TELSTRA CORPORATION LIMITED

Digital Transformation Agency

Digital Identity Legislation - Position Paper

Public submission

14 July 2021

CONTENTS

EXECUTIVE SUMMARY

Telstra welcomes the opportunity to respond to the Digital Transformation Agency's (**DTA's**) Digital Identity (**DI**) Legislation Position Paper.

We appreciate the large amount of work and breadth of thought that has gone into the development of this second phase consultation. On the whole, we consider the position paper addresses most of the key elements required to develop the legislation necessary to establish and manage a Trusted Digital Identity Framework (**TDIF**) for Australia.

Our submission contains a few final thoughts for the DTA's consideration around four themes of: 1) security and safeguards; 2) users, privacy and express consent; 3) liability provisions; and 4) some residual technical and framework matters.

Regarding security and safeguards, we propose that certification for Relying Parties would assist in mitigating the risk of potential fraudulent attempts by malicious actors attempting to set themselves up as Relying Parties for the purpose of obtaining user identities or attributes. We note that this is already partly contemplated in the Position Paper for Relying Parties wishing to access so-called "Restricted Attributes". We also consider the role two-factor and multi-factor authentication might play as an additional security safeguard.

In relation to users, privacy and express consent, we again note the risks associated with (potentially) overlapping legislation in the form of the Privacy Act (currently being reviewed) and bespoke privacy requirements enshrined in the Digital Identity (**DI**) Legislation.

On the theme of liability and redress, we make a few recommendations specifically looking at the possible unintended consequences of the uncapped nature of some of the liability provisions. We use notifiable data breaches and the role of the Oversight Authority (**OA**) as advocate on behalf of victims of identity fraud as examples. We also make a comment on excluding previous civil penalties that are unrelated to conducting an identity services business from the accreditation checks for new participants.

Finally, we make a handful of observations on more technical matters associated with the framework such as some benefits on limiting the scale of the number of Accredited Participants, the Technical Standards Board, a request for public consultation on standards (technical and otherwise), the introduction of timeframes for decisions made by the OA, clarification for Accredited Participants wishing to simultaneously operate outside the TDIF, along with our support for the DTA's decision to exclude the Document Verification Service (**DVS**) and the Face Verification Service (**FVS**) from the DI Legislation.

01 Introduction

Telstra welcomes the opportunity to respond to the Digital Transformation Agency's Digital Identity Legislation Position Paper. We acknowledge and applaud the considerable effort invested by the DTA in the preparation of the Position Paper. Clearly, a lot of thought has gone into its preparation, with aspects of the scheme thoroughly considered from all angles including users, participants, implementation and oversight.

Due to the considerable effort to date, our submission only calls out a final few matters for the DTA's consideration, along the following themes:

- Section 02 contains our thoughts on some additional arrangements that could be introduced to improve overall security of and trust in the scheme, including introducing additional rigor to certify Relying Parties, and security controls such as two-factor and multi-factor authentication;
- Section 03 considers two matters related to Users, privacy and express consent;
- Section 04 contains our concerns about some aspects of the proposed liability aspects of the framework along with comments on consideration of previous civil penalties for applicants applying for accreditation; and
- Section 05 contains our recommendations on a few technical and framework matters.

02 Security and safeguards

Good security and consumer safeguards are fundamental to user trust in the system, and trust is ultimately fundamental to the success of the framework. In this regard, we appreciate the DTA's focus on privacy protections, consumer safeguards and security requirements throughout the Position Paper, as robust obligations in the legislation will serve to build user and participant trust in the system.

Overall, we consider the proposed obligations as described in the Position Paper satisfactory to build this trust, however, we offer some suggestions in the subsections below that if adopted, could further enhance trust in the scheme.

2.1. Certification for Relying Parties

Telstra supports the DTA's proposal to have an Accreditation process for Identity Providers (IDPs), Attribute Service Providers (ASPs), Credential Service Providers (CSPs) and for Identity Exchanges (IDXs). Accreditation will ensure these various service providers meet rigorous standards for privacy and security before they are formally added to the scheme, and we fully support the DTA's proposal to apply this additional level of rigour to providers of the scheme.

