Submission: Australian Government Digital Identity Legislation Position Paper

Shengshi Zhao, Kim Nicholson, Lyria Bennett Moses and Monika Zalnieriute

[2021] *UNSWLRS* 86

UNSW Law
UNSW Sydney NSW 2052 Australia

16 July 2021

Australian Government Digital Transformation Agency
By submission form

Submission: Australian Government Digital Identity Legislation Position Paper

We are grateful for the opportunity to provide feedback on the Position Paper on the proposed legislation for the Digital Identity system (**Legislation**). This is a joint submission prepared by the UNSW Allens Hub for Technology, Law and Innovation (**Allens Hub**), and the Australian Society for Computers and Law (**AUSCL**).

About us

The Australian Society for Computers and Law (‘**AUSCL’**) is an interdisciplinary network of professionals and academics focussed on issues arising at the intersection of technology, law and society. It is a registered Australian non-profit charity with a charter to advance education and advocacy. AUSCL was officially launched in July 2020, but its member State societies were formed as early as 1981. AUSCL provides a forum for learned discussion and debate through its Policy Lab, Working Groups and Events Program attracting support and engagement across Australia and globally.

The UNSW Allens Hub for Technology, Law and Innovation **(‘Allens Hub’)** is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens 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 Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

About this Submission

Our current submission is not intended to be a comprehensive response to all of the issues raised in the Australian Government's Position Paper on Digital Identity Legislation. Instead, our current submission is limited to comments and feedback on the following areas:

1. Independent oversight of the system;
2. Onboarding to participate in the system;
3. Individual and User expectations;
4. Privacy and consumer safeguards;
5. Security requirements and incident responses;
6. Record keeping and data retention; and
7. Liability and redress framework.

Our submission reflects the views of our respective organisations, and does not reflect the views of our employers, clients, workplaces or any other associations of which we may be part.

1. Independent Oversight of the System

The position paper indicates in Sec 3.1 that the Legislation is intended to ensure effective governance and regulation of the system by means of:

- an independent statutory office holder, the Oversight Authority (**OA**), advised by expert Advisory Boards appointed by the Minister;
- the Information Commissioner overseeing compliance with the additional privacy safeguards in the primary Bill for the Digital Identity system.

Various issues must be addressed to ensure the effectiveness and independence of the OA including:

- Availability of a public-facing channel to consider and address any issues or complaints raised by the public;
- Accountability and transparency mechanisms to ensure at all times the unbiased stance of the OA, influenced by any external or vested interests;
- Adequate and appropriate levels of resourcing to ensure the effective operation of the OA's compliance frameworks. The OA must have the financial and technical capacity to perform its regulatory and compliance functions, such as by ensuring staff have high proficiency in the skills and knowledge required for inquires inquiry and investigations;
- Sufficient capacity of the OA to effectively manage and perform its function particularly during the the initial introduction of the Digital Identify system which can be reasonably anticipated to involve confusion and disputes;
- the Office of the Australian Information Commissioner must receive appropriate additional funding and resourcing to manage the increased workload associated with the Digital Identify system;
- The *Privacy Act 1988* and the proposed *Data Availability and Transparency Bill 2020* should apply to the Oversight Authority to protect the privacy of the general public;
- Consideration should also be given to other oversight bodies, for example the role of federal, state and territory bodies that oversee police agencies and their role in investigating incidences of prohibited activities in the legislation (such as speculative profiling).

2. Onboarding to Participate in the System

It is proposed in Sec 5.4 that the Legislation will allow for a government body, company, trust, partnership or unincorporated association wishing to participate in the system as a relying party to apply to the Oversight Authority be onboarded to the system. Once approved, the relying party will be listed on the Participant Register and will become a Participant in the system.

It is worth considering that the system requires clear onboarding guidelines for Participants to register. It is also worth considering what types of information will be available to participating organisations in the Government's Trusted Digital Identity Framework (TDIF), whether they will be able to share users' personal information with each other, and what level of access they will gain once they become Participants.

Another point to consider is the geographic location of Participantsand their staff members. Personal information of Australian citizens should not be held on servers located outside Australia or stored by or within overseas organisations. Even if there is a local presence of an international company, technical support and system administrators may still reside overseas and be able to access data from overseas. Overseas access to personal information may expose Australian data to foreign jurisdiction, such as the United States' Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) or European Union's General Data Protection Regulation (GDPR). It is crucial that information in the Digital Identity system is retained and managed within Australia and to ensure the integrity of the system.

