Digital Identity Legislation

Have your say submission

December 2020

Anonymous submission

Executive summary

The Digital Identity legislation is an exciting and monumental initiative for not only the Australian Government, but businesses, citizens, residents and consumers alike. Digital Identity will be a key pillar of a flourishing data economy. It will give citizens and consumers greater access to and control over their personal identity and data through a centralised and trusted authority.

The Digital Identity legislation is very much focused on the mechanics of the Digital Identity and is focused on the participants and ecosystem however, lacks the end user perspective. This message should be the driving theme of the Digital Identity and by missing this, it bypasses the purpose and benefits of the Digital Identity. This emphasises the need for a regulatory body, which is consumer focused, to be associated with and deliver the Digital Identity to bring this perspective to the forefront.

Until the Digital Identity can robustly articulate this angle, the benefits will not be able to be realised and the project will likely require significant recalibrating to get back on track. It is essential to take a user-centric approach when designing the Digital Identity solution and legislation which focuses more on the outcomes of the Digital Identity rather than the approach.

There exists opportunities in Government, such as the Consumer Data Right (CDR), to leverage proven solutions, operations, skillsets and experience to successfully deliver the Digital Identity. There is strong overlap between the CDR and the intention, solution and delivery of the Digital Identity and leveraging this opportunity will significantly advance the Digital Identity through early and accelerated realising of benefits to end-users, reduced CAPEX and OPEX and focused outcomes.

The CDR and Digital Identity have shared requirements such as accreditation, on-boarding, ecosystem maintenance, cyber security, etc. and is a fully operational division within the ACCC. It is resourced with experienced individuals who have delivered a proven CDR solution therefore this raises the question – why duplicate these operations and solutions when they can be easily leveraged? A very relevant example is the operational CDR Register and Accreditation Application Platform (RAAP). This solution has similar requirements to Digital Identity and leveraging this established solution should be investigated.

Overtime, the organic progression of the CDR may potentially shift towards digital identity due to the strong synergies between consumer data and citizen identity therefore, there is a good fit and opportunity both for the CDR and Digital Identity alike, to benefit and propel objectives as a single unit.

The key risk associated with Digital Identity involves breach of data privacy and data leaks, the association with the ACCC, if Digital Identity were to fall in the CDR, will position the Digital Identity to best respond in the incidence that there is an issue and will prioritise the end-user to come to a resolution. Being tied to an independent regulatory body that is extremely experienced in representing consumers interests, will promote confidence and trust within the Digital Identity which will positively impact the benefits.

Consultation questions:

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

1B) Are there additional matters which should be considered?

1A)

With the intention of the Digital Identity to not only centralise citizen digital identity but to also provide a single source of truth of citizen identity to transact with businesses for goods and services, the need to appropriately govern the way in which Digital Identity is performed is crucial to maintaining the integrity of the data and solution and protecting citizens and consumers as they transact with the government and businesses alike.

Providing permanent governance arrangements is necessary and should be included in the Legislation, similar to the function of a regulatory body. Policy, enforcement and compliance will create confidence in the solution and generate trust in the Digital Identity. The Australian Competition and Consumer Commission (ACCC) has successfully demonstrated this capability through the delivery of the Consumer Data Right (CDR) in 2020. The trust already established in CDR and ACCC could be leveraged by Digital Identity should they share a similar oversight authority.

The CDR’s objective is to provide consumers with the ability to efficiently and conveniently access their personal data held by businesses (data holders or DHs), and to authorise the secure disclosure of that data to trusted third parties (accredited data recipients or DRs). This exchange has significant similarities to the objective of Digital Identity and strong synergies exist between the CDR and Digital Identity.

1B)

The high level matters of legal authority, privacy protections, governance, amendments are all appropriate matters to be considered. However, further consideration on how Digital Identity fits in with current data initiatives (e.g. CDR) and also how best to co-exist and leverage current infrastructure to expedite an effective data economy for Australia.

Consultation question:

3) Is a publicly available ‘Digital Identity Participant Register’ an appropriate mechanism to communicate who will be covered by the Legislation?

3)

Yes, noting that the Consumer Data Right (CDR) already includes an operational “Register” (RAAP – Register and Accreditation Application Platform). A detailed requirements gathering and gap analysis exercise would be required although, it is anticipated the RAAP and proposed Digital Identity Participant Register would share significant requirements and functionality. Why recreate something that already exists?

In addition, the capability, resources and processes to support and manage the proposed “Register” already exist and are operational within CDR e.g. accreditation, on-boarding, off-boarding, incident management, ecosystem monitoring, cyber security etc.

There also exists other opportunities to indicate Digital Identity participant accreditation in addition to the Register such as a trust mark or another visual, convenient and instant indicator of accreditation, similar to the “https” to indicated a secure website. It is important to consider a user-centric approach when designing the Digital Identity solution and considering a suite of ways to indicate participant accreditation.

Consultation question:

4) Are the proposed obligations on relying parties described above reasonable? Should there be any additional obligations?

4)

Yes, they are reasonable obligations for relying parties. To create more robust obligations, the below list could also be considered as additional obligations for relying parties

- are a fit and proper person
- are able to take the steps required to adequately protect Digital Identity data from misuse, interference, loss, unauthorised access, false modification or disclosure
- have internal dispute resolution processes meeting the requirements of the Digital Identity Rules
- are a member of a relevant external dispute resolution scheme
- have adequate insurance to compensate consumers for any loss that might occur from a breach of their Digital ID obligations, and
- have an Australian address

Consultation question:

7) What factors should be considered in the development of a charging framework for the system?

7)

Digital identity charging mechanisms should be considered in consultation with existing and planned data sharing solutions i.e. CDR.

Value for money should be a major consideration when developing charging mechanisms. High charges will become a barrier to entry for participants and limit the usability of the ecosystem and there is the risk that charges will be passed onto the end user. All options to maintain low/appropriate charges should be explored including:

- What already exists that could be leveraged to reduce implementation and operating costs for digital identity?
- Where could synergies exist with current data sharing solutions?

The above questions should be considered both for the Federal Government to build, implement and operate but also for Participants to reduce their requirement to integrate with multiple solutions.

The CDR is operational with established capability and Digital Identity should leverage these synergies to keep charges low/appropriate.

When developing a charging framework it is also important to consider the implications of charging participants to use the Digital Identity;

- What service level agreements are expected from the Digital Identity by participants?
- How will performance be monitored and reported on?
- If participants will be charged to use the Digital Identity, what will participants consultation and involvement expectations be?
- Will the Digital Identity be mandatory for businesses to use or opt-in?
- What alternatives exist if a business were to opt-out of Digital Identity given the choice?
- Though the Digital Identity benefits businesses, it will perform in the best interests of consumers, is this a conflict considering the business will be bearing the cost?

These implications emphasise the need to get the Digital Identity right the first time and early to be in a position to confidently charge participants a fee to use the service that will genuinely deliver benefits. The risks and costs associated with developing the Digital Identity solution in isolation are significant especially when a comparable operational solution such as CDR already exists.

Consultation questions:

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?

22B) What is the optimal structure of a new body?

22A)

Yes, there are options that exist today within Government that could be leveraged to fulfil the role of an independent Oversight Authority for Digital Identity. There are many benefits to be captured through leveraging an existing established independent body for the Digital Identity over starting up a new independent body including;

- Reduced expenditure through economies of scale and leveraging the existing capabilities, experience, skills, resources, processes, operations, etc.
- Accelerated delivery and results by leveraging parts of or an existing similar solution and established capabilities
- Improved accuracy and quality through experience and lessons learnt
- Greater opportunity to grow and evolve the Data Economy where like initiatives are grouped together
- Leveraging a brand with consumer and citizen recognition and pre-established trust

In order to unlock these benefits though, it is important that the best established independent body is selected.

The existing option presenting strongest synergies would be the ACCC, primarily based on their oversight and successful go-live in July 2020 of the Consumer Data Right (CDR). The CDR has significant similarities and requirements to Digital Identity. This response will explore key similarities between Digital Identity and the CDR where relevant to selecting the best Oversight Authority.

While ACCC is the best established option it should be considered that a new semi-autonomous structure within the ACCC, similar to the Australian Energy Regulator (AER), would enable the Oversight Authority to leverage the benefits and umbrella of the ACCC whilst creating the right governance structure to best deliver and operate these solutions.

Trust

Trust in both the Digital Identity solution and the Oversight Authority is critical for a successful ecosystem. The ACCC is independent and importantly is seen by consumers and citizens as independent, this is a key pillar to building trust.

ACCC also has established and proven processes and capability to successfully accredit, on-board and monitor participants. The testing and security validation before participants are accredited to participate in the ecosystem is an important feature of building trust. The effort that is required to successfully accredit, on-board and manage the eco-system to maintain this trust should not be underestimated. This already established process and capability can be leveraged for Digital Identity. Where a participant does not comply with their obligations ACCC has established and trusted Compliance and Enforcement capability that can also be leveraged for Digital Identity.

Consultation questions:

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?

22B) What is the optimal structure of a new body?

22A) *Continued*

Privacy
The ACCC, as the lead regulator, in combination with the Office of the Australian Information Commissioner (OAIC) are established and already provide privacy that is aligned to Digital Identity requirements.

The privacy of consumer data is of the utmost importance to the CDR as demonstrated by the robust privacy guidelines comprising of 13 privacy safeguards;

1. Open and transparent management of CDR data
2. Anonymity and pseudonymity
3. Seeking to collect CDR data from CDR participants
4. Dealing with unsolicited CDR data from CDR participants
5. Notifying of the collection of CDR data
6. Use or disclosure of CDR data by accredited data recipients or designated gateways
7. Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways
8. Overseas disclosure of CDR data by accredited data recipients
9. Adoption or disclosure of government related identifiers by accredited data recipients
10. Notifying of the disclosure of CDR data
11. Quality of CDR data
12. Security of CDR data and destruction of de-identification of redundant CDR data
13. Correction of CDR data

The full Privacy Safeguard Guidelines can be found here.

