University of New South Wales Law Research Series

Submission to Phase 3 Consultation – Trusted Digital Identity Bill Package

Lyria Bennett Moses, Simon Michael Taylor, Shengshi Zhao, Kim Nicholson and Tim de Sousa

[2021] *UNSWLRS* 88

UNSW Law
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

AUSCL

AUSTRALIAN SOCIETY FOR COMPUTERS & LAW

Allens Hub
for technology, law & innovation

27 October 2021

Digital Transformation Agency
By webform: https://www.digitalidentity.gov.au/have-your-say/phase-3/submission-form

Phase 3 consultation - Trusted Digital Identity Bill package

About us

The UNSW Allens Hub for Technology, Law and Innovation ('the UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The Australian Society for Computers + Law (AUSCL) is an interdisciplinary network of professionals and academics focussed on issues arising at the intersection of technology, law, and society. We are a not-for-profit, registered Australian charity with a charter to advance education and policy development. AUSCL was officially launched in July 2020 - but we have been active in this space since 1981 when the first of our constituent State-based member societies were formed. AUSCL provides a forum for learned discussion and debate through its Policy Lab, Working Groups and Events Program, and attracts support and engagement across Australia and globally.

About this Submission

Our submissions reflect our views as researchers and are not an institutional position.

The Digital Identity Bill package is one of a number of current intersecting reforms at different stages of the policy and political process. This includes reforms to the *Privacy Act*, the *Data Availability and Transparency Bill*, critical infrastructure changes, cyber security regulations being explored in the Department of Home Affairs, identity matching legislation and agitation for greater funding for the OAIC. It is very difficult to comment on part of this process (such as this package) without knowing the outcomes for the whole. For example, if the *Data Availability and Transparency Bill* were to pass, it could be worth considering what the relationship between the National Data Commissioner and the new oversight body might be. Similar intersecting questions arise across and between the different threads of policy reform. It would certainly be easier to contribute to policy debates with a clearer picture of all of its parts.

However, we have made some specific suggestions on the Bill package. In particular:

1. The title of the Bill should remove the term "Trusted".
2. Documentation surrounding the Bill should avoid terms such as 'voluntary', which misrepresent the position under the Bill.

3. The definition of 'biometric' should align with requirements in the TDIF.
4. The Bill should include specific provisions as to what occurs when things go wrong (eg identify fraud, data breach). In particular:
    a. The Bill should explain the consequences where apparent consent is not actual consent; and
    b. The Bill should identify a party or fund liable to compensate individuals suffering loss as a result of using the system.
5. Requirements should be introduced in relation to (1) what constitutes consent, (2) demonstration of consent and (3) documentation of consent .
6. The Bill should require accredited TDIF providers to re-accredit every 3 to 5 years and in the context of mergers and acquisitions by providing updated security compliance documentation.
7. The Bill should be edited by:
    a. clarifying the meaning of 'online';
    b. the contractual mechanism for *Privacy Act 1988* compliance be replaced with inclusion through the statute itself;
    c. supplementing listed functions of the Oversight Authority;
    d. remove reference to de-identification in s 132;
    e. limiting offences that allow for information to be used or shared.

Our rationales for these recommendations are explained below.

The Title

The title of the exposure draft Bill is Trusted Digital Identity Bill 2021. We question the utility of including the term 'Trusted' in the title and suggest it be removed.

It is not necessary for this term to appear in the title when a framework for a Digital Identity System is being established. A position of neutrality which does not presume the trustworthiness of a digital identity system should be adopted. Further, the question of whether the system is ultimately 'trusted' is not one for the system's designers (technical or legal) to make. It is a question for those asked to trust the system, specifically its users.

The Bill may allow for other systems that facilitate or manage the verification or authentication of the identity of individuals. The "trusted" digital identify system constitutes only a proportion of the Bill and other frameworks and additional concepts may be expanded or introduced in years to come.

We thus recommend that the title of the Bill is renamed as *Digital Identity Bill 2021*.

Voluntariness

Documentation around the new digital identity scheme is framed in terms of voluntary participation. There are different contexts in which this term is used. For example, the heading on page 13 of the guide refers to "Two voluntary schemes", but voluntariness here refers to a choice by an entity to be involved as an onboarded accredited entity or as a participating relying party. However, as page 28 correctly points out (at least in the second column), there will be situations where an individual will be required to generate or use a digital identity. This reflects s 30(2) of the Bill which allows for exemptions to be granted.

Leaving aside the question of whether such exemptions are a good idea and the circumstances in which they will be granted, it is important in a sensitive context such as this to be upfront with the Australian public. If there are going to be services people can only access by participating in this scheme, that should be stated directly. Some of the confusion and concern by participants in the

roundtable we held related specifically to lack of clarity around what 'voluntariness' means in the context of the digital identity scheme. The possibility that individuals may not have a real choice as to whether to participate is also a factor to consider in the decision to include provisions that essentially assign any loss where things go wrong to those individuals (discussed below).

