of periodic reviews;*

(f) *the entity must have effective programs to prevent, detect, investigate and report cyber security incidents, and digital identity fraud incidents, in relation to its facility.*

31. The Law Council is aware of some concern that the onboarding requirements may present a barrier to boutique and small law practices who lack the financial and technological resources necessary to qualify as a relying party. In particular, there are concerns that boutique and small law practices may lack the financial and technological resources necessary to comply with paragraph 7(1)(a) of the TDI Rules, which require prospective relying parties to test the interoperability of its facility and the TDIF. It is possible that boutique and small law practices will not have sufficient financial and technological resourcing to develop and implement a plan in accordance with the TDI Rules.

32. While the Law Council acknowledges that the TDI Rules are an important aspect of regulating who can be a participating relying party, the onboarding requirements to qualify as a relying party may be onerous for some boutique and small law practices for the above-mentioned reasons. There are many instances where legal practitioners are required to verify an individual's identity on a day-to-day basis.[8] This underscores the importance for the legal profession in ensuring that any requisite onboarding requirements are accessible.

33. At a broader level, the Draft Bill and associated rules are part of a 'whole-of-economy solution' that enables the Government and private sector entities in all states and territories to participate in the TDIF.[9] The Draft Bill and associated rules will result in a significant shift in how business will be conducted in Australia and how users interact with those services. Accordingly, consideration should be given to ensure that the onboarding requirements do not effectively preclude some boutique and small law practices, and by extension, their clients, from participating in the TDIF.

34. Moreover, the Law Council understands that where boutique and small law practices are onboarded, their access to the TDIF may be reliant upon third party software providers (e.g. practice management software and searching provider). In which case, boutique and small law practices may not have the capability, as users of that software, to supervise the software provider's compliance with the TDI Rules. It is expected that the software provider will be required to establish and manage their facilities in compliance with the TDI Rules.

[8] For example, verification of client identity requirements under the anti-money laundering regime and verification of identity requirements which are undertaken by Public Notaries. There are many documents which legal practitioners are asked to witness on a day to day basis that require the practitioner to be satisfied about an individual's identity.

[9] Digital Transformation Agency, *Your guide to the Digital Identity legislation* (October 2021) 4.

35. This aspect of the Draft Bill (and associated TDI Rules) may require further consideration and additionally, the Law Council suggests that boutique and small law practices should be provided with the necessary education and assistance to ensure they can meet the onboarding requirements to ensure equal participation in the scheme.