We note, however, that a far less rigorous process is used for adding Relying Parties to the scheme, presumably in part, to reduce barriers to participation. Relying parties are only[1] required to meet: 1) the onboarding data and technical rules; 2) a check in relation to national security (as defined in the Criminal

[1] We note that in relation to Restricted Attributes, there is reference made to the Relying Party having to demonstrate that its "*protective security, privacy and fraud control arrangements are effective and working as intended*." (See section 7.4.4, first bullet point at the top of p.51). What we propose in this section of our submission is that a minimum set of basic checks, such as these, should apply to Relying Parties.

Code); and 3) an assessment of whether they are fit and proper persons.[2] Once onboarded, a Relying Party becomes a Participant in the scheme and according to the definitions in Section 2, is able to obtain "*verified Attributes*[3] *or assertions provided by identity providers and attribute service providers to enable the provision of access to a User of a service*."[4]

Given Relying Parties are able to obtain attributes of a User of the scheme, albeit with the User's "*express consent before enabling their authentication to a service*"[5], we propose a higher level of rigor is required for adding Relying Parties to the scheme to reduce the risk of malicious actors becoming Relying Parties in order to obtain User Attributes fraudulently. We envisage this additional rigor could be achieved through a certification that include additional checks on:

- the veracity of the organisation, beyond the nation security/criminal code checks mentioned in section 5.4.4 of the Position Paper, to cut down on scam operators establishing an on-line presence to spoof Users into consenting to transfer of their attributes;
- sighting documented privacy and security policies; and
- evidence of compliance with Australian or international standards for privacy and security in IT systems, data storage and related processes.

We also recommend the DTA should have the ability to periodically audit Relying Parties for proof of correct use of information and for information security practices.

2.2. Trustmark

Telstra welcomes the DTA's intention to introduce one or more trustmarks to be associated with the TDIF. We agree with the DTA that the creation and awarding of trustmarks to accredited participants can give consumers confidence and encourage uptake of the use of a digital identity.

2.3. Two factor and multi-factor authentication

We observe with interest that the Position Paper makes no mention of additional security controls such as two-factor, or multi-factor authentication. While we would not advocate for such requirements to be enshrined in legislation as mandatory for Participants in the system,[6] we do see a place for reference to these requirements in guideline documents that support the scheme. For example, this could be something referenced in a guideline produced by the Technical Standards Board, and should align to existing recognised security standards and frameworks.

We therefore consider it would be helpful if the DTA made statements, perhaps through something like this position paper, to articulate its views on a minimum set of security mechanisms Accredited Participants (IDPs, ASPs, CSPs and IDXs) should be expected to implement in their systems. This would help to ensure that each time a request to verify the identity of a User to a Relying Party is fulfilled, there is a high confidence that the fulfillment is not fraudulent.

---

2 Section 5.4.4, p.20-21, bullet points 1, 2 and 4.

3 According to Section 2, p.3., an **Attribute** is defined as "An item of information or data associated with an individual. Examples of attributes include name, address, date of birth, email address and mobile phone number."

4 Section 2, p.5, definition of "Relying Party".

5 Section 3.5, p.9, fourth bullet point.

6 The reason for not wanting specific measures or technical controls enshrined in legislation is legislation is difficult and slow to amend, and with likely evolution in this space, we would not want to see specific methods enshrined that may be superseded in the future.

03 Users, privacy and express consent

3.1. Potential for overlapping or conflicting Privacy obligations

We observe the Position Paper[7] says "… *the Bill will include privacy safeguards additional to those in the Privacy Act. It is proposed the Information Commissioner will monitor and investigate breaches or suspected breaches of these additional privacy safeguards*." While we support the proposition that the Information Commissioner (aka Privacy Commissioner) will "*monitor and investigate*" matters related to these "*additional privacy safeguards*" such that there is a single point of accountability to ensure consistency in relation to privacy matters, and note that the DTA's proposal is that "*The Legislation is not intended to duplicate or conflict with established principles in existing legislation, for example, the Privacy Act*",[8] we nevertheless express our concern about the creation of privacy obligations in multiple legislative instruments. Extreme care will need to be taken to ensure that the additional privacy safeguards do not conflict with the Australian Privacy Principles (APPs), and that the APPs don't inadvertently create unworkable privacy obligations. For example, APP 2 requires an APP entity to provide individuals the option of not identifying themselves (anonymity) or the option of using a pseudonym. Anonymity is the antithesis of identity, and broadly adopting the APPs as the legislative instrument to apply to Accredited Participants could easily have unintended conflicts if applicability is not clearly defined.

