Digital Identity Legislation

Have your say submission
Phase 2

July 2021

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 digital 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 consultation paper approaches Digital Identity as an independent, standalone ecosystem. When considering the Digital Economy, the Consumer Data Right (data sharing) and Digital Identity should be viewed as complementary activities within the same legal and technical ecosystem. With the addition of action and payment initiation functionality to the Consumer Data Right (CDR), the two activities would converge to unlock the true value of the Digital Economy – enabling the provision of streamlined digital processes for consumers.

There is only one digital economy, and to construct discrete legal and technical silos around complementary processes would create unnecessary friction that could impede, rather than assist, the development of Australia's digital economy.

There exists opportunities in Government, such as the CDR, to leverage proven governance, solutions, operations, skillsets and experience to successfully deliver Digital Identity. There is strong overlap between the CDR and the proposed delivery of Digital Identity and leveraging this opportunity will reduce the financial burden on taxpayer funds, increase speed to market and improve accuracy and quality of delivery through experience.

Leveraging the synergies between the CDR and Digital Identity would demonstrate the Australian Public Sectors mandate of national reusability. National reusability is a key guiding principle of the Australian Data and Digital Council (ADDC) where opportunities for reusability are encouraged across people, process and technology of government services.

ACCC's role as a trusted regulator, safeguarding consumers and strengthening competition, its leading class enforcement capability and independence from Digital Identity (i.e. it is not a Digital Identity provider), further support the ACCC as the best candidate to administer Digital Identity.

As a taxpaying Australian, I am motivated to see our Digital Economy flourish so I can benefit from greater competition, increased convenience and innovative products. I am also interested in the optimal delivery of Digital Identity and strongly believe that the ACCC is the best placed Australian government service to administer Digital Identity. Expenditure of taxpayer funds should be considered wisely. Where there exists opportunity for reusability, this should be leveraged, enabling redirection of taxpayer funds to social and new initiatives that do not have the opportunity of re-use.

Governance of the Digital Identity system

There are parallels between the proposed Digital Identity governance structure and the current structure employed to govern the Consumer Data Right (CDR). Aligