16 July 2021

Digital Transformation Agency
50 Marcus Clarke Street
CANBERRA ACT 2601

digitalidentity@dta.gov.au

RE: Digital Identity Legislation – Phase 2 Consultation

ACCAN thanks the Digital Transformation Agency for the opportunity to contribute to Phase 2 of the Digital Identity Legislation consultation. We will provide feedback on several of the key areas on which the DTA is seeking to develop clear positions. These are:

- scope of the legislation and interoperability with other systems
- regulatory oversight of the system
- privacy and consumer safeguards
- trustmarks
- liability and redress framework
- penalties and enforcement
- administration of charges for the Digital Identity system.

1. Scope of the legislation and interoperability with other systems

ACCAN welcomes the new interoperability principle that has been introduced to clarify how entities on the Participant Register will work together to provide a seamless user experience with the Digital Identity system and that Relying Parties are required to offer a choice of identity providers. We are also pleased that, in principle, consumers will not be compelled to join the Digital Identity System if they choose not to.

However, we question whether the decision to 'opt out' of using the Digital Identity System will prove so inconvenient for consumers that by default they will feel compelled to participate. Similarly, if the alternative to using the Digital Identity System is prohibitively difficult, consumers without reliable internet access will be prevented from accessing public services online via the Digital Identity System.

Furthermore, although the publicly accessible Participant Register is intended to provide consumers with the opportunity to make informed decisions about using the system, we doubt it will deliver this outcome in practice. Without appropriate consumer education, ACCAN harbours concerns about the ability of consumers to fully understand the categories of Accredited Participants, the differences between their roles and the services they are permitted to offer when choosing whether to 'opt in'.

Given the complexity of the accreditation process, and the complicated tiered system dictating the types of personal information an entity is permitted to collect, it is quite conceivable that an average consumer might not understand what level of data collection and exchange they are agreeing to, making genuinely informed consent difficult or, for some consumers, impossible.

2. Regulatory oversight of the system

ACCAN agrees that effective governance of the Trusted Digital Identity system is essential to instil public trust and confidence in the system, and to facilitate the system's efficient operation. We reiterate our point that, to be capable of promptly responding to any data breaches or mishandling of personal information to minimise consumer harm, any long-term Oversight Authority must receive adequate financial support and resources to execute its regulatory and enforcement function effectively.

3. Privacy and consumer safeguards

ACCAN is pleased to see the introduction of legislative safeguards to protect the personal information of individuals who choose to use a digital identity. We welcome the three principles that have guided the development of the privacy and consumer safeguard policies in this Position Paper – privacy protection, building on existing laws and balancing strong consumer and privacy protections with fostering participation.

First, robust privacy protection, and interoperability of the Digital Identity Legislation with existing privacy laws including the *Privacy Act*, is crucial to ensure comprehensive privacy protection for consumers. Given the volume of personal information consumers will be providing to participate in the system, data breaches and hackers will have the potential to expose consumers to security vulnerabilities with serious consequences. The TDIF's system specific privacy and consumer protections system will help supplement the regulatory gaps in the current privacy regime.

Second, ACCAN agrees that fostering the participation of businesses and government in the Digital Identity system should not be prioritised over consumer protection. The principles of data minimisation, decentralisation and limited access are essential to minimise potential consumer harm arising from breaches of security and data integrity. ACCAN welcomes the restrictions on the creation and use of a single identifier across the system, data profiling and collection and use of Biometric Information.

We also approve of the requirements for Users' express consent before enabling their authentication to a service. However, ACCAN flags the underlying problem with obtaining genuinely informed consent from consumers, given the complexity of notice and consent agreements that consumers are asked to agree to. This underlying problem also informs ACCAN's response to the trustmark system proposed in the Position Paper.

4. Trustmarks

In principle, ACCAN is supportive of the Legislation establishing trustmarks as part of the Digital Identity system as the system expands beyond Australian Government entities. Clearly identifying which Accredited Participants and Relying Parties on the Participant Register are certified by the scheme, and which roles and level of services they are accredited to provide, has the potential to enable consumers to engage with the system in a more informed way.

However, ACCAN has reservations about the effectiveness of a trustmark system in circumstances where consumers have little or no understanding of what these trustmarks represent. Research recently conducted by Deakin University found that consumers felt trustmarks would have limited utility in informing and protecting consumers in the absence of accompanying consumer education.[1]

[1] Deakin University, *Regulating the Internet of Things to protect consumer privacy*, unpublished - https://accan.org.au/grants/current-grants/1611-regulating-the-internet-of-things-to-protect-consumer-privacy

ACCAN notes that the Position Paper acknowledges the need for "an initial period of building recognition of the digital identity trustmark(s) associated with TDIF accreditation and use of the system" to make the trustmark system effective. However, ACCAN encourages the Digital Transformation Agency to roll out a dedicated consumer education program to allow Users to understand the trustmark system, rather than just hoping "consumers will become more familiar with the trustmark(s) as uptake increases".

