

SUBMISSION

Australia's Draft Digital Identity Legislation

October 2021



Disclaimer and Copyright

While the DLA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

© The Digital Law Association (DLA)

This work is licensed under the Creative Commons Attribution 2.0 Australian Licence.

(CC BY 3.0). This licence allows you to copy, distribute and adapt this work, provided you attribute the work and do not suggest that the DLA endorses you or your work. To view a full copy of the terms of this licence, visit

<https://creativecommons.org/licences/by/3.0/au/>

Contents

ABOUT THIS SUBMISSION	3
1 Bill of Digital Rights and Freedoms.....	5
2 Narrow application and interpretation.....	10
3 Law Enforcement and Privacy: Judicial oversight	13
4 Law Enforcement and Privacy: Digital Identity System Design.....	14
5 Data profiling.....	15
6 Accessibility for Australians abroad	15
7 Innovating alongside best practice – self sovereign identity	17
8 Global and technical interoperability.....	18

ABOUT THIS SUBMISSION

The Digital Law Association is an organisation dedicated to the promotion of a fairer, more inclusive, and democratic voice at the intersection of law, policy and technology.

Our mission is to encourage leadership, innovation, and diversity in the areas of technology and law by:

- bringing together the brightest legal minds in the profession and in academia to collaborate; and
- developing a network that promotes digital law, and particularly female leaders in digital law.

This document was created by the Digital Law Association in consultation with its members. In particular, the compilation of this submission was led by:

- Joni Pirovich
- Susannah Wilkinson
- Amiinah Dulull

This submission has been contributed to by the following Digital Law Association members:

- | | |
|---------------------------|---------------------|
| ➤ Sarah Jacobson | ➤ Christine Bulos |
| ➤ Stephen Alexander | ➤ Jenny Ng |
| ➤ Andrew Dahdal | ➤ Natasha Blycha |
| ➤ Heather Delfs | ➤ Andrew Collins |
| ➤ Dawn Raides (pseudonym) | ➤ Rose MacDonald |
| ➤ Uchenna Anyamele | ➤ Andrew Collins |
| ➤ Mel Karibasic | ➤ Laurence White |
| ➤ Sean Tran | ➤ Eloise L'Estrange |

Submission Process

In developing this submission, our members have engaged through email correspondence, video calls, and worked in teams to conduct research and prepare briefing papers about the issues raised by the proposed digital identity legislation. The consultation window of one month was incredibly short for such significant legislation and we thank our volunteers for their incredible and intensive contribution to this submission.

Recommendations

Recommendation #1	<i>Digital identity is the cornerstone of the digital economy and any legislation enabling a digital identity system should be broad enough to safely unlock the benefits of the digital economy but with rights and freedoms protected in a bill of digital rights and freedoms.</i>
Recommendation #2	<i>If our Recommendation #1 will not be considered by the Minister or will be commenced as an ongoing piece of work, the Bill be written to allow for an application as narrow as possible, rather than a wide application (which should only be facilitated by consulting with all relevant stakeholders throughout the consultation process).</i>
Recommendation #3	<i>That the Bill incorporates independent and (preferably) judicial oversight over the disclosure of information to enforcement bodies under section 81 and that any accredited entity that acts upon the recommendation or decision of an oversight body in relation to section 81 not be liable for a civil penalty under such provision.</i>
Recommendation #4	<i>That the system in which digital identity information is collected, used and disclosed is designed in a way that assures a person's privacy is protected and safeguarded. These systems should be designed with data stewardship principles in mind, and with the benefit of latest review process on identification of ethical issues with technology design.</i>
Recommendation #5	<i>That section 80 of the Bill provides for safeguards against the dangers of data profiling.</i>
Recommendation #6	<i>That the proposed expansion of the TDIF for the purpose of enhancing accessibility of Australian government and private sector online services to all Australians include Australians not currently residing in Australia.</i>
Recommendation #7	<i>Revise language and technical requirements in both the proposed legislation and TDIF to allow for the incorporation of SSI services and provide for the fluidity of innovation in technology.</i>
Recommendation #8	<i>The legislation should provide for integration of provisions to recognise accredited providers in third party jurisdictions.</i>

1 Bill of Digital Rights and Freedoms

Recommendation #1

Digital identity is the cornerstone of the digital economy and any legislation enabling a digital identity system should be broad enough to safely unlock the benefits of the digital economy but with rights and freedoms protected in a bill of digital rights and freedoms.

