Electronic Frontiers
AUSTRALIA

w www.efa.org.au
e email@efa.org.au
@efa_oz

12 July 2021

Mr Jonathon Thorpe
General Manager - Digital Identity
Digital Transformation Agency
Level 3, 50 Marcus Clarke Street
CANBERRA ACT 2600

By eLodgement

Dear Mr Thorpe

RE: PUBLIC CONSULTATION ON AUSTRALIA'S DIGITAL IDENTITY LEGISLATION

Electronic Frontiers Australia ("**EFA**") appreciates the opportunity to provide this submission in relation to the Digital Identity Consultation ("**the Consultation Paper**"). EFA's submission is contained in the following pages.

Established in January 1994, EFA is a national, membership-based non-profit organisation representing Internet users concerned with digital freedoms and rights. EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context. EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of digital communications systems.

As you may be aware, the writer has been involved with consultation with the Digital Transformation Agency ("**the DTA**") since its inception as regards to the digital identity framework. These submissions are intended to supplement comments and opinions expressed in each of the prior consultations.

We trust that these submissions are of assistance.

Yours sincerely,

Angus Murray
Chair of the Policy Committee of
Electronic Frontiers Australia

List of Recommendations

Recommendation One: The Digital Identity System should be abandoned until the introduction of an enforceable federal human rights framework and a tort for serious invasions of privacy.

Recommendation Two: The definition of 'Identity' ought to be provided in the Legislation as a narrow and exhaustive concept incapable of wider interpretation.

Recommendation Three: A person ought to be able to:

1. **By default, opt out of the creation of a digital identity;**
2. **Alter or amend their digital identity; and**
3. **At any stage, require that their digital identity be deleted (in a similar manner to the "right to be forgotten").**

Recommendation Four: The Oversight Authority and its Advisory Boards ought to be responsible for the integrity of the system rather than the utility of the system.

Recommendation Five: The administration, including the staffing, of the Oversight Authority ought to be included in the Legislation.

Recommendation Six: The Legislation does not include provisions for automated decision making and any such proposal be the subject of further consultation prior to introduction of a Bill.

Recommendation Seven: The Legislation ought to include provisions where a Participant will be "offboarded" as a consequence of an adverse finding of the Information Commissioner and where the Participant is found to have offended any 'privacy law' where that term is defined broadly to include any statutory or common law obligation.

Recommendation Eight: Any standard or rules for the issuance of 'trustmarks' be made publicly available for consultation prior to their being submitted to the Australia Consumer and Competition Commission

Recommendation Nine: Accredited Participants ought to be subject to strict liability for compliance with the rules and requirements relating to accreditation and the system.

Submissions

We have adopted the abbreviations contained within the Consultation Paper for convenience alone and the adoption of the DTA's key areas ought to be understood in the context of EFA's longstanding and broad submission that Australians ought to be afforded a base-line safeguard of their rights and freedoms by the introduction of an enforceable federal human rights framework and a tort for serious invasions of privacy.

In this context, it is our overarching submission that the TDIF and the Legislation should be abandoned until an enforceable federal human rights framework and a tort for serious invasions of privacy is introduced into Australian law.

Recommendation One: The Digital Identity System should be abandoned until the introduction of an enforceable federal human rights framework and a tort for serious invasions of privacy

While we appreciate the DTA's intention with respect to the benevolent use of digital identity in Australia, it ought to be trite that such a system could be prone to future abuse and, in our view, that potential for abuse would be significantly reduced with the attitudinal and actual protection of human rights that would arise from the DTA directly recommending and endorsing that the Digital Identity Framework occur in tandem with the introduction of an enforceable federal human rights framework and a tort for serious invasions of privacy.

If the submission that the system should be abandoned until the introduction of an enforceable federal human rights framework and a tort for serious invasions of privacy is not accepted, we submit that there are general issues with the current regime that require remediation.

At the outset, it is clear that there is an important interaction between the Legislation and the TDIF Rules. Although this is structurally important, it imports certain concepts into the Legislation which is, in our view, inappropriate. Most operatively is the definition of "identity" contained within the Glossary of Abbreviations and Terms (Release 4, Version 1.3) of the Trusted Digital Identity Framework ("**the Glossary**") which provides that:

> ***Identity*** *(ID). (a) information about a specific Individual in the form of one or more attributes that allow the Individual to be sufficiently distinguished within a particular context; (b) a set of the Attributes about a Person that uniquely describes that Person within a given context*.

The Glossary relevantly defines "Attributes" as follows:

> *An item of information or data associated with a subject. Examples of attributes include information such as name, address, date of birth, email address, mobile number, etc.*

There is no definition provided for "a subject" and we assume that that reference is a reference to a "person" or an "individual". In any event, we consider that this definition is unacceptably broad. At present, the wide and non-exhaustive definition of 'identity' could be used to

aggregate information about an individual including their creditworthiness, political or religious views and beliefs, medical and health status, sexual orientation, etc.

In our submission, it is critically important that legislation is a strict enactment of the intent of Parliament that is inherently safeguarded against scope creep. In this regard, the definition of "identity" is manifestly broader than it ought to be in the context of the description of the digital identity system. That description is reproduced from the Consultation Paper as follows:

> *The Digital Identity system is a simple, safe and secure way for Australians to verify their identity online. With millions of people already using Digital Identity to access over 75 government services, Digital Identity is transforming the way Australians and Australian businesses engage with government services. The Australian Government is committed to rolling out a whole-of-economy Digital Identity system to:*
>
> - *enable Australians to prove who they are online and reduce the administrative burden for small and medium businesses, so they can get on with doing business.*
> - *support an increased number of Australians to transact end-to-end digitally, improve privacy and accessibility, and reduce fraud.*
> - *enable innovative digital sectors of the economy to flourish.*

In our submission, there is no reasonable basis (other than where a covert attempt to introduce a broader system than necessary exists) to extend the definition of "identity". In this context, we accept the intention seemingly expressed in Section 7.4.4 as regards to 'restricted attributes'; however, we do not accept that ambiguous restrictions on the prescription of attributes are an adequate safeguard against scope creep. It is our submission that this system has the potential for abuse and the definition of identity ought to be drafted in a clear and narrow manner to avoid potential scope creep that would serve only to amplify the potential for abuse and harm.