The Position Paper clearly states the need for the Oversight Authority to decide which category of trustmark applies to respective Participants and TDIF Providers, given the complexity of categorisation under the Digital Identity system. This highlights the need for consumer education to inform Users about the trustmark system, including the role to which the various trustmarks apply, and what implications this might have for consumers in terms of the collection and use of their personal information.

5. Liability and redress framework

Under the legislation, the Oversight Body will be authorised to provide practical support to consumers in effectively monitoring and enforcing compliance with the Legislation, including advising and assisting consumers to deal with the consequences of cyber security incidents, advocating on their behalf, coordinating with law enforcement and other organisations involved in managing the consequences of identity theft and investigating and collating evidence that could be used in litigation.

However, it appears that the proposed framework imposes no requirement on the Oversight Body to ensure consumers are compensated for their losses, and that its role in consumer redress and recovery is primarily to redirect affected consumers to identity and cyber support services. For example, the Oversight Authority will work with cyber support services such as the government-contracted ID Care to assist victims of identity theft or fraud and liaise with credit agencies who may have relied on false information provided by the Digital Identity system.

As a body sponsored by major banks, the services ID Care provides appear to be geared towards corporations, and consumer services are limited to advice on what to do if an individual has been scammed. ACCAN therefore questions the consumer benefit of the Oversight Body referring individual consumers to ID Care. The outcome for consumers will be that one advisory body, the Digital Identity Oversight Authority, will refer them to another advisory body, ID Care, without any guarantee of tangible redress.

We note that the Oversight Authority is exempt from any penalties for any loss or injury directly or indirectly suffered by Users for acts or omissions by the Oversight Authority done in good faith in the exercise of the powers, performance of functions or role of the Oversight Authority. This exemption limits the redress available for Users who are the victims of poorly handled security incident response, disaster recovery, monitoring and enforcing of TDIF rules, use of information made available through the system and sharing of data relating to Participants.

Given, under the proposed legislation, the Oversight Authority faces no liability for consumer harm resulting from acts or omissions in good faith, ACCAN harbours concerns about the effectiveness of this purely advisory approach. This could replicate the issues consumers experience with the Telecommunications Industry Ombudsman (TIO). ACCAN often receives consumer complaints that the TIO offers advice to consumers but does not adequately monitor the outcome to ensure the issue has been dealt with. This leaves consumers without an adequate resolution or financial compensation and forces the responsibility for safety and security once again back onto the consumer.

ACCAN submits that the Oversight Authority needs to have the power to create an easily resolvable complaints resolution process so that consumers can easily access a free complaints resolution service which will reverse any consumer harm suffered.

6. Penalties and enforcement

ACCAN understands from the Position Paper that the Legislation will establish a penalty and enforcement framework to ensure the privacy safeguards enshrined in the Bill can be enforced by the Information Commissioner and support the Oversight Authority to effectively monitor and enforce compliance with the Legislation.

Under the Legislation the Oversight Authority will be authorised to seek civil penalties, enforceable undertakings and injunctions for matters relating to contraventions of the enforceable rules, misuse of trustmarks, recordkeeping and breaches of obligations on offboarded Participants. The Oversight Authority will also have the power to issue notices to provide information or documents (using common provisions for providing a notice stating the information sought and a timeframe) and to seek civil penalties for a failure to comply with a notice.

ACCAN reiterates its point made regarding the liability and redress framework, that the Oversight Authority needs to play a stronger role in consumer protection, monitoring the outcome of the civil penalties and undertakings it seeks, and ensuring consumers are compensated for loss or damage as a result of using the Digital Identity System.

7. Administration of charges for the Digital Identity system

It is proposed the Legislation will not impose charges on Users for the administration of the Digital Identity System, but that the Legislation will not regulate fees charged by relying parties to an individual wanting to access its service(s) using the system. This approach leaves open the opportunity for relying parties to impose charges on consumers for use of the Digital Identity System.

Although Principle 1 of the Charging Principles states “charges should foster inclusion, facilitate affordability for Users and relying parties, and incentivise adoption,” there is enough flexibility in this principle for consumers to be liable to considerable charges in the interests of “incentivising adoption” by relying parties.

Given ACCAN’s earlier point that opting out of the system may, in practice, be unfeasible, consumers may be left in a position where, to access public services, they are forced to pay to access services that were previously free. Similarly, consumers should not be excluded from using private services by having to pay to prove their identity.

ACCAN therefore submits that there should be no cost to consumers to use the service or, as an alternative, there should be requirement that Relying Parties offer at least one free digital identity system.

Sincerely

Stephanie Whitelock

Policy Officer