Reasons for a Bill of Digital Rights and Freedoms for Australians

The design and introduction of a Bill of Digital Rights and Freedoms for Australians is strongly recommended before the draft digital identity legislation is introduced. Digital identity is the cornerstone, not just of national digital economies but of the global digital economy. If introduced in its current form to address a narrow utility of digital identity to access government services, the digital identity legislation would miss the context, requisite interoperability and flexibility needed to ensure the initial and ongoing protection of rights and freedoms of Australians in the digital economy as well as support the diverse participation of all Australians that choose to participate in the digital economy.

To repeat the Digital Law Association's recommendation in response to the third issues paper of the Australia as a Technology and Financial Centre Senate Inquiry, proper economic modelling should be commissioned by the government to assess the economic benefits that can be captured from digital assets, digital identity and the digital economy. Without due consideration of the rights and freedoms that require protection in the digital economy and without more holistic consideration of how Australians can and will engage in the global digital economy, the economic modelling used to justify introduction of digital identity legislation has not taken into account the full potential of the digital economy or the costs of not designing a flexible, holistic, inclusive and ethical digital identity system.

Foundational legislation of this significance must take account of the long term impacts on people's willingness to interact voluntarily with, and safely in, the digital economy. As we saw with the COVID Safe app, poorly designed digital systems do not achieve desired outcomes nor have longevity.

What is being built and done, let alone what is possible in the near to medium term, in the digital economy has already exceeded the limits of our existing national laws and regulations as demonstrated by some of the recent digital asset policy consultations. Any legislation in respect of digital identity should be adequate to accommodate for the impact of emerging technology and associated shifts in business and human behaviour in the digital economy.

The twelve digital asset policy recommendations recently handed down in a report by Senator Andrew Bragg (**Bragg Report**) exemplify the pace and breadth of change due to emerging technologies and the global digital economy. The key pillar missing from the Bragg Report is digital identity. The same key pillar was missing from the UK Law Commission's recent consultation on digital assets. The transformational impact of blockchain technology, as well as its transparency and security, has surpassed the hype stage and is well recognised as a technology that could form the basis of critical global digital infrastructure.

Where ownership of digital (cryptographic) assets can only be proven by reference to who controls the private key, and no existing national law requires an entity or person to maintain a register of holders of private keys for each digital (cryptographic) asset, there is a genuine opportunity for digital assets to be connected to a person's digital identity and for there to be

broader options of digital identity management than is currently contemplated by the proposed legislation.

With this background, we stress that the proposed digital identity legislation will “date” quickly and will become a highly controversial piece of legislation to amend. If rights and freedoms to be protected in the digital economy are not properly considered and included in the legislative framework at this crucial point, Australians are at risk of being left behind – not better served – and unable to initially or continually capture the economic benefits of the global digital economy.

Ensuring a safe, thriving digital economy that is also diverse and inclusive

The draft digital identity legislation is focussed on solving the narrow problem statement that the Digital Transformation Agency (DTA) and the Honourable Stuart Robert MP (**Minister**) have posed for the design of Australia’s digital identity legislation – that is, a safe, secure and convenient way for Australians to prove their identity online, but (at least initially) to access government services. We acknowledge there has been an effort to enshrine important privacy and consumer protections but efforts to ensure diversity and inclusion of access to digital identity which would in turn ensure that a ‘safe, thriving digital economy’ is also diverse and inclusive are less apparent from the Phase 3 Consultation materials.

Whilst the proposed legislation seeks to enshrine the utility of digital identity it does so without consideration for context or flexibility for evolving identity and technologies, which could further entrench systemic disadvantage, and practices and communities in the digital economy that are not diverse or inclusive. We understand that a Statement of Compatibility is being prepared to assess the proposed digital identity bill’s compatibility with the rights and freedoms recognised in the seven core international human rights treaties which Australia has ratified. However, the absence of this Statement on 1 October 2021 when the Consultation on Phase 3 of Australia’s Digital Identity legislation was opened points to the substantial further work to be undertaken before the bill can in good conscience be introduced to Parliament.

The necessary work of designing a Bill of Digital Rights and Freedoms should be undertaken by the Australian Human Rights Commission (**AHRC**) in consultation with industry, traditionally underrepresented groups in Australia, and digital natives that are at the vanguard of what the global digital economy could look and feel like in the near and medium term. We strongly encourage the Minister to formalise a scope of comprehensive work as soon as possible for the AHRC to develop a Bill of Digital Rights and Freedoms for Australians.

The DTA is to be commended for pioneering the important work of digital identity to this point. Now that the digital identity work is at the stage of being introduced into law, it is appropriate that the scope of work and consultation be extended to include the rights and freedoms that require protection in digital economies. We understand that the DTA has already been consulting with the AHRC in relation to privacy and children and that the increase in scope required to access more traditionally underrepresented groups of Australians should be led by the AHRC.

