DIGITAL SERVICES BOARD

Tasmanian Government

Submission on the Digital Identity Legislation consultation paper

The Digital Services Board (the Board) is the primary oversight and decision making forum for the Tasmanian Government's digital transformation agenda. The Board's role is to consider, champion and support investment in the implementation of digital strategies, policies and initiatives with whole-of-government benefits.

The Board is chaired by the Secretary of the Department of Premier and Cabinet and comprises the secretaries of all Tasmanian Government departments as well as the Chief Executive Officer of TasTAFE.

Overview

The Board strongly supports the development of an overarching framework and national approach to digital identity verification, service provision and access.

The Board views the proposed structure and scope of the legislative framework for digital identity outlined in the consultation paper, to be comprehensive and believe it will appropriately address key issues of privacy, security, choice and consent.

Privacy and data breaches

The Board requires further clarity on the responsibilities regarding funding, managing and coordinating any data breach or cyber security incident in the digital identity ecosystem.

The Board notes that the (Commonwealth) Privacy Act, and the Australian Privacy Principles contained in it, are being reviewed – although neither terms of reference nor timeframes for this review are provided. It would be helpful for further detail of this review and/or its outcomes to be included in the next stage of consultation on the digital identity legislation.

In addition, the Tasmanian Government will need to review the draft Bill to understand the impact, implications and any potential conflicts with Tasmanian privacy legislation. This will include ensuring that the legislation doesn't limit the ability for state government departments to share information they would otherwise be lawfully allowed to, as a result of Tasmania being part of the digital identity ecosystem.

Digital literacy

Tasmania's relatively low levels of digital literacy and, in some regional and rural areas, limited internet access is an important consideration with respect to the provision of choice and accessibility under the digital identity system. More so as the consultation paper acknowledges that some local councils, small government agencies and/or smaller private sector organisations may be unable to support both in-person and online service provision.

Alternative identity verification mechanisms, other than that proposed by the digital identity legislation, will be needed for some time into the future to meet Tasmania's needs.

The Board submits that development of the legislation, and indeed the operation of the framework, should seek to ensure that no one is excluded from access to government and other essential services.

Comments

While the Board has not addressed every question in the *Digital Identity Legislation Consultation Paper,* the following section details comments considered pertinent to specific questions.

Responses to specific questions:

Purpose of the Legislation

1A) Are the matters above (legal authority, privacy protections, governance, amendments) relevant matters which should be included in the Legislation?

These are considered essential if the digital identity system is to be operate successfully across both government and non-government environments.

1B) Are there additional matters which should be considered?

Consideration should be given to the user's ability to provide informed consent regarding the use of the identity, how they do that, and making it clear they have control over the identity and its use.

The applicability of other regulatory frameworks eg the EU General Data Protection Regulations (GDPR) should be considered.

Structure of the legislative framework

2A) What matters covered by the TDIF should be incorporated into the primary legislation?

The power for the oversight authority to set and maintain written policy and oversight of the system. While providing the power to set the operating rules to the Oversight Authority, the legislation also needs to have protections against sudden and detrimental changes that will impact the relying parties or identity service providers.

2B) What matters covered by the TDIF should be incorporated into Operating Rules?

The Board supports inclusion of the TDIF Accreditation process under the Operating Rules to enable public trust that the accreditation process is robust and not easily changed.

The Operating Rules should also include penalties for failure to observe obligations with respect to security and privacy considerations.

2C) What matters covered by the TDIF should remain as policy?

TDIF principles and procedures, including those that provide practical advice to digital identity providers and identity users regarding their use of the system.

Scope of the Legislation

3) Is a publicly available 'Digital Identity Participant Register' an appropriate mechanism to communicate who will be covered by the Legislation?

The Board supports the need for a highly transparent process to identify those entities involved in order to build and keep trust in the identity system.

4) Are the proposed obligations on relying parties described above reasonable? Should there be any additional obligations?

Proposed obligations are reasonable. The TDIF references the Australian Government Information Security Manual, however given relying parties may not be government, consideration could be given to aligning obligations with an international security standard such as ISO 27001.

5) Are the concepts outlined above appropriate to include in a definition of 'Digital Identity' for the Legislation? Are there any additional concepts that should be included?

The definition should be such that it doesn't limit or affect digital identity implementations that are not part of the TDIF. Therefore the legislation needs to define what the TDIF is and also needs to distinguish between 'the Exchange' and other identity exchanges that may be peripheral to the TDIF.

6) Does the Legislation need to include a definition of Digital Identity information, or is it preferable to rely on the definitions of personal, sensitive, or protected information in other Commonwealth Acts?

