18 December 2020

Digital Transformation Agency
280 Elizabeth Street
SYDNEY NSW 2010

digitalidentity@dta.gov.au

ACCAN thanks the Digital Transformation Agency for the opportunity to contribute to its consultation on the proposed Digital Identity Legislation. It is ACCAN's understanding that there will be future opportunities to provide input on the draft Digital Identity Legislation, and consequently our comments are high level and only address some of the questions outlined in the Consultation Paper.

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

All of the privacy and consumer protection safeguards in the TDIF must be enshrined in law. ACCAN is concerned that any privacy or consumer protection safeguards not enshrined in law will lack the enforcement necessary for organisational compliance. This is particularly important given that the TDIF currently includes privacy protections above and beyond those provided by the *Privacy Act*.

However, ACCAN submits that any matters which are included in the Legislation should also remain in the TDIF to ensure these provisions are reinforced by other non-legislative and administrative instruments. Indeed, given that the TDIF will continue to form the basis for the accreditation of entities involved in the Digital Identity system, it is essential that these provisions remain in this Framework.

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

The Operating Rules will be structured to give certainty to prospective Participants about the requirements for participation in the system. As they include more procedural requirements, we understand that the Operating Rules will need to be flexible to ensure scalability of the regulatory system as the TDIF is expanded and non-Commonwealth entities choose to participate.

ACCAN supports the proposal that the Legislation will give the Oversight Authority the power to set and maintain Operating Rules. We believe that legislative backing for this power will support clarity of functions, and consistency in consumer protections. As outlined above, we believe that the Legislation and its accompanying legislative instruments must reinforce non-legislative instruments such as 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?

The definition of Digital Identity should be harmonised with the Privacy Act to create a robust network of privacy protections for consumers. As ACCAN has submitted in response to the Attorney General's Department Privacy Act Review Issues Paper, the current definition of personal information and sensitive information in the Privacy Act needs to be expanded to suit modern data collection practices.

7) What factors should be considered in the development of a Charging Framework for the system?

ACCAN opposes the development of a Charging Framework[1], as it will discourage some non-government organisations from using the Digital Identity system. To encourage use of the system by a majority of non-government organisations the system should be free of charge.

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

ACCAN agrees with the 2018 'Privacy Impact Assessment of the system and TDIF'[2] recommendation that the privacy regime that applies to Accredited Participants should be enshrined in legislation. Enshrining the privacy and consumer safeguards currently contained in the TDIF - including liability, penalties and redress for fraud or misuse of data – in primary legislation is necessary to ensure consumers are protected. The threat of adequate penalties for breach will encourage organisations and entities to comply with these provisions.

The key privacy issues in any Identity system are meaningful genuine consent and protection against 'function creep' – i.e. when information is used for a purpose that is not the original specified purpose. The privacy and consumer protections that should be enshrined in the Digital Identity legislation therefore include:

- ensuring the system remains voluntary (not mandatory);
- prohibition on the commercialisation of personal information and profiling of individuals; and
- protection against gradual or incremental changes to the system that might result in an erosion of privacy over time.

[1] The Charging Framework covers activities where the government charges the non-government sector for a specific government activity such as, regulation, goods, services, or access to resources or infrastructure - www.finance.gov.au/government/managing-commonwealth-resources/managing-money-property/managing-money/australian-government-charging-framework

[2] As mentioned in the Consultation Paper.

ACCAN submits that enshrining these provisions in law is necessary because any privacy and consumer protections not included in legislation will not be enforceable. Based on experience in the telecommunications industry, legislative penalties for failure to adhere to consent requirements and appropriate data use are essential to ensure industry compliance.

The enforceability of privacy and consumer protection provisions will become increasingly important as the Digital Identity system is rolled out to more government and non-government services and a larger pool of organisations and entities have access to consumers' personal data. Consumers will want the safety of their data guaranteed before choosing to use the Digital Identity system.

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

ACCAN supports the creation and use of a Digital Identity being a voluntary choice and appreciates that users will have the option to deactivate their use of the system at any time. Guaranteeing genuine user consent to be involved in the Digital Identity system is crucial.

For some Australians there may be practical or personal reasons why traditional verification processes are easier or more accessible. Some consumers may be unable to afford digital communications technologies and may therefore not be able to engage with the Digital Identity system. In addition, seniors may be more comfortable using in-person or paper-based identification, and people with disability, such as those with vision impairment, may require alternative verification processes.

For the Digital Identity system to be genuinely voluntary and facilitate consent by all participants, the Legislation must include rules around the extent of choice available to Users to verify their identity and must maximise the range of verification choices available.

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?