There is another sense in which participation in this scheme may not be voluntary. Presumably consent to generate a digital identity will be given in a similar way to online consent more broadly (virtual box ticking). However, it is possible for identity fraud to occur in that step. This will hopefully be rare, but it may (depending on security protocols) be possible for a person to establish a fake digital identity in the name of another, particularly in domestic contexts where individuals may have access to identity documentation of household members It is not clear how the legislation would operate in this scenario. For example, will the civil penalty in s 73 apply where an accredited entity discloses an attribute to a relying party in the honest belief that they had the express consent of the individual concerned? Unless such a scenario is impossible (and that would be a strong claim), it should be made clear in the legislation what consequences follow for individual victims and perpetrators as well as other actors in the system who rely on what they believe to be an individual's consent.

Biometric Revisions

In the Bill, biometric is defined in s 9 as 'any measurable biological characteristic'. This is very broad. In particular, it includes biometrics[1] not covered in the TDIF accreditation rules. For example, Biometric Verification (p 59-63) provides information on use of face comparison, Photo ID, RFID, image acquisition to authorisations like OTP which are static modes of identification. If the intention is to restrict the Bill to those or related methods, then the definition needs to be narrowed.

Alternatively, , the TDIF revised biometric requirements in s 3.8 need to expand to accommodate the broad definition, which would include the use of voice recordings. 'Voice' is already a significant means of data acquisition and authentication in Australia.[2]If the alternative is pursued, the revised rules should specify *for each mode of collection*, like voice recording, the following:

- types of hardware (microphone or camera) for the mode of accessibility to use in Digital ID;
- specific requirements for the matching tests,[3] and for different modes of comparison (image, voice, typing) with user-interface instructions that directs users on how to provide this data;
- clarifying the audit log, reporting and destruction of data;[4] to be specific for each mode of collection under TDIF accreditation rules s 3.9 retention and use of biometric information.

Requirements to document consent

The Bill has included additional privacy safeguards to protect personal information, including requirements for express consent in sections 38, 73, 74, 76, 77, 79, 80 and 82. However, the Bill does not provide details for capturing and verifying such express consent. It is not clear what constitutes

[1] Authentication on individuals can be assigned with identity categorisations using voice, motor skills, keystrokes etc. Yampolskiy R. and Govindaraju, V. (2008). Behavioural biometrics: a survey and classification. International Journal of Biometrics, 1(1), 81-113.

[2] For example, in the banking sector and for the Australian Taxation Office, voice print authentication is adopted for three main reasons: (1) accessibility, facilitated by common phone hardware (microphone) and broadly established telecommunications; (2) reduction in user trouble shooting for production requirements e.g. sufficient illumination on faces in collection of photographic images (as required by 3.8.3(6) of TDIF accreditation rule document); (3) increase in authentication efficiency and ease of data collection.

[3] As Clare Garvie notes in the use of facial recognition across US policing contexts 'the algorithm you purchase and use influences the result … but there are no vetting lists even for law enforcement': Garvie, Clare. "Face Recognition in U.S. Investigations: A Forensic without the Science Webinar." In UNSW Grand Challenges, online presentation, August 5: UNSW Sydney, 2020.

[4] The ATO voiceprint collects 120 characteristics 'such as pitch and tone and how you speak' https://www.ato.gov.au/general/online-services/voice-authentication/ providing data determinations on individuals e.g. gender, demographics, and possibly level of education.

express consent, how TDIF providers can show proof for express consent and whether individuals or the TDIF providers have obligations to keep proof of such consent.

Consent is defined as 'express consent or implied consent' under the *Privacy Act 1988* (Cth) s 6(1). Express consent is defined as 'consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement' by the OAIC.[5]

Additional requirements should be included to require the entity using or disclosing personal information to provide proof of consent. Our recommendation is for the Bill to include:

- definition of *consent* or *express consent* in the Definitions section, consistent with the definitions provided by the OAIC above;
- additional wording to require TDIF providers to demonstrate such express consent. Suggested wording in *italics*: an entity may use or disclose personal information in certain ways if the individual to whom the information is disclosed has expressly consented to the use or disclosure *and if the entity is able to demonstrate such express consent*; and
- an additional section to set out requirements for TDIF providers to document such express consent for a certain period of time (e.g. 7 years).

It is noted that specific requirements to keep a record of express consent have been included in the Trusted Digital Identity Framework Accreditation Rules. It is recommended to keep such requirements in the Bill.

Clearer consequences where things go wrong

The above example exemplifies the need to consider carefully how the Bill will operate when things go wrong.

Some of the sections that deal with this issue are worded in ways that are confusing. For example, s 39(1)(c):

> If, while onboarded to the trusted digital identity system, an accredited entity: provides, or fails to provide, the service in good faith, in compliance with this Act and with the technical standards that apply to the entity the entity is not liable to any action or other proceeding, whether civil or criminal, brought by an accredited entity or a participating relying party in relation to that service.