Emerging technologies and approaches

There are various types of identity management in the digital world, consisting of centralised identities, user-oriented identities, federated identities, and self-sovereign identities (**SSI**).¹

¹ Fraunhofer Institute (2021) ‘Self-Sovereign Identity Foundations, Applications, and Potentials of Portable Digital Identities Project Group Business & Information Systems Engineering’ *Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT*, Bayreuth, 9.

Digital identity management systems available are evolving from completely centralised to more decentralised approaches in the pursuit of guaranteeing data protection, portability, and interoperability.² SSI is considered the next evolutionary stage of digital identities.³ Unfortunately, the proposed legislation is not flexible enough to support SSI which will leave Australia behind in the global digital economy.

Under an SSI system, distributed ledger technology can serve to create a permission-less, interoperable, and decentralised digital identity framework.⁴ The user is the administrator of their identity and has much more control over their data and information than others have, know, or share about them. Unlike centralised, third-party, and federative models (i.e., Australia's Digital Identity Framework), the SSI approach does not require an entity for managing people's identity. Neither an identity provider nor a service provider, such as the accredited identity service provider envisioned in the Australian Digital Identity Framework,⁵ is needed to manage one's credentials and authenticators on their behalf. With SSI, an identity provider effectively becomes an identity issuer.⁶

The main benefit of the SSI system includes the facility to enable interoperability between different solutions.⁷ As the cryptographic proofs of ownership are found on a decentralised network, the adoption of SSI protocols and standards would allow for private and public entities to store proofs of information within the same accessible decentralised networks.⁸ With respect to Australia's Framework, it appears that onboarding entities would have to comply with any technical standards issued by the Oversight Authority,⁹ and to date the TDIF requirements have not permitted SSI technology to be "accredited".

SSI models hold the potential to be highly scalable; however, this is also dependant on the implementation of proper trust frameworks, mature and robust decentralised ledgers, and proper regulations.¹⁰ In a federated identity management system, such as Australia's existing (although not enough entities became accredited to fulfil the federated identity system) or proposed system, the low number of identity providers, and their burden to maintain large infrastructures and assume high costs to provide security can render them less reliable and scalable than an SSI system.¹¹

The Federal Republic of Germany, the Kingdom of Spain and Finland have recently partnered with one another to pursue opportunities for collaborating on cross-border digital identity based on SSI, to ensure that all solutions and components of digital identity will meet European standards and reflect European ethical values on Digital sovereignty.¹² Through their partnership, they aim to ensure the sharing of best practices and knowledge (technical, regulatory, operational) in the sphere of digital identity and SSI, and are designing and conceptualising a cross-border pilot to be implemented in 2022.¹³ There have also been other regional efforts to develop public-permissioned regional networks, such as European Blockchain Services Infrastructure in Europe and LACChain in Latin America.¹⁴ This is the

² Lopez, Marco (2020) 'The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain Interamerican' *InterAmerican Development Bank*, 14.

³ Mühle, A; Grüner, A; Gayvoronskaya, T and Meinel, C (2018) 'A survey on essential components of a self-sovereign identity', *Computer Science Review*, 30: 80–86.

⁴ Lim, Jonathan (2020), 'Self-sovereign identity: the harmonising of digital identity solutions through distributed ledger technology' *ANU Journal of Law and Technology* 2(1): 1.

⁵ *Exposure Draft: Trusted Digital Identity Bill 2021*, s 7.3.3.

⁶ Lopez as above, n 2, 21.

⁷ *Ibid*, 98.

⁸ *Ibid*, 46.

⁹ *Exposure Draft: Trusted Digital Identity Bill 2021*, s 36

¹⁰ Lopez as above, n 2, 46.

¹¹ *Ibid*, 18.

¹² See *Declaration for cooperation and exchange of best practices in the field of self-sovereign identity between the Federal Republic of Germany and the Republic of Finland*, signed in duplicate 22 September 2021.

¹³ See *Joint Declaration on cooperation and exchange of best practices in the field of self-sovereign identity between the Federal Republic of Germany and the Kingdom of Spain*, signed in duplicate 29 July 2021.

¹⁴ Lopez as above, n 2, 46.

sort of effort and partnerships that the Digital Law Association encourages the DTA to initiate in conjunction with efforts by the AHRC.