Since state governments don't all use the same classification system, there should be a common set of definitions that apply to the TDIF legislation, but for consistency, the legislation should reference definitions already in common use within other legislation, so as not to generate confusion.

Financial sustainability of the system

7) What factors should be considered in the development of a charging framework for the system?

The Board notes that the cost of using the system, as well as the administrative or legal burden associated with becoming accredited, participating in the system, and meeting any liability obligations (should they arise) will be key considerations for the Tasmanian Government in becoming a participant in the TDIF and could be a significant barrier to entry. The Tasmanian Government needs to have clear understanding of the financial implications of any usage fees that it will be charged, as well as its obligations in terms of any redress or penalties in the instances of misuse.

The intention that users will not be charged for the use of a digital identity is supported, as applying charges for identification will preclude some community members from accessing services.

Digital services, enabled through digital identity are increasingly becoming fundamental infrastructure analogous to roads and bridges required for the Australian community. The Board therefore considers that the Australian Government should fund the core digital identity ecosystem; charges to state governments should be minimal; and the charging model should be volume-based but have a mechanism for predictable costs and provide incentives for private sector adoption (eg. 'free' tier for small consumers).

Liability

8D) What other best practice mechanisms and processes should be considered to support Users when things go wrong?

The provision of support to victims of cyber crime and identity theft is strongly supported. Protections should be included to prevent identity theft, such as recent fraudulent claims for early release of superannuation, or abuse from those given authority to act on another person's behalf.

The interaction with the new *National Plan to Combat Cybercrime* may also need to be considered where relevant in designing the final legislation and operating environment, including any proposed changes to legislation arising from that plan.

The roles, responsibility and liability for support arrangements need to be clearly defined.

Privacy

9A) Should the proposed privacy and consumer protections listed above be enshrined in primary legislation?

Inclusion of the privacy protections in the primary legislation is supported, particularly the prohibition on commercialisation of data, profiling of users, or the creation and use of a single identifier.

The legislation needs to clearly articulate what would be classed as a 'single identifier'. In section 4.4.1 of the consultation paper, it is stated that "an identity exchange must create a different identifier for each relying party". If a state government broker/ exchange uses the TDIF exchange, it needs to be clear whether they are also required to use this model. If so, this may break or greatly complicate content and attributable sharing options across state government departments, even if the user agrees to it. Further, there is a use case where an individual may want to link separate identities in the system eg. to transition or consolidate their accounts.

Choice

10A) Should the Legislation include rules around the extent of choice available to Users to verify their identity?

The legislation should stipulate that individual users be allowed to use alternative methods to verify their identity. Some individuals will have difficulty using digital identification. This may include individuals who:

- Are not technologically literate,
- Have communication issues, which may include language barriers or disability
- Do not have access to a phone or computer, or do not have private access
- Cannot afford to purchase the latest technology (for example, myGovID is not accessible using some older operating systems).

There is a risk that digital identity will only be available to those members of the community who can afford to purchase the latest technology. The Tasmanian *Premier's Economic and Social Recovery Advisory Council Interim Report July 2020* found that Tasmania performs poorly on all three measures of digital inclusion – accessibility, affordability and overall ability to use digital technology for work, study and day-to-day access to essential services.

Relying parties who fail to provide alternative identification options may exclude some users from their service. This issue is less about choice and more about rights and accessibility.

The Board supports legislative and regulatory parameters that enable widespread accessibility to digital identity, and allow users to authenticate their identity through other means if digital identity systems are inaccessible. Ideally, users should never feel forced into creating a digital identity purely to access a particular program or service.

Digital identification systems should be developed with the aim of ensuring accessibility for a broad range of users. Systems should be easy to understand and access, using a range of devices. Consideration should be given to the accessibility requirements for people who only have access to shared technology, such as library computers or the family phone.

10B) Should any types, or all types of relying parties be obliged to provide an alternative identity verification mechanism, and what exceptions should be available?

While noting potential challenges for smaller public and private sector operations, the Board considers that guiding principles to support the legislation should strongly encourage the provision of alternate verification mechanisms. This is especially so for governments, and organisations funded to provide services on behalf of governments (funded service providers), as well as providers of emergency assistance and essential services.

Restrictions on data profiling

11A) What types of profiling of behavioural information should be prohibited and allowed?

The Board supports the legislation prohibiting profiling or having third parties building up a dataset to on-sell for marketing purposes. The user experience design focus is also supported, so users only have to provide the information once.

11B) Should a public register of Attributes be maintained?

The proposed 'Digital Identity Participant Register' is supported as it will assist in building trust with the public regarding the Digital Identity system.