3.2. Continued use of a Digital Identity in an offboarding context

Section 6.6.3 of the Position Paper outlines a proposed procedure to "… ***establish*** *a Digital Identity with another identity provider if their existing identity provider is offboarded from the system*" (emphasis added). Under the proposed process, "*metadata and logs of a User's previous Digital Identity may be linked to their current Digital Identity through a system-run process…*". While the Position Paper does not explicitly require express consent from the individual User(s) concerned, we nonetheless assume that express consent is required before the "transition" of an identity to a new IDP is invoked, and we also assume that the choice of which IDP will be the User's new identity provider will be at the sole discretion of the User.

What concerns us more than the absence of a requirement for express User consent prior to the transition to a new IDP is the assumption that "metadata and logs" alone would be sufficient to (re-)establish a verified identity with a new IDP. Given the express prohibition on sending biometric data through the system, and the assumption that other verifiable items of proof-of-identity (images of passports, drivers licence, medicare card, etc) are similarly unlikely to be transferred through the system as attributes of a User, we are not sure how a verified identity could be reconstructured purely from metadata and logs alone. We recommend further consideration be given to how this might work in practice.

7 Section 6.4.6 first paragraph, p.38.

8 Section 7.1, middle of p.44.

04 Liability, redress and penalties

4.1. Notifiable data breaches and unlimited liability

We observe section 7.4.15 of the Position Paper[9] says "… *a failure to notify a data breach would count as a breach of system rules, leading to compliance action*." Commensurate with the liability position described elsewhere in the Position Paper, we note that if an Accredited Participant is deemed to have breached the system rules, the Participant would be exposed to unlimited liability. We recommend that if the DTA proceeds as proposed to legislate that a failure to notify a data breach would also count as a bread of the system rules, then this coupling to the NDB scheme should be limited to data breaches of which an Accredited Participant is aware, to avoid exposing Accredited Participants to liability for events of which they have no knowledge or visibility.

4.2. Liability

As we will outline further along in our submission (section 5.2), online identity systems are a target for malicious actors due to the high value of (stolen) personal information. Due to the high risk that any identity system will be a target for malicious actors, we consider the following broad principles should be adopted for the creation of the DI Legislation:

- The benefits of the framework will be shared by Users, Participants (both Accredited and unaccredited Relying Parties) and by Government. Hence, we consider the downside risks should also be shared, meaning all participants and Government should bear some liability.
- Accredited Participants should not bear unlimited liability for loss and damage flowing from their non-compliances – liability for such losses and damage should be capped from the outset as part of the statutory contract.
- Regarding section 9.4.3, the Commonwealth should bear some liability for its participation in the framework. Its employees should not be immune from liability: they would be covered by the Legal Services Directions, which provide for the Commonwealth to give or fund legal assistance to an employee who has acted, or is alleged to have acted, negligently, i.e. failed to exercise the legal standard of 'reasonable care' owed in the circumstances, unless the employee's conduct involved serious or wilful misconduct or culpable negligence.

4.3. Redress

We previously expressed our concern to the DTA that where a User of the system is a victim of a cyber security incident resulting in the user suffering a loss, redress between the Participant and the User will be difficult where there is no direct relationship between the User and the Participant, as would be the case for an Identity Exchange (IDX). We thank the DTA for taking our concern into consideration and for ascribing a new role[10] to the Oversight Authority (OA) to advocate on behalf of Users (individuals) who are victims of identity fraud. We understand this advocacy will involve the OA acting as intermediary between the User and Participant, and may include facilitating the establishment of a relationship between the parties to give affect to the redress.