Acknowledgement of traditional owners

We acknowledge the traditional owners of Australia and indigenous jurisprudence where the land is itself a living repository of the law. From this viewpoint (as we understand it) the notion of articulating and indeed listing “human rights” or “digital rights”, including the need to control identity and property and the need to have a static and “universal” application of rights, in the way we have proposed below is entirely unnecessary and wrong. With the one-month time frame for the Phase 3 Consultation, we have not had the opportunity to co-develop the proposed Bill of Digital Rights and Freedoms with our First Nations peoples nor other traditionally underrepresented groups in our diverse, multicultural society. We have sought diversity of views through the collection of Digital Law Association members that have volunteered to contribute to this submission in what has been an incredibly short time frame for such important subject matter.

As the indigenous jurisprudence shows, identity and digital identity is not just a utility – it carries context and meaning from that context. The right to identify myself based on the attributes I say are true, including data that I can treat as my own, has been a concept of emerging significance as jurisdictions around the world including Australia seek to enhance a person’s economic agency and self-determination, enhance privacy protections and put data back in the hands (or digital hands) of its rightful owners.

Illustrative Bill of Digital Rights and Freedoms for Australians

We have set out an Illustrative Bill of Digital Rights and Freedoms for Australians. The Illustrative Bill is intended to catalyse an important and ongoing discussion of the fundamental rights and freedoms Australians can expect as they increasingly experience life online. Appropriate penalties for breach of rights and freedoms in the Bill must be considered and could be mirrored on the GDPR approach. We acknowledge that Australia does not have an existing Bill of Rights but that Australia recognises and protects a number of human rights and freedoms across a range of laws at federal and state and territory levels, the Australian Constitution, and the common law.¹⁵

There are five explicit rights in the Australian Constitution. These are:

- the right to vote (section 41),
- protection against acquisition of property on unjust terms (section 51 (xxxi)),
- the right to a trial by jury (section 80),
- freedom of religion (section 116), and
- prohibition of discrimination on the basis of State of residency (section 117).

The High Court of Australia also determined in 1992 that Australia’s form of parliamentary democracy (grounded in the Constitution) requires a degree of freedom for individuals to discuss and debate political issues. Other rights Australians enjoy are those under the Australian Human Rights Commission Act 1986, the Racial Discrimination Act 1975, the Sex Discrimination Act 1992, the Disability Discrimination Act 1992, and the Age Discrimination Act 1996.

¹⁵ Attorney-General’s Department, ‘Human rights protections’ available at [Human rights protections | Attorney-General’s Department \(ag.gov.au\)](https://www.ag.gov.au/human-rights-protections).

Illustrative draft of a Bill of Digital Rights and Freedoms

1. Right to other rights

All Australians, regardless of physical location, have the right to the same fundamental legal rights in the digital medium as those afforded to them in the analogue environment.

For example: protection of acquisition of property on unjust terms, right to vote, freedom of movement, religion, assembly, expression political issues, freedom from discrimination etc.

2. Right to disconnection

All Australians, regardless of physical location, have the right to be identified and interact with the government in an analogue way.

Note: This right is intended to ensure that people are not excluded from the economy/community who do not use online services, applications or platforms.

3. Right to Digital Access

All Australians, regardless of physical location, have the right to access the digital medium(s) and cannot be excluded from the digital medium(s) on unjust terms.

Note: This right is intended to ensure that people cannot be excluded from the digital economy/digital community, if for example that exclusion has been configured to exert political or economic control unjustly.

4. Right to Digital Identity

All Australians, regardless of physical location, have the right to access and inform their own digital identity.

Note: This right is intended to deal with individuals losing control of their own identity (to the State and to proprietary interests) and 'field style' reductionist identity attributes that do not allow people to express who they are in a way that is culturally open.

5. Right to Data

All Australians, regardless of physical location, have the right to access, curate and control their personal data. This includes the right to erasure.

Note: This would push Australian privacy law closer to GDPR style compliance requirements and would need express legislative change.

6. Right to distinct analogue personhood

All Australians, regardless of physical location, have the right to define their thoughts and actions as separate from their data footprint.

At what point does the switch between evidence of (my conduct) and substantive

identity take place when the law increasingly relies on my digital identity.

2 Narrow application and interpretation

Recommendation #2

If our Recommendation #1 will not be considered by the Minister or will be commenced as an ongoing piece of work, the Bill be written and allow for an application as narrow as possible, rather than a wide application (which should only be facilitated by consulting with all relevant stakeholders throughout the consultation process).

Intended outcomes

- Reduce misapplication of the relevant law (when the Bill is passed) and avoid the inclusion of privacy breaching identifier elements in the future.
- All the views of the relevant stakeholders, underrepresented groups, especially those in relation to privacy and human rights, are taken into account to ensure that the proposed legislation does not encroach on human rights laws and privacy laws or have broader reach that would give rise to unintended consequences.