Article 8 of the GDPR states that the processing of personal data of a child under 16 years old is only allowed if "consent is given or authorised by the holder of parental responsibility over the child."

ACCAN submits that this restriction should be adopted by the Digital Identity system, and children under the age of 16 should not be subject to collection and processing of personal information by organisations and entities without the express authorisation of a responsible adult, as per Article 8 of the GDPR. This means:

- The responsibility for safe data collection practices is shifted away from children, and the obligation to provide adequate privacy protections for children falls to responsible adults including regulators, entities and organisations.
- A child under 16 years old is regarded as not having the capacity to understand that entities are collecting their personal information and using it for marketing and other purposes.

However, ACCAN would caution against any override mechanisms being used for paternalistic purposes, for instance to restrict access to the Digital Identity system for young people with disability.

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?

ACCAN agrees that in some instances people might need support to engage with the Digital Identity system. This support must be able to be tailored to the unique needs and circumstances of the person needing assistance.

The Legislation must clearly outline the circumstances in which a supporter may be nominated by the person needing support, the process for nominating a supporter, and the activities that the supporter is or is not authorised to perform. Activities enshrined in Legislation could include, for instance, supporting someone to use and engage with the Digital Identity system, helping someone understand and interact with the registration process, or helping them manage correspondence regarding the system. In all instances, the supporter must be required to ascertain the wishes of the individual engaging with the Digital Identity system, and to promote and protect their rights when engaging with the system.

The Legislation must also specify the authorisation process by which the person needing support can assign people to this role. Protections and safeguards must be put in place to ensure that supporters are acting appropriately and are upholding the rights of the person using the Digital Identity system. The Legislation must enshrine a consistent process for authorising or appointing supporters to engage with the Digital Identity system.

Individuals must also be given the choice to not assign a supporter, even if they recognise they would benefit from additional assistance for their engagement with the system. As outlined above, traditional verification processes will still be necessary for some Australians.

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?

The Legislation must recognise that Australia is a party to seven core human rights instruments,[3] and has legal obligations under these international treaties. As such, the Legislation must protect and promote human rights and prevent all forms of discrimination. This includes all forms of racial discrimination, disability discrimination, and gender- and age-related discrimination. While some of these instruments have specific articles dealing with privacy and other types of safeguards, some may not. This does not mean that these human rights instruments shouldn't be considered in the Legislation. The Legislation must acknowledge the impacts of different types of discrimination and seek to eliminate any types of discrimination (including intersectional discrimination) that could be present throughout the Digital Identity system.

[3] https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/international-human-rights-system

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

The proposed approach to accessibility and usability is appropriate. ACCAN supports the Legislation incorporating accessibility requirements and requirements around user testing.

It is ACCAN's position that user testing must be performed with a broad range of people, including those who are typically not included in such testing. This could include, for instance, people with communication disability, people with autism, people with intellectual disability, people with spinal cord injuries, young people with disability and older people with disability. People involved in user testing must be appropriately renumerated for their time and expertise.

In relation to accessibility, it must be recognised that the Web Content Accessibility Guidelines (WCAG) are routinely updated. As such, we believe it would be more appropriate to future-proof the Legislation by including references to successor accessibility standards. This could be achieved, for instance, by the Legislation referencing 'the most up to date version of WCAG' rather than 'WCAG 2.0'. This is particularly pertinent as the most up to date Guidelines are currently WCAG 2.1, and efforts are underway to draft WCAG 3.0.

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?

ACCAN agrees that effective governance of the Digital Identity system is essential for the efficient operation of the system and for instilling public trust and confidence, and that the Legislation should grant power to a permanent Oversight Authority to ensure privacy and consumer safeguards enshrined in the Legislation are strictly enforced.

Whether this function is fulfilled by an existing body such as the Office of the Australian Information Commissioner, or by a new body established for this purpose, it is imperative that the Oversight Authority is adequately resourced to execute its regulatory and enforcement function effectively. The Oversight Authority will need the ability to promptly respond to any data breaches or mishandling of personal information in order to minimise the damage caused, and that will only be achieved with adequate resources.

25A) Are the roles and functions outlined above appropriate for the Oversight Authority?

25B) Are there any other functions that should be undertaken by an Oversight Authority? If so, what?

ACCAN agrees that the Oversight Authority should administer the accreditation process for Accredited Participants, manage service onboarding, independently monitor fraud and security and service monitoring and incident response.

ACCAN also submits that the functions of the oversight authority should also include customer experience functions such as investigating complaints and administering the complaints handling mechanism.

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

Consumer representative organisations must be part of the Privacy Advisory Committee to ensure that consumer privacy issues are considered.

Sincerely

Stephanie Whitelock
Policy Officer
ACCAN