While we thank the DTA for taking our earlier concern into consideration, we have concerns with the way 'advocacy' has been expressed in the Position Paper. Specifically:

---

9 Second last paragraph on p.56.

10 Section 9.4.4, p.62.

- Section 9.4.4 states that the OA will "… *advocate on behalf of individuals who are victims of identity fraud*." We are interested to understand what "advocate" involves in this context. For example, would the OA pursue and prosecute Accredited Participants? In case of dispute, we query whether the OA should take one participant's side against another.
- We are also concerned that an obligation on Accredited Participants to "*provide support services for business and individuals affected by identity theft and cyber security incidents*" could lead to Accredited Participants incurring significant costs, given the large number of businesses and individuals who could be affected by even one such incident.

We recommend there should be some tightening of the obligations, both on the OA and on Participants (both Accredited and unaccredited) in relation to the requirements outlined in section 9.4.4, to prevent an undue burden of risk and expense being applied to Participants in the system. Uncapped liabilities and open-ended obligations are likely to be a disincentive to participation in the scheme.

4.4. Accreditation and previous civil penalty orders

In relation to accreditation of participants, section 5.4.3 of the Position Paper notes the Oversight Authority will accredit applicants where it is satisfied of matters such as whether the applicant is a "fit and proper person", including whether the applicant has any criminal convictions or civil penalty orders. While we understand the purpose of this position, we are concerned that consideration of previous civil penalty orders may adversely affect applications from large, multifaceted businesses wishing to operate in the identity provision space. Multifaceted businesses may be required to pay civil penalties for breaches of codes or legislation in one part of their business, which are unlikely to affect their ability to provide identity services safely and effectively.

We propose that any consideration of previous civil penalties as part of accreditation should be limited to considering whether the previous civil penalties would adversely affect the applicant's ability to undertake the role for which it is seeking accreditation.

05 Technical and Framework matters

5.1. A pragmatic limit on scale is required

We observe that the Position Paper places no limits on the number of IDPs, ASPs, CSPs or IDXs (Accredited Participants) that can be involved in the scheme. While this may be attractive from the perspective of consumer choice, and from the perspective of avoiding a rush to join the scheme to prevent missing an arbitrary cut-off on the number of Accredited Participants, we remain concerned that no limit potentially creates unnecessary scaling challenges for participants (especially Relying Parties), should the number of IDPs, ASPs, CSPs or IDXs grow too large.

We observe from Figures 5, 6, 7 and 8 in the Position Paper that Relying Parties only connect to IDXs, and not directly to any of the IDPs, ASPs or CSPs. While this does effectively limit the number of *physical* connections (each Relying Party need only have a connection to each IDX), the number of *logical* connections (relationships) remains a function of the number of IDPs, ASPs and CSPs. We readily acknowledge the role that standards will play in ensuring a level of consistency in the various attributes, credentials and other information that flows from IDPs, ASPs and CSPs to Relying Parties, but even so, there will be nuances permitted within the formats allowed by the standards. What this means in practice is that every Relying Party will need to conduct interoperability testing *with each* IDP, ASP and CSP through the onboarding process. Simply running a standard suite of "bench tests" (tests conducted in an off-line environment) with some default identities will not be sufficient to ensure the

reliable and robust transfer of personal information of the nature dealt with by the TDIF; real-world testing will be required. Further, each time a new IDP, ASP or CSP is added, all existing Relying Parties will be required to conduct a full suite of tests with the new service provider, again to ensure the reliable and robust transfer of personal information.

Restricted Attributes are a case in point. Section 7.4.4 of the Position Paper contemplates an array of possible Restricted Attributes including information classified as sensitive information under the Privacy Act, healthcare identifiers, other matters the Minister considers relevant, etc. If a new healthcare ASP is added to the framework, it will be just as important to test the correct flow of attributes to authorised third parties as it is to test that requests for Restricted Attributes about an individual from a Relying Party not authorised to obtain such information are blocked by the system.

We agree with and support the Interoperability Principle[11], as we consider this principle facilitates the greatest consumer choice, which in turn will build participation in the scheme. We consider that the Interoperability Principle should not be compromised as a possible solution to the scaling problem, and yet, to solve the scaling problem, some limit is required to prevent the potential burden on Relying Parties.

