Identity Vault Submission to Australia's Digital Identity Legislation

Phase 2 Consultation

Introduction

Identity Vault Pty Ltd is a digital identity start up and wholly Australian owned. Identity Vault is currently developing a digital identity application and identity platform based on "The Digital Identity Framework" published by the Digital Transformation agency.

Identity Vaults initial design was created to provide verification for online gaming communities, improving safety and confidence for younger gamers and their parents. The digital identity application will enable people to create a digital identity then use this digital identity to biometrically verify themselves to access communities and services. Identity Vault additionally would like for its customers to utilise their digital identity for all available online interactions.

If there are any questions associated with this response or if additional information is required, please contact Identity Vault at:

[redacted]
[redacted]
[redacted]

General Overview

Identity Vault is grateful for the opportunity to provide feedback on this phase 2 consultation for the Digital Identity Legislation.

We broadly agree with the direction of the legislation, however have identified several key areas where further clarity or definition is required.

The additional privacy and consumer safeguards proposed for the legislation will potentially lead to a 2 tiered identity provider industry, those Digital Identity providers that are accredited and those that are subject to looser standards. In our opinion the privacy and consumer protection standards proposed for this legislation should be enshrined in the Privacy Act 1988 and thus applicable for all companies wishing to offer digital identity products.

The security requirements to be documented as part of the legislation should contain minimum protective security and fraud standards for all accredited participants. To reduce the requirement to make regular changes to the proposed legislation the standards should document the desired outcomes and be agnostic to the technology required to achieve those outcomes.

In the pages below we have documented specific feedback on each of the key areas we have identified in the proposed legislation. We would be happy to discuss any of these points in more detail if required.

Questions/ Feedback

Section: Purpose of Digital Identity Legislation

3.1 Independent oversight of the system

The Legislation will ensure effective governance and regulation of the system. Effective governance will be assured by:

an independent statutory officeholder, the Oversight Authority, advised expert Advisory Boards appointed by the Minister,the Information Commissioner overseeing compliance with the additional privacy safeguards in the Bill.
These permanent governance arrangements will aim to give Users confidence that privacy and consumer safeguards enshrined in the Bill are strictly enforced.

Identity Vault believes best practice would have the expert Advisory Board containing representation from all stakeholder groups within the digital identity framework to ensure equal representation across the environment. Furthermore Identity Vault would like to see an advisory group established containing a deeper representation of stakeholders to advise and provide recommendations to the Board.

3.3 Accreditation scheme

The Legislation will also provide the legislative authority for the Oversight Authority to administer and manage an accreditation scheme for entities seeking TDIF accreditation for their digital identity activities, including for those outside the system. TDIF Providers will meet the same safeguards in the Bill and TDIF rules as Accredited Participants in the system.

Identity Vault believes the Oversight Authority should administer and manage entities accreditation for activities within the system. Those activities falling outside the system will be subject to existing legislation such as the Privacy Act etc

3.4 Enforceable set of rules

It is proposed the Minister be given power to issue technical standards relating to how technology in the system works. These could include standards for security, interoperability and data specifications.

Identity Vault would like to recommend that these technical standards be minimum standards and in order to encourage competition and innovation, if individual Accredited Participants wish to exceed these minimum standards they should be free to do so. In order to achieve this innovation the standards should be contained in the legislation.

3.5 Privacy and consumer safeguards

The Digital Identity system is designed to ensure the privacy of Users is protected and strong safeguards are in place to ensure choice, data protection and accessibility.

In addition to the existing privacy protections in the Privacy Act, the TDIF currently includes a range of system specific privacy and consumer protections for Users. These protections include:

- *restrictions on the creation and use of a single identifier across the system*
- *restrictions on data profiling*
- *restrictions on the collection and use of Biometric Information*
- *requirements for Users' express consent before enabling their authentication to a service.*

In September 2018, the second privacy impact assessment recommended legislation to ensure Accredited Participants are legally bound to key privacy standards specific to the system. Additional privacy impact assessments will be undertaken as the system expands to ensure privacy requirements are upheld.

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*

Identity Vault would be comfortable in aligning with these principles as a potential accredited participant however would like to recognise that the Australian digital identity framework is not the only digital identity framework. Other frameworks such as FIDO will not be as strict on the key points mentioned above. Examples of this would be the use of Facebook or Google profiles to login to secure sites. These companies business models are based on data profiling. This approach could leave Australian digital identity participants at a significant disadvantage to global competitors.

3.5.1 Security requirements

Identity Vault believes that the legislation should not be used to drive outcomes/behaviours from a technical delivery standpoint as Technology will change and evolve over time. The best technology solution today will not be market leading in the future.

We would recommend not to regulate the technology, legislate the standards, and allow for innovation through technology by the participants.

As an example the TDIF appears to be creating a new way to authenticate when there are existing standards already in use e.g. OAuth2, Open ID Connect etc. Additionally adding some changes to Open ID Connect could potentially create vulnerabilities. We agree with the response provided by Vanessa Teague's in the phase 1 consultation feedback.

We believe using one technical solution is not the answer for broad online usage.

As an example comparing two such solutions,

TLS is a long term identification artifact, it is static, as data within cannot be altered or changed because it is cryptographically signed itself. It is usually issued for several years.

OpenID is more convenient for communication between technical actors, as its token is self-contained and brings information important for specific system itself. It can be filled with information needed for specific use case then signed by SSO server.

4 Structure of the Digital Identity Legislation

The legal framework for the system will include:

- *a Bill passed by Parliament (the Trusted Digital Identity Bill)*
- *rules*
- *written guidelines and policies.*

The Bill will include subject matter that will not need to regularly change to keep pace with technical developments, such as the privacy safeguards for individuals. It will also include important subject matter that should only be altered by Parliament, such as a power authorising the Minister to set charges.

Identity Vault believes that this approach is the best way to manage the behaviours of participants The only suggested change being regulating a minimum technology standard as discussed in Section 3.5.1 with scope for participants to exceed these standards to drive innovation rather than limiting innovation by regulating and enforcing one set of technical standards.

5.4.1 Scope of the legislation

The Legislation is not intended to apply to all digital identities and digital identity systems in Australia.

Identity Vault believes that only applying the legislation to certain digital identity systems and not all digital identity systems operating in Australia may not provide the right outcome for consumers in Australia. Those digital identity providers outside the Australian framework will be able to operate at a competitive advantage in commercial settings.

7.4.3 Restrictions on data profiling

It is proposed the Bill will prohibit Accredited Participants from collecting, using and disclosing information about a User's behaviour on the system, except to:

- *verify the identity of a User and assist them to receive a digital service from a relying party*
- *allow the User to view their own behaviour on the system (for example, on a dashboard)*
- *support an identity fraud management function*
- *respond to a lawfully made requests for information for an investigatory purpose[10] (subject to the prohibition on speculative profiling for an investigatory purpose)*
- *improve the performance or usability of the participant's digital identity system*
- *de-identify the data to create aggregate data.*

Additionally, it is proposed the Bill will prohibit Accredited Participants from using attributes and other information obtained from the digital identity system for prohibited purposes, even with a User's consent. Prohibited purposes will include:

- *unrelated marketing[11]*
- *speculative profiling[12] on digital identity information for an investigatory purpose[13]*
- *another purpose prescribed in legislative rules.*

These restrictions will not apply to attributes received by relying parties. The attributes received by relying parties by their nature are more limited and more suitably regulated under general privacy laws such as the Privacy Act.

Identity Vault, whilst agreeing with the above approach, would like to highlight that this could lead to digital identity systems and products that are outside the system gaining a commercial advantage through being able to utilise their data in areas broader than the 6 points mentioned above.

7.4.11 Acting on behalf of another and minimum age

It is proposed the Bill will provide a basic mechanism to authorise arrangements for a person to act on behalf of another. The specific operational details of appointing, managing and terminating an authorised representative will be covered by the rules. This will provide more flexibility for the vast array of circumstances that would need to be considered for such an arrangement. It is proposed the same privacy and security safeguards will apply to an authorised representative as they do to a User. These provisions do not intend to override any existing Commonwealth or state and territory laws regarding authorised representative arrangements.

It is proposed the Legislation will provide a default minimum age of 15 years for the use of a Digital Identity in the system. The Legislation will provide the Oversight Authority with the ability to override the default minimum age limit in circumstances where it considers appropriate (for example, to match a relying party's statutory minimum age requirement for access to its service).

Identity Vault believes the minimum age for the use of a digital identity should be lower than the minimum age suggested above. Australian children can open bank accounts in their own name at banks in Australia from as young as 9 years old. Social media accounts are able to be opened at 13 years old.

Younger Australians are active users of online services, particularly games, online communities and social media. Opening up the digital identity to users younger than 15 will provide them and their parents with confidence.

9.3 What's changed since the Consultation Paper?

There will be a liability framework in the Legislation and Accredited Participants will not be financially liable for losses suffered provided they have acted in good faith and complied with the legislative rules and requirements relating to accreditation and the system. It is proposed there will be a statutory contract between Accredited Participants and relying parties on the system, giving Participants the right to seek loss or damages where another Participant has breached the system's rules. There will also be provisions outlining redress mechanisms to help recover losses and damages resulting from cyber crime and identity theft.

9.4.2 Financial liability

It is proposed under the Legislation that an Accredited Participant will not be liable for loss or damage suffered by a Participant using the system provided the Accredited Participant was acting in good faith and in compliance with the legislative rules and requirements relating to the system.

If the Accredited Participant does not comply with the legislative rules and act in good faith, the Accredited Participant would be liable for loss and damage suffered by all Participants flowing from that non-compliance.

Identity Vault agrees with this approach for Accredited Participants.

11.4.3 Selection of service providers to the system

To become a service provider in the system, the entity must be both TDIF accredited and onboarded to the system. A process will be required to select which TDIF accredited entities can be onboarded to the system and therefore become a service provider in the system.

A service provider to the Digital Identity system means a company or government body seeking to perform a TDIF accredited role for the system; that is, an identity provider, credential service provider, attribute service provider and identity exchange. The DTA proposes to select service providers outside a legislated process, which would be conducted by an Australian Government agency, effectively providing a controlled entry into the system.

The Legislation will support this selection method by requiring entities seeking to become a service provider to be on the Participant Register, which would require them to be onboarded to the system and to have an agreement with the Australian Government to provide services.

Competitive neutrality principles would apply to ensure the Australian Government would not enjoy competitive advantages over private sector competitors. In particular, it is noted that Charging Principle 1 should not apply to the competitive disadvantage of private sector competitors.

This section of the proposed legislation appears to restrict the opening of the system to the private sector mentioned in Section 3 and the principles of an open federated system. This appears to indicate that even if an entity is accredited and onboarded, that an additional selection process would be required at the discretion of the DTA.