At least on one reading, this suggests that if an accredited entity *fails to provide the service in good faith*, it is *not* liable (see words underlined above). This could be reworded for grammatical clarity as:

> If, while onboarded to the trusted digital identity system, an accredited entity: acts in good faith, in compliance with this Act and with the technical standards that apply to the entity, the entity is not liable to any action or other proceeding, whether civil or criminal, brought by an accredited entity or a participating relying party in relation to its provision of that service or failure to provide a service.

However, even redrafted, this clause (and the Bill) fails to clarify who is liable to individuals ultimately negative impacted by identity fraud as a result of the use of the system. This is an important question to answer. One option is to establish a fund so that individuals can be compensated for harm that result from security flaws or human error in the operation of the system. An alternative is to determine a basis on which an entity can required to compensate individuals for harm caused by its failure to comply with the various requirements.

Duration of the accreditation validity

The Bill does not include an expiry date of a TDIF provider accreditation, which implies that once a provider has been accredited, such accreditation will remain valid indefinitely, and the provider will not be obligated to renew or re-certify its TDIF accreditation. The Trusted Digital Identity Framework

[5] See definition of consent, express consent and implied consent, provided by the OAIC Chapter B of the APP Guidelines, https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts#consent.

Accreditation Rules require a TDIF provider to keep relevant credentials up to date but the Rules do not include any audit, review, renewal or re-accreditation process. A TDIF provider has the obligations to maintain its current security standards and keep up to date with the latest technology. The current technical requirements may be obsolete in five years, which is why internationally recognised certification bodies (e.g. ISO, NIST, SOC) require entities to be re-certified every 3 to 5 years.

It is recommended for the Bill to consider a similar approach and require accredited TDIF providers to re-accredit every 3 to 5 years by providing updated security compliance documentation. This would not incur additional costs as TDIF providers are already required to maintain their relevant security certifications and annual penetration testing reports. The accreditation renewal process will be a simple check once every 3 to 5 years for the Oversight Authority to ensure that all TDIF providers are still compliant with the requirements set out in the Trusted Digital Identity Framework Accreditation Rules.

The Bill should also incorporate a reporting requirement for accredited entities to report large company mergers and business acquisitions. For example, Nuance the voice provider for the ATO voiceprint services has 30+ internal acquisitions since 2006, and has recently been acquired by Microsoft.[6] This should trigger a re-accreditation process, which would be preferable to the s 87 mechanism.

Suggested edits to exposure draft bill

In this section, we make some specific drafting suggestions on different clauses within the Bill not dealt with above.

1. Section 9 defines digital identity as 'a distinct electronic representation of the individual that enables the individual to be sufficiently distinguished when interacting online'. This definition should be supplemented by the specific user conditions for 'interacting online'. For example, if 'online' means having an established Internet connection, it should refer to a person using a computer terminal,[7] a person on a mobile phone, and a person in a teleconference. This would then distinguish user data from connected devices in the Internet of Things. The same 'online' definition should be applied across the Bill including in s 3.
2. In section 65(2)(c), an entity not bound by privacy law can instead enter into an agreement to act in accordance with some aspects of the *Privacy Act 1988*. A better mechanism would be amend the *Privacy Act* so that it applies to any entity that has a trusted provider agreement with the Commonwealth. This ensures that the obligations are not merely contractual, but rather fall within the regulatory provisions of the *Privacy Act* directly. This would require amendment to several provisions, including s 6D(4) (excluding such entities from the definition of small business) and s 5B(2) (providing that such entities have an Australian link).
3. The list of functions of the Oversight Authority provided in Section 87 does not include the following essential functions 1) to assess and issue TDIF accreditations, and 2) to provide ongoing audit and review on accredited TDIF providers, and the right to revoke TDIF accreditations based on the audit results or any evidence of non-compliance. We recommend to include these additional functions in the list.
4. Section 132 provides that information has to be destroyed or de-identified in particular circumstances. However, de-identification is a risk-based process and there are ever-increasing

[6] 'Demand for speech recognition continues to be high, and the combination of Nuance's intellectual property and Microsoft's cloud and analytics capabilities will result in more sophisticated offerings with increased interoperability. In addition, Microsoft can apply the technology to other industries and use cases, which could lead to more development within speech recognition and AI'. https://healthtechmagazine.net/article/2021/07/what-microsofts-nuance-acquisition-means-healthcare-industry

[7] This is a specific category in HCI human computer interaction biometrics—utilising input devices such as keyboards, mouse, touchscreen

ways for de-identified information to be re-identified. It would be better to remove reference to de-identification here and require destruction of information.

5. The provisions that allow for information to be used in the context of offences against a law of the Commonwealth/State/Territory (eg ss 75, 81) should be limited to "serious" offences.

Yours sincerely,

Lyria Bennett Moses (UNSW Allens Hub)

Simon Michael Taylor (UNSW Allens Hub)

Shengshi Zhao (AUSCL)

Kim Nicholson (AUSCL)

Tim de Sousa (AUSCL)