The Position Paper notes the Minister will be given the power to issue Technical Standards[12], and we recommend these will need to be very tight to ensure interoperability between all participants (both Accredited and unaccredited) of the TDIF. Regardless of any limits imposed on the number of Accredited participants (as described in this section), the framework will nevertheless quickly become unwieldy and potentially unworkable if there are too many variations in the information, or formats of the information, permissible within the framework.

5.2. Limiting scale also reduces the 'attack surface'

A further point on limiting the number of Accredited Participants[13] relates to cybersecurity benefits arising from reducing the attack surface.[14] Online identity systems are a target for malicious actors due to the high value of (stolen) personal information, and increasing the number of participants in a meshed network creates more openings for malicious actors to target.

We acknowledge cybersecurity is a foremost consideration of both the TDIF and the DI Legislation, nevertheless, maintaining a secure environment becomes increasingly difficult as the attack surface increases. While restricting the number of Accredited Participants is not a guarantee of a risk-free environment, increasing the number of participants does increase the risk.

5.3. Technical Standards Board

We agree with and support the creation of various advisory groups, including a Technical Standards Board. We agree with and support the approach outlined in Section 6.4.2 of the Position Paper, which proposes that the board should in part be made up from entities participating in the scheme. We consider it very important that industry representation is included on any Technical Standards Board(s).

---

11 Section 5.4.6, bottom of p.22. The Interoperability Principle only applies to Relying Parties, and requires them to accept a DI from any IDP listed on the Participant Register.

12 Section 3.4, top of p.9.

13 We consider there should be no limit on Relying Parties. The Position Paper's definition of Accredited Participants only includes IDPs, ASPs, CSPs and IDXs.

14 See https://en.wikipedia.org/wiki/Attack_surface for a definition.

Timelines on when reviews and updates are to occur should be legistated to ensure currency and compliance.

5.4. Public consultation on standards.

We observe section 3.4 of the Position Paper proposes 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*." and that specifications will be Notifiable Instruments.[15] While clearly it is the intent of the Position Paper[16] that the Technical Standards Board is intended to develop and write the standards, we are concerned that such instruments will only be notifiable, thereby not affording the opportunity for public consultation. Given such standards are likely to take multiple months to develop, we consider it would be appropriate for public consultation on a final draft of any such standards or rules to be added as part of the process of developing the standards ahead of the Minister making the instrument. This would afford the opportunity for potentially affected parties who are not party to the various advisory boards to comment.

5.5. Timeframes for Oversight Authority Decisions

Section 6.4.5 of the Position Paper lists the various functions of the Oversight Authority, including functions such as Accreditation, suspending or terminating Participant's use of, or participation in, the system, etc. Where appropriate to the function, we consider it would be helpful for the DI Legislation to set out expected timeframes for both the Oversight Authority (e.g., time to assess and approve an application) as well as timeframes for Participants (e.g., to appeal a suspension or termination decision).

5.6. Accredited Participants wishing to simultaneously operate outside the TDIF

The Communications Alliance submission to this consultation contains a section on Accredited Participants wishing to simultaneously operate outside the TDIF. We agree with the observations raised by Communications Alliance, and support their request to clearly explain in the legislation how two Accredited Participants might simultaneously conduct transactions either inside the system (captured under the legislation) and outside the system, including articulating the "delineation" that is required to demonstrate which transactions are inside, and which transactions are outside the system.

5.7. DVS and FVS should not be covered by the DI Legislation

The Position Paper notes in section 5.3 that the Document Verification Service (DVS) and Face Verification Service (FVS) will not be covered by the Digital Identity (DI) Legislation. The DTA's rationale for this is that these services are key inputs for identity providers to verify attributes of a User creating a Digital Identity. We agree with this assessment, and consider that it is more appropriate for these services to be captured under a set of standards, preferably aligned to international standards where possible, rather than being captured as part of the DI legislation. The use of standards, and possibly a legislative instrument that is independent of the DI legislation will enable the DVS and FVS to more readily evolve with technology.

---

15 Section 4, top of p.13 where it says rules and specifications will be notifiable instruments.

16 Section 6.4.2, p.34 second bullet point and also last paragraph on p.34.