Strong parallels exist between the CDR and Digital Identity safeguards with Digital Identity focused on;

- Limiting the collection, use and disclosure of personal information to a narrow purpose
- Minimising retention of information and keeping data stores separate
- Giving Users choice of how they verify their identity
- Giving Users control through consent and transparency

Consultation questions:

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?

22B) What is the optimal structure of a new body?

22A) *Continued*

Security

ACCC has established strong security capabilities for the CDR that are aligned with Digital Identity requirements. Data security requirements are built into the CDR system. Accredited providers must follow strict information security requirements around governance, minimum system controls, testing, monitoring, evaluation and reporting. Generally, they are required to destroy or de-identify your data if it is no longer needed.

Providers must also comply with the Notifiable Data Breaches scheme, including telling the consumer and the Office of the Australian Information Commissioner (OAIC) about any serious data breach.

The minimum information security requirements that accredited data recipients must comply with includes;

1. Have processes in place to limit the risk of inappropriate or unauthorised access to its Consumer Data Right data environment
2. Take steps to secure its network and systems within the data environment.
3. Securely manage information assets within the Consumer Data Right data environment over their lifecycle.
4. Implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the Consumer Data Right data environment in a timely manner.
5. Take steps to limit, prevent, detect and remove malware in regards to its Consumer Data Right data environment.
6. Implement a formal information security training and awareness program for all personnel interacting with Consumer Data Right data.

Again, similarly, security is embedded in the Digital Identity system design. The TDIF includes specific security requirements which Participants must comply with to become and remain accredited. The system is protected by strict security protocols set by the Australian Government and all data is securely encrypted and stored in Australia.

Integrity

The CDR is co-regulated by the ACCC and the OAIC and the Data Standard Body (DSB) are responsible for the creation of the technical standards for the sharing of consumer data. The OAIC are the primary complaints handler under the CDR scheme. The OAIC will have a range of investigative and enforcement powers to handle privacy complaints and carry out other regulatory activities with respect to privacy. The OAIC have released a draft version of the Privacy Safeguard Guidelines.

The ACCC, OAIC and DSB have established processes and capability that are aligned to Digital Identity requirements.

Consultation questions:

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?

22B) What is the optimal structure of a new body?

22B)

Adopting a similar structure to the CDR, Digital Identity requires two key capabilities to successfully and appropriately deliver the intended service and outcomes;

- Policy, compliance and enforcement: Translating rules into Digital Identity policy and developing mechanisms to ensure participants meet their legislative obligations
- Operational Delivery: Plan, design, deliver and run of the solution

The policy, compliance and enforcement capability would resemble the traditional functional vertices structure with separate function for each respective area of scope of the capability (policy, compliance and enforcement). In this structure, each function would work closely together to achieve the end-to-end policy delivery.

The operational delivery capability would comprise of the full spectrum of technical capabilities needed to deliver and support the Digital Identity eco-system. These functions span a typical ITIL Plan, Design, Build, Test, Run lifecycle with Cyber Security embedded across all of the functions and Execution and Realisation supporting the successful delivery of outcomes.

These capabilities are established and exist as part of the CDR division within ACCC. Digital Identity could leverage this structure to accelerate development of the data economy for Australia.

Consultation questions:

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?

25A)

Yes, the roles and functions outlined are appropriate for the Oversight Authority as the traditional BAU functions in addition to the functions already undertaken by the interim Oversight Authority.

These roles and functions are established and successfully operating as part of the CDR. Digital Identity should leverage these to exploit economies of scale, leverage established trust and ultimately expedite the delivery of Digital Identity and the data economy.

25B)

A notable omission from the list relates to driving ecosystem growth, similar to a traditional business development function. The benefits from Digital Identity will be optimised as the volume of data holders and data recipients in the ecosystem increases but most importantly, as consumers/citizens adopt and take up Digital Identity.

For ecosystem participants, it is not enough to rely on legislation to drive adoption of the Digital Identity and instead, effort should be taken to communicate the benefits to participants which will drive behaviours around early adoption and also voluntary adoption to create a thriving ecosystem. Optimal value will be unlocked when participants willingly opt-in to join the Digital Identity and the bigger the ecosystem grows.

With ecosystem participants only representing one side of the transaction, it is important to also focus attention on the end-user in the exchange – the consumer or citizen. Consumer adoption must be driven at the point at which consumers are looking at ‘buying’/entering into a transaction that requires a secure identity. Instead of driving a message from the Government around Digital Identity, it is important to contextualise this message and drive it at the checkout or conversion points and where the benefits will be realised for the end user to achieve the best possible response.