Recommendation Two: The definition of 'Identity' (including the definition for 'attribute') ought to be provided in the Legislation as a narrow and exhaustive concept incapable of wider interpretation.

It is apparent that digital identity will be generated by the Accredited Participant and; while we understand that this is likely the easiest approach for the system to operate, we consider that safeguards ought to be put in place surrounding the generation of digital identity. Specifically, we submit that a person ought to be able to:

1. By default, opt out of the creation of a digital identity;
2. Alter or amend their digital identity; and
3. At any stage, require that their digital identity be deleted (in a similar manner to the "right to be forgotten").

Recommendation Three: A person ought to be able to:

4. **By default, opt out of the creation of a digital identity;**

5. **Alter or amend their digital identity; and**
6. **At any stage, require that their digital identity be deleted (in a similar manner to the "right to be forgotten").**

In relation to the oversight of the system, we agree that a "double check" comprising an Oversight Authority composed of privacy and consumer advocates, Privacy Commissioners, technical advisors and experts is appropriate. However, this authority should not include private secretary participants. Namely, we agree with the structural flow chart depicted at Figure 10 as contained within the Consultation Paper; however, that flowchart ought to remove "private sector participants" from the Oversight Authority. We make this submission because the Oversight Authority and its Advisory Boards ought to be responsible for the integrity of the system rather than the utility of the system. In our view, questions of utility best arise in the context of applications for accreditation as an accredited provider rather than oversight of the system.

Recommendation Four: The Oversight Authority and its Advisory Boards ought to be responsible for the integrity of the system rather than the utility of the system.

Furthermore, we respectfully do not accept that it is appropriate for the DTA to make a recommendation to the Government regarding the appropriate portfolio from which staffing can be obtained for the Oversight Authority after the Legislation is proposed. In our submission, trust, transparency and accountability are fundamental to a digital identity system in Australia and the details of the responsible person(s) and portfolios for the oversight of the system ought to be known prior to its introduction.

Recommendation Five: The administration, including the staffing, of the Oversight Authority ought to be included in the Legislation.

In relation to oversight by the Information Commission, we agree that this is a sensible approach outline in the Consultation Paper; however, we reiterate the need for an enforceable framework that empowers individuals to take action directly against the responsible Minister and any Accredited Provider that, directly or indirectly, causes harm to an individual. We submit that this relief would be appropriately founded in an enforceable human rights framework and a tort for serious invasions of privacy.

Notwithstanding the need for an enforceable human rights framework and a tort for serious invasions of privacy mentioned above, we agree that the Administrative Appeals Tribunal is the appropriate forum for first instance external merits review of decisions made by the Oversight Authority as articulated at page 39 of the Consultation Paper. However, we do not accept that the section regarding Automated Decision Making (Section 6.5.3 of the Consultation Paper) has been expressed in sufficiently clear terms to be considered at this stage. There are complex legal and administrative issues arising from the use of automated decision making[1] and this ought to be the subject of further and fuller consultation.

[1] See for example: Murray, A. (2019). *Legal technology: Computer says no ...but then what*? The Proctor, 39(8), 48–49.

Recommendation Six: The Legislation does not include provisions for automated decision making and any such proposal be the subject of further consultation prior to introduction of a Bill.

In relation to participation with the digital identity system, we agree with the circumstances where participants may be "offboarded" from the digital identity system; however, we submit that this list should also include circumstances where the Information Commissioner makes adverse findings against that participant or has offended any 'privacy law' where that term is defined broadly to include any statutory or common law obligation.

Recommendation Seven: The Legislation ought to include provisions where a Participant will be "offboarded" as a consequence of an adverse finding of the Information Commissioner and where the Participant is found to have offended any 'privacy law' where that term is defined broadly to include any statutory or common law obligation.

We also submit that the offboarding arrangements should also clearly inplay with the revocation of Trustmarks. In this regard, we understand that the Consultation Paper effectively suggests that the Legislation will provide for the registration of certification trade marks with rules that will govern their license and use. We welcome this approach; however, we reserve comment regarding the same until further information is provided. In this regard, we recommend that any standard or rules for the issuance of 'trustmarks' be made publicly available for consultation prior to their being submitted to the Australia Consumer and Competition Commission.

Recommendation Eight: Any standard or rules for the issuance of 'trustmarks' be made publicly available for consultation prior to their being submitted to the Australia Consumer and Competition Commission

In this context of trust, we appreciate and agree that a non-financial means to redress borne by a Participant including providing assistance with re-establishing a stolen digital identity is appropriate. However, we do not accept that a Participant's financial liability should be limited to circumstances where they have acted in good faith and are in compliance with the legislative rules and requirements relating to accreditation and the system. In our submission, the harm that may be suffered by the individuals using the scheme has the potential to be serious and longstanding and the accreditation ought to impose strict liability.

Recommendation Nine: Accredited Participants ought to be subject to strict liability for compliance with the rules and requirements relating to accreditation and the system

We trust that these submissions are of assistance and please do not hesitate to contact us should you require any further information or assistance.