Detailed technical security requirements also need to be addressed for any participants, if onboarding to this system means they will gain access to additional personal information. Additional data governance, privacy and incident management requirements should also be included and addressed in detail.

The legislation will also allow for application only in-part TDIF Providers, which means TDIF providers will be accredited based on their specific roles. Government bodies or companies which choose to be TDIF-accredited for roles they perform in their own digital identity systems can rely on TDIF accreditation to build trust in their systems without being subject to the entirety of the Legislation. This may be an area of risk as organisations may take advantage and advertise as being TDIF-accredited without being legally liable for all the requirements. It will be a concern if TDIF providers are accredited for only some of the roles they perform so are not subject to the same privacy and security standards for all of the roles they perform. The legislation may wish to require TDIF-accredited entities to state clearly the roles for which they are and are not accredited and specify the applicable requirements for each specific role to avoid misunderstanding.

3. Individual and User Expectations

From an individual and consumer perspective, some of the common considerations of working with various TDIF providers may include:

- transferability and portability - whether identity registered and verified at one provider can be ported to another provider easily;

- cybersecurity and data safety - whether all the providers are subject to the same security requirements;
- jurisdiction - digital identity related information should not be stored on overseas servers or handled by overseas organisations;
- digitalising certain paper records for convenience, such as wallet, credit cards, licences and professional certification;
- consistency in the verification process - different providers should adopt the same ID verification process to ensure a consistent user experience;
- consistency in the collection notices - express consent needs to be collected from the users and passed on to relevant parties. There should be a specific mechanism and a consistent approach across various providers, and a simple way for users to understand the process. It is recommended for organisations to use consistent infographics or videos to explain collection, disclosure, and use of identity information in a simple way.

Other considerations may include multi-language support for different cultural backgrounds, and guardian verification for minors using the TDIF service.

4. Privacy Safeguards for Individuals and Consumers

The position paper provides in Sec 3.5 that the Trusted Digital Identity Framework (TDIF) currently includes a range of system specific privacy and consumer protections for Users. One of the key purposes of the legislation is to ensure privacy and consumer safeguards within the TDIF are enshrined in law, providing enhanced protections for User data and personal information on the system. This will provide clarity for Users on:

- how their data will be used and the requirement for consent;
- who can access their data and in what circumstances, with strict penalties for misuse of that data;
- what the liability, penalties and redress are for fraud or misuse of data.

This area may be at least partially addressed in the reforms to the Privacy Act (Cth) as the reform process aims to address these areas. The new Digital Identity Legislation should reconcile with the new Privacy Act to avoid any conflicts.

Concerns in relation to Data Enrichment and other issues

Moreover, there currently is no clear definition or description of data enrichment in any legislation, and in practice there are many variations of data enrichment. Data specialists often gather various streams of insights, many de-identified, from different sources and run advanced algorithms to generate new insights attributable to individual consumers for data enrichment.

It needs to be addressed that data enrichment today is no longer a simple solution of taking data from one source to combine with the other source. It is a process involving many data streams and often it does not need personal information to achieve data enrichment. Any sharing of insights on an individual level, even de-identified, may be used for data enrichment.

It is also worth noting that one of the privacy protection mechanisms requires decentralising personal information storage. By creating a unique digital identity and centralising the storage of relevant IDs for verification purposes, it may create additional identity theft risks for users using

digital identity. It is strongly recommended that a Privacy Impact Assessment be conducted over the operational solution before this initiative goes live.

Finally, there is a suggestion that Accredited Participants will be entitled to "de-identify the data to create aggregate data". It is important to understand in this context that de-identification is a process, not an end-state. In other words, it is possible to re-identify data that has gone through a de-identification process. It would therefore be useful to specify a meaning of "aggregate data"; the work in NSW on a quantified personal information factor may be useful here.

5. Security Requirements and Incident Responses

The position paper provides in Sec 3.5.1 that the TDIF accreditation scheme and the Digital Identity system are designed to provide Users, TDIF Providers, Accredited Participants and Participants alike, a safe and secure framework to access and provide digital identity services.

Additional technical requirements should accompany the Legislation so that participating organisations will be required to meet the same security standards. The legislation should consider introducing the requirement for an annual security audit for accredited organisations. The Legislation should also consider designing re-accreditation, annually or every three years, into the process to ensure organisations continue to meet the same security standards (similar to ISO re-accreditation).

Security audit and assessment should be provided by the Oversight Authority to ensure compliance. Incident response will be supported by the Australian Government through the Australian Cyber Security Centre (ACSC). Information sharing for security and incident management purposes should be governed with strict access and data retention requirements. Personal information should be de-identified in the data sharing process where possible.