Prevent wide application of legislation

The form of legislation that is ultimately passed should be construed and written as narrowly as possible, rather than allowing for a wide application and interpretation that could potentially be misapplied and include privacy breaching identifier elements in future.

The word “biometric” has been used quite widely throughout the proposed legislation and needs qualification. While biometric information such as fingerprint biometrics are commonly accepted for use, other forms such as facial recognition remains as something that the Human Rights Commission in the recent Human Rights and Technology Final Report has warned about its use. Hence, it is currently not advisable for it to be used until proper rules are made for it.

What this also means is that the development of the law on its regulation of biometrics needs to move in tandem with the development in the Human Rights and Technology Final Report.

Protecting the Australian Privacy Principles (APPs)

Individual privacy is notably seen to be rapidly diminishing as time passes, and hence, any such new legislation passed must take into account the human rights to autonomy, privacy and freedom.

Security

With technology ever-increasing and evolving, human and AI hacking mechanisms are developing at the same rapid rate. Consideration should be given to using a hash-based matching for credential fields rather than data transfer; noting potential scaling issues, this would align the system to OpenID and OAuth services which have operated securely for years across thousands of online services.

The economic benefits of introducing a Digital Identity System based on a federated model

and that leverages the existing notifiable data breach scheme must be carefully weighed against the real risks of identity theft and data breaches, via the potential hacking of Government systems, which has indeed occurred before. In addition, the remedies available to the victims of a data breach are insufficient and largely inaccessible under the current Australian regime. Accordingly, system designs should look beyond the sharing and transfer of information and towards privacy enhancing technologies and methods of sharing results of checks of information and attributes that are held by an individual.

Security controls for the proposed digital identity system have not been defined. The Government is bound by the ISM (Information Security Manual) controls, although compliance is ad-hoc based on ANAO audit findings over the past decade. The system should be independently audited and penetration tested regularly with the results made public.

The private security is not required to comply with the ISM and it is unclear what, if any security controls, auditing or transparency commercial providers will be required to meet. This is a significant risk in that commercial providers (Credential Service Providers) will apply their own security controls with little transparency or assurance of their effectiveness. By comparison the credit card industry faced a similar problem around 2003-2005 in that payment gateway companies were passing large numbers of credit card identities with varying levels of security. This approach resulted in ongoing, significant fraud and identity theft through security breaches at these commercial providers. Visa/Mastercard then implemented the PCI-DSS security standard which was mandated and audited for all agents collecting credit card information which significantly reduced the number and severity of privacy breaches.

Insurance is needed to protect individuals whose identity is stolen through a security compromise of this system. An example is the US Department of State that was the subject of a security compromise and data loss of staff's personal information. All affected staff were provided with lifetime identity theft protection and support as a result. It would be expected that this system will be a high value target for organized crime, the Government needs to ensure that when a security breach occurs, Australians are protected to the greatest extent possible.

Including the views and access requirements of all relevant stakeholders in the consultation process

Given that Australia is based upon a democratic system, the views of all individuals should be taken into account during the final drafting and passing of the proposed legislation. This should include the views of those that favour the upholding of individual privacy and confidential information. Personal identifiers that are ultimately included should be taken through a rigorous consultation process with various human rights bodies and privacy law entities.

The service should offer no discrimination in terms of services available or service timeframes between those with a digital identity and those who do not have one. Current websites advertise examples with significantly slower non-digital identity service levels that could easily be aligned to the performance of the digital identity system with the introduction of modern document verification services into the workflow. As it stands the proposal is discriminatory against those who choose or are not able to use a smartphone to manage a digital identity.

It is also unclear what the digital identity can be linked too. For example Medicare

information is segregated from welfare information via legislation. What are the controls for the digital identity? Without controls in place it is reasonable to expect that the digital identity will be eventually linked to all Government information.

Creation of digital identity needs to have a robust process, equal to or greater than the creation of passports. This process requires quality control checks and auditing in addition to the standard processes to ensure that digital identity is irrefutably linked to an individual and that that is the individual who has initiated its creation. Failure to ensure the individual creating the ID or that the process to create it is robust is likely to lead to the digital identity being used for fraud and it being difficult to prosecute offenders.

The use of external Credential Service Providers provides a significant risk of fraud for digital identity. By comparison the Australia Government does not allow corporate entities to create passports, despite the passport counting for less proof of Identify then this system.

The creation and validation of digital identity should be restricted as a Government service and NOT outsourced to commercial providers. Doing so with the above risks makes the system open to abuse.

Consultation process

This consultation process should include independent bodies as well, to ensure full spectrum coverage and assurances. Possible contactable entities include the below.

Australian Human Rights Organisations to consult with:

- Australian Human Rights Commission
- Human Rights Council of Australia
- Amnesty International, Australia
- Refugee Council of Australia
- The Change Agency Education and Training Institute
- NSW Council for Civil Liberties
- ACT Human Rights Commission
- The Victorian Equal Opportunity and Human Rights Commission

Privacy related organisations to consult with:

- Australian Privacy Foundation
- Office of the Australian Information Commissioner (OAIC)
- The Information and Privacy Commission NSW (IPC)
- Office of the National Data Commissioner
- National Data Advisory Council

3 Law Enforcement and Privacy: Judicial oversight

Recommendation #3

That the Bill incorporates independent and (preferably) judicial oversight over the disclosure of information to enforcement bodies under section 81 and that any accredited entity that acts upon the recommendation or decision of an oversight body in relation to section 81 not be liable for a civil penalty under such provision.

Intended outcomes

- Ensure independent oversight of the disclosure of information to enforcement bodies so that accredited entities are not the main safeguard against enforcement overreach under section 81.
- Increase trust and integrity in the Digital Identity System.
- Reduce the likelihood of evidence that is obtained under section 81 be excluded on the basis that it was obtained improperly or illegally.

Accredited Entities as the Safeguard against Enforcement Overreach

Unless there is a warrant or active proceedings, accredited entities would be the main safeguard against enforcement overreach where a request for disclosure is based on an enforcement body's reasonable suspicion that an offence or relevant breach of law has been committed (**requisite reasonable suspicion**). Despite the lawfulness of a disclosure being contingent on the enforcement body having the requisite reasonable suspicion, it is the accredited entity (as the disclosing party) that will bear the liability risk if that objective standard is not made out.

From the perspective of the accredited entity, we consider this liability position to be unfair because these entities will not have control over the processes that would lead to an enforcement body forming the requisite reasonable suspicion. Furthermore, we believe that it is inappropriate that accredited entities need to be satisfied that the enforcement body had the requisite reasonable suspicion, before disclosing the requested digital identity information. Given that some accredited entities will be private organisations (e.g. Eftpos), such entities may not have the capability to make such an assessment.

Although a similar provision exists in APP 6.2(e) of the Privacy Act, we note that this Act is currently under review, particularly on its effectiveness in protecting personal information and providing a practical framework for promoting good privacy practices.

Public Trust & Integrity in the System

Investigatory information is also incredibly sensitive and could be detrimental to an individual's life if released to the public. This is especially so if the individual was later exonerated. To promote public trust in the Digital Identity System it would be preferable that judicial (or similar) oversight be embedded in any such disclosure for enforcement-related activities, as has been done in the *My Health Records Act 2012 (Cth)* (**MHRA**) (see MHRA s 69A).

It is important that robust safeguards against oppressive overreach by enforcement bodies are demonstrably in place and fully functioning. Trust in the digital identity system will erode if private companies with no public entity duties are effectively responsible for ensuring that

the legal safeguards are met under s 81. Trust in the system is key to encouraging engagement in the Digital Identity System, particularly from marginalised populations, many of whom are disproportionately targeted by law enforcement.

Ensuring admissibility of Evidence

Incorporating further independent oversight of the authorised use and disclosure of information would also encourage good evidentiary practices that assures admissibility. It would be beneficial for the judiciary and any other experts to be engaged on this point, specifically on effecting control of the admissibility of the information gathered for DigitalID in proceedings unrelated to the permitted purpose for the collection of that information.

4 Law Enforcement and Privacy: Digital Identity System Design

Recommendation #4

That the system in which digital identity information is collected, used and disclosed is designed in a way that assures a person's privacy is protected and safeguarded. These systems should be designed with data stewardship principles in mind, and with the benefit of latest review process on identification of ethical issues with technology design.

Intended outcomes

- A digital identity system that treats a person's information sensitively and appropriately to avoid unintended and harm consequences to individuals.

Our notes of review

The Digital Identity System must be transparently designed in a manner that ensures that personal information is treated sensitively and with care. Recently, we have seen an instance where the myGov and Services Australia systems inadvertently disclosed a domestic violence victim's address to her abuser ([link](#)). This breach of the Privacy Act was caused by poor system design that failed to appreciate the flow of an individuals' information and inadvertently endangered this person's life.