11C) Should there be additional restrictions on access to Restricted Attributes?

The Board considers that the relying party application should also give consideration to how consent of the user is being managed for the Restricted Attributes.

Biometrics

12A) Are there any other safeguards on Biometric Information that should be included in the Legislation?

The discussion paper places an emphasis on consent and holding of personal data only for the purpose intended and minimal length of time for the service to be effected. The deletion of biometric information needs to be very clear and workable and set clear expectations, roles, responsibilities, timeframes and penalties. This should include consideration of whether the user should be able to have their biometric information deleted from all parties systems (IdPs, credential providers, relying parties' systems) through the one request.

12B) Are there any that have been proposed above that should be modified or excluded, and if so, why?

Consideration should be given to information access for policing/investigation to the extent that proposed safeguards do not result in a reduced ability to detect and apprehend people who misuse the system. Provisions should allow for law enforcement access to this data in response to complaints about misuse.

13A) Do you agree with the proposed approach for Biometric Information?

The Board agrees that Biometric Information should only be used for 'one to one' matching.

13B) Will the limitations on Biometric Information overly constrain innovation or rule out legitimate future use cases?

The limitations should not impede the ability of authorities to detect, apprehend and prevent misuse, fraud and criminal use of the system.

Consent

14A) Should the legislation specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party?

Yes, consent is regarded as a key principle and must be enshrined within the proposed legislation.

14B) Should the Legislation specifically provide an opt-out mechanism enabling individuals to opt out of the system after they have created a Digital Identity?

The inclusion of an opt-out mechanism is strongly supported. This is important to ensure safety of users, but also to increase trust in the system.

A person should be able to withdraw their consent and understand the implications of doing so. There should be a clear mechanism for reclaiming or establishing a new identity when there has, or there is perceived to have, been a security breach of the identity or the credentials used to establish it.

The proposed 'opt out and disable' provision should be replaced with an 'opt out and remove' provision (consistent with GDPR provisions).

Age

15) Should there be a minimum age set for a person to be permitted to create their own Digital Identity? If so, what should it be?

Given the wide range of possible uses for Digital Identity and thresholds in different systems and legislation, the Board considers the matter of age is best addressed in guiding principles, not legislation.

Acting on behalf of another

16) How should the Legislation cover situations where a person lacks capacity, is not capable, is too young or lacks interest or motivation to engage personally with the system?

It will be important to ensure there is a mechanism for resolving issues around digital identity creation and usage in situations where another person has authority to act on someone else's behalf (eg power of attorney situations).

Children, elders and persons living with disability may require assistance to use digital identification, or may need someone to undertake activities on their behalf. It is critical that processes are in place to ensure that vulnerable people are not exploited, or that identity is not stolen as a result of proxy arrangements.

The determination of capacity will require careful consideration. The National Disability Insurance Agency (NDIA) considers that all people have decision-making capacity until proven otherwise. However this does not necessarily equate with the capacity to use a digital identification system.

It would be advantageous to use consistent definitions when referring to the process of acting on behalf of another person. The National Disability Insurance Scheme (NDIS) uses the term 'nominee' where a person is appointed to act on behalf of, or make decisions on behalf of a participant. The National Disability Insurance Scheme (Nominees) Rules 2013 defines the roles and responsibilities of Nominees.

The NDIA and Tasmanian Guardianship and Administration Board websites suggest that most adults with disability do not need a formal guardian or financial manager, but have a family member or friend help them to make decisions and undertake actions. Guardians are infrequently used and tend to make significant decisions, such as over the sale of a house, or a disputed care plan. Rules around appointing a nominee must acknowledge the role of unpaid family carers while also protecting the rights of the individual. A nominee may need to have multiple accounts on one device.

The issues for children and young people should be considered in conjunction with discussion at 4.7 around age. Some children and young people may lack interest or motivation to be engaged with digital

identity, in which case their parent or guardian would generally be able to access services on their behalf and separate digital identification of the child would not be required.

The legislation should clearly articulate:

- What actions a nominee can undertake, including their duty to consult with the participant.
- What documents or evidence will be required to appoint or nominate another party to undertake digital identification on their behalf.
- How nomination can be transferred or cancelled, and the privacy of the user guaranteed, for example if a person with disability decides to change their nominee, or a young person leaves out-of-home-care. An easy-to-access opt-out mechanism will be critical to ensure that nominees can be removed when they no longer have nomination authority.

Legislation should be considerate of jurisdictional legislation, systems and processes.

Privacy Impact Assessments

17) Should the requirement for a PIA remain in the TDIF accreditation requirements or should it be required in the Legislation or Operating Rules?