6. Record Keeping and Data Retention

The position paper provides in Sec 7.4.8 that metadata and activity logs may be retained by Accredited Participants for a period of seven years (consistent with many of the disposal authorities under the Archives Act and retention obligations under the *Corporations Act 2001* (Cth)) after a User deactivates their digital identity or their account is deleted for inactivity, or in the case of an identity exchange, seven years after it is collected.

Several aspects should be considered regarding record keeping and data retention:

- The new Digital Identity Legislation should specify its relationship with existing data retention legislation to avoid any conflict and further fragmentation of this already complex area of law;

- If a state government agency collects digital identity information, it may fall under State records management legislation (e.g. State Records Acts), and relevant record disposal may be permitted by the Board of the State Archives and Records Authority;

- There may be different retention requirements for logs and metadata related to digital identity verification (e.g. when the application was initiated, whether it was successfully verified, etc.) versus the actual personal information (e.g. names, date of birth, driver's licence number, a copy of passport for verification, etc.). For inactive users, it will be

preferred if the actual personal information can be de-identified in storage immediately following account deactivation. This means information such as names, emails and date of birth will be de-identified, but account numbers, unique user identifiers, account activities, user history, deactivation date, system logs and non-personal metadata information will be retained for 7 years;

- Whether users have a right under the Privacy Act to request their personal information be deleted - organisations may refuse to permanently delete a user's personal information if the Legislation requires organisations to keep the entire records for 7 years. This may need to be considered as an accredited organisation may no longer be accredited and users may wish for the organisation to delete their personal information;
- Collection notification - if users will not be able to request their personal information be deleted for 7 years, this should be communicated to the users clearly in the collection notice prior to users providing their personal information;
- Using or sharing of information related to digital identity - deactivated users may not expect their digital identity to be used or shared. If organisations will continue to hold such information for as long as seven years, relevant requirements should be in place to restrict organisations from using or sharing such information collected from deactivated users.

We welcome the suggestion of conducting a full Privacy Impact Assessment to consider this aspect.

7. Liability and Redress framework

Assuming the Legislation is open-ended so that digital identity can be used in potentially any context, there are contexts where substantial and irreversible risk of harm to individuals from identity fraud may arise. In our view this is an area of very significant concern.

Examples include use in land transactions, where the Torrens system means that transfers are rarely reversed even in the context of identity fraud, and large transactions where customers agree to be bound as part of standard terms and conditions. In such cases, it is completely inadequate to merely offer Users "advice and assistance" (even if extensive) - rather, it is important to consider whether and how financial losses are compensated. Failure to address such issues will adversely impact trust in the system, and ultimately its effectiveness.

From an individual User perspective, it does not matter *where* liability falls. It is proposed to limit liability on Accredited Providers (to situations involving bad faith or legislative breach) and on the Oversight Authority. It seems therefore that, in most cases, the proposal is for the loss to lie with individual victims of identity fraud. This is despite the fact that those individuals are the least able to avoid the loss (they do not control cyber security practices of those in the system), are the least able to measure and understand the risk (including due to a lack of transparency about cyber security protocols), and are the least likely to seek insurance against the risk (partly due to a lack of such understanding). Limitations on liability, if offered, should therefore be accompanied by a practical, accessible mechanism to compensate Users who suffer financial loss as a result of using the system.

The most efficient mechanism for this may be to establish an assurance fund or compensation mechanism (funded by fees or through insurance) in the Legislation. The current proposal that places responsibility and the onus of proof on Users who suffer financial loss (compared against a standard that in most cases of harm will not apply) fails to incentivise the adoption and maintenance of strong

cyber security practices. Indeed, it places Users in a worse position than under the current law (due to limitations on liability), and is unethical.

Should the proposal proceed on that basis, there would need to be very clear warnings to Users as to the financial risk of participation and the effective loss of a right of action against potentially negligent parties in the event of financial loss in some circumstances. Any limitations of liability should not extend to non-Users whose identities are stolen through the system as such are not given an opportunity to consent.

Consultation

Please contact us if you would like to discuss any aspect of this submission either in person or as a round table discussion.

Yours sincerely,

Marina Yastreboff
President
Australian Society for Computers & Law

Lyria Bennett Moses
Director
Allens Hub for Technology, Law and Innovation

With thanks to our authors:

Shengshi Zhao, Kim Nicholson of Australian Society for Computers & Law
Lyria Bennett Moses, Monika Zalnieriute of Allens Hub for Technology, Law and Innovation