These systems should be designed with reference to data stewardship principles, which is a governance methodology that ensures that data is accessible, usable, safe and trusted. These governance policies can be used to encourage systemic design and culture of data use and governance that:

- ensures that personnel are accountable to the flow of information; and
- protects individual's information.

These systems should also ensure that information passes through a system that has been designed so that sharing of information between government agencies or other use and disclosure, takes into account fundamental protections against unnecessary and potentially harmful disclosure.

5 Data profiling

Recommendation #5

That section 80 of the Bill provides for safeguards against the dangers of data profiling.

Intended outcomes

- Increase public trust in the Digital Identity System by providing for safeguards against abuse that may arise through data profiling.

Our notes of review

The Bill prohibits data profiling at section 80. However, subsection (2) provides an exception for certain entities to use it. This needs further qualification due to the dangers of data profiling when used for enforcement purposes even when it is an authorised use. For example, it may cause discrimination towards people of colour (see [Human Rights and Technology Final Report](#)). Hence, section 80 needs to provide for safeguards against abuse.

6 Accessibility for Australians abroad

Recommendation #6

That the proposed expansion of the TDIF for the purpose of enhancing accessibility of Australian government and private sector online services to all Australians include Australians¹⁶ not currently residing in Australia.

Intended outcomes

- Enable Australians who are temporarily or permanently living abroad to easily access Australian online services requiring authentication in compliance with Australian law.

Broadening the scope of the Digital Identity legislation and associated instruments to include Australians living abroad

In principle, the TDIF (including the *TDI Bill*, draft *TDIF Accreditation Rules 202x* and the draft *TDI Rules 20xx*) could be expat-friendly by acknowledging the following factors:

- Access to the TDIF system from geo-locations outside Australian territories should be possible and permissible (or even perhaps mandated) for all Australians – even though residing abroad. There are **two** considerations when examining accessibility in this context:
 - the first is the ability of Australians abroad to engage with and use the TDIF; and
 - second, the ability of onboarded entities to handle such information within the TDIF system even though it may interface with foreign jurisdictions.

Importantly, **rule 9 subsection (2)** of the *Trusted Digital Identity rules 20xx* (draft) specifies

¹⁶ Including citizens and Permanent Residents.

that:

...an entity must not engage in or cause or permit another person to engage in:

- (a) holding, storing or handling digital identity information at a place outside Australia;*
or
- (b) transferring digital identity information to a place outside Australia for storage, processing or handling.'*

Under **subsection (3)**, this prohibition does not apply to:

- (a) conduct undertaken to comply with a request by the individual to whom the digital identity information relates, being a request made from a place outside Australia;*
or
- (b) conduct undertaken to verify the identity of an individual or authenticate the digital identity of, or information about, an individual.*

From the perspective of Australians abroad, this regulatory posture is positive. The question is whether this approach effectively secures the ability of Australians living abroad to fully benefit from the TDIF system. The policy choice is between supporting Australians living abroad (who may not be part of the taxpayers) against increased compliance and technical burdens upon the TDIF system and participating entities within Australia. As Australians, even those residing abroad should also benefit from Australia's digital infrastructure.

Legislators may wish to consider strengthening this position by mandating that Australians living abroad have a 'right' to access the TDIF no different to any other Australians. This discussion, however, may more appropriately fall within the scope of a contemplated Digital Bill of Rights.

Particularly in relation to 'Attribute Collection, Verification and Validation'¹⁷, compulsory attributes such as (Table 2, item 3) 'Mobile Phone number' must include the capacity to record foreign phone numbers. It is appropriate that the attributes in Table 3 that may (as opposed to must) be collected include the attributes of 'residential address' and 'postal address' as in many parts of the world, address infrastructure is lacking.

There should be greater clarity and consistency in relation to identity documents issued by foreign governments to Australian living abroad and how they are recognised within the TDIF.¹⁸ It is acknowledged that foreign issued identity documents cannot (alone) form the basis of a verified digital identity. The current approach taken, however, has room for improvement.

Under the current *Accreditation Rules*¹⁹ (draft), the approach taken to the validity of foreign documentation is inconsistent. Foreign military identity documents and foreign passports (with a valid visa stamp), for example, are permitted forms of identity documents. By contrast, foreign bank account statements and cards issued by foreign banks are prohibited. Other documentation such as 'educational certificates' specifically state that the documentation must be issued by an Australian institution. Whereas other categories such as 'Motor vehicle registration' makes no mention of whether such documentation must be issued by Australian authorities or otherwise.

¹⁷ Rule 3.6 (draft) *Trusted Digital Identity Framework Accreditation Rules 202x*.