The Board considers that the requirement for a PIA remain part of the accreditation requirements and, consistent with the consultation paper proposal under section 3.2.1 (p. 11), be included in the Operating Rules.

Human Rights

18) In addition to the right to privacy and anti-discrimination in relation to accessibility and disability, how should the Legislation safeguard and ensure the enjoyment of Australians' human rights?

As noted in response to Question 10A, there is a risk that digital identification will only be available to people who are technologically savvy and have access to the latest technology. The most disadvantaged members of the community may not be able to afford, access or utilise digital identification. The provision of social services must not be preferenced or reserved only to those individuals who can use digital identification.

Accessibility and anti-discrimination

19) Is the proposed approach to accessibility and usability practical and appropriate? Should any other considerations be taken into account?

The system should be inclusive of all users, regardless of their ability and environment. To achieve this, the user journey should be mapped and tested with a wide range of users.

Other specific accessibility considerations should include:

- Use of plain English/ plain language in the Legislation, Operating Rules and related system documentation to support clear messaging and transparency for consumers.
- Ensuring accessibility for people with a range of disability types. At a minimum, the system should meet the latest Web Content Accessibility Guidelines.
- Ensuring that it can be effectively used by people who have slow or sporadic internet connections and regardless of their geographical location.
- How people can access digital identification if they use public or shared technology.

- Accessibility should be tested using a range of platforms and operating systems, including older and cheap technology. Systems should be compatible with older operating systems where possible.

The Australian Government could encourage participants to ensure their sites are accessible by requiring that they meet the Web Content Accessibility Guidelines to be eligible to use digital identification.

Penalties

20) What additional mechanisms, including penalties and redress mechanisms, should be included in the Legislation to prevent disclosure or misuse of personal or other information?

A Compliance register could be developed that identifies any breaches and actions that have been or will be undertaken to ensure that a breach is remedied or is unlikely to happen again. This could be similar to the National Disability Insurance Scheme Quality and Safeguards Commission's NDIS Provider Register, as outlined in the provider register and compliance and enforcement actions.

The Tasmanian Government will give further consideration to appropriate penalties for these types of offences once the detail of the proposed offences is known.

Disclosure of personal information

21) Should the Legislation include provisions to enable the disclosure of information in specified circumstances? If so, what should those circumstances be?

The legislation should complement existing relevant legislation (primarily the *Privacy Act 1988*) and include provisions for the release of information where explicit consent has been provided. The legislation should also allow for disclosure for law enforcement purposes as per the *Privacy Act 1988* and other legislation.

Governance

22A) Are there established independent bodies that could fulfil the role of an independent Oversight Authority for Digital Identity, or is a new independent body required?

The Board supports the establishment of the Oversight Authority as a new, independent, accountable and transparent body. The role of the Oversight Authority will be crucial in ensuring that the legislation is applied effectively and is appropriately enforced, in order to ensure user protections are upheld.

It will be particularly important to ensure appropriate accountability mechanisms are in place, including that its performance and operation is periodically reviewed.

22B) What is the optimal structure of a new body?

As state governments are potentially large users of the national Digital Identity system to enable secure easy access to digital services, the new oversight body should include members from jurisdiction governments and peak bodies to assist in building confidence in the system.

23) What type (or types) of information should be required to be publicly reported by the Oversight Authority, to increase transparency in the system?

While agreeing with the transparency provisions, the accuracy of biometric algorithms is difficult and potentially meaningless to report on alone, as success of verification services is dependent on a number of factors including image quality (for face matching) and accuracy of any biographic data that is used as

part of a verification. Accuracy should be reported on success of services similar to document verification.

Reporting could also include the number of requests made (and by whom) and approved, for access to Restricted Attributes.

24A) What is the appropriate period for review of the governance structure of the Oversight Authority?

The proposal of three years initially, then every five years seems appropriate and reasonable.

25A) Are the roles and functions outlined above appropriate for the Oversight Authority?
The creation and maintenance of a strong Oversight Authority is supported. Customer experience should be one of its key functions, particularly complaints management, user protection and user assistance.

There is a mix of running, providing the service including monitoring and charging for it, combined with investigations including fraud etc. The Board suggests the operating and charging for the service should be separate from, and subject to oversight by, the Oversight Authority.

26A) What other committees or advisory structures do you think may be needed?

The Board considers that the committees and structures must ensure that there is input into the digital identity ecosystem from a broad cross section of the Australian community.

26B) What other organisations or bodies could supply members of the Privacy Advisory Committee?

State governments and key business/ public privacy advocacy groups could have membership to increase public confidence in the system.