¹⁸ It is acknowledged that the Accreditation rules do provide some flexibility for 'individuals unable to meet identity proofing requirements': Rule 3.3, *Trusted Digital Identity Framework Accreditation Rules 202x*. Although these rules are contemplated as applying to disadvantaged groups such as Aboriginal or Torres Strait Islanders, it can also apply to Australians living abroad holding IDs issued by foreign governments.

¹⁹ Schedule 4 (Commencement of Identity (COI) documents), Schedule 5 (linking documents), Schedule 6 (Use in the Community (UITC) documents) and Schedule 7 (Photo Ids).

Greater clarity, particularly with respect to this last category would be useful.

Examples of how the TDIF (and its proposed expansion) can benefit Australians abroad

1. Processing birth and citizen certificates for children born to Australian parents
2. Renewing or replacing lost or expired documentation (including passports)
3. Receiving, filing and processing court related documents
4. ID verification for updating or changing personal details on government and private sector databases
5. Engaging in all manner of financial services while abroad (One of the most common being applying for homes loans with Australian banks while abroad).
6. Establish and maintain lawful accounts as an Australian citizen with Australian-based private sector organizations engaging in activities banned in some foreign jurisdictions.²⁰

7 Innovating alongside best practice – self sovereign identity

Recommendation #7

Revise language and technical requirements in both the proposed legislation and TDIF to allow for the incorporation of SSI services and provide for the fluidity of innovation in technology.

Intended outcomes

- Increase the interoperability, flexibility and integrity of the Digital Identity System by including the capacity to integrate decentralised digital identity solutions, like SSI.
- Increase opportunities for integration of emerging and future technologies and best practice privacy enhancing technologies.

Our notes of review

In its current form, this proposed legislation excludes the capacity to integrate decentralised digital identity solutions, like SSI. Soozee's Phase 3 Consultation submission, endorsed by the DLA, provides an excellent summary of active and successful SSI programs operating around the world. A comparison table between federated identity management systems such as the existing (unlegislated) and proposed legislated model for Australia and an SSI system is provided below.

Comparison: Federated Identity Management System (Australian Model) versus SSI System

Feature	Federated	SSI
---------	-----------	-----

²⁰ For example, Crypto-Asset related dealings may be banned in some countries limiting two-factor authentication with a foreign number. Australians legitimately dealing from Australian bank accounts with Australian based service providers should still be able to access such services.

Individuals can generate their own identifiers	N	Y
Individuals are in control of their own authenticators (i.e. private keys)	N	Y
Individuals are in control of their own digital credentials and certificates	N	Y
Individuals can have control over their identifiers in case of loss or theft of their keys	Y	Y
Individuals can retrieve their credentials and certificates in case of loss or theft of their keys	Y	Y
Individuals can access the data associated with their digital identity	U	Y
Enabled zero-knowledge proofs	N	Y
Personal identifiable information (PII) is minimised	N	Y
Right to be forgotten can be easily guaranteed	N	Y
Repositories of authenticators and credentials are portable	N	Y
Identity providers do not keep centralised databases with user's data	N	Y
Identity providers do not have access to information about people's access to services or interactions with others	Y	Y
Implementations comply with regulatory policies	Y	Y
Trust frameworks are developed to allow the definition of identity providers and levels of assurance	Y	Y
Identity is easily retrievable in the case of a natural disaster	Y	Y
Data breaches less likely	N	Y

Y = Yes N = No U = Unclear

8 Global and technical interoperability

Recommendation #8

The legislation should provide for integration of provisions to recognise accredited providers in third party jurisdictions.

Intended outcomes

- Increase opportunities for integration of emerging and future technologies in particular across jurisdictions.

Our notes of review


While interoperability of providers is addressed in the draft legislation, it does not expressly address the need for international interoperability. Digital identity is necessarily borderless; to realise a robust, accessible, seamless user-experience for Australians, any Digital ID system needs to be internationally interoperable.

As previously stated, the Federal Republic of Germany, the Kingdom of Spain and Finland have recently partnered to pursue opportunities for collaborating on cross-border digital identity (based on

SSI) to ensure that all solutions and components of digital identity will meet European standards and reflect European ethical values on Digital sovereignty.

Article 14 of the EU equivalent of this Bill, eIDAS (*European Regulation (EU) No 910/2014*) allows trust service providers outside the EU to be recognised as legally equivalent to those in the Union provided the third country is recognised under an agreement with the EU.

FIND US AT

 @digitallawassociation

 @DigitalLawAssoc

 @digitallawassociation

 @DigitalLawAssoc

CONTACT US

 info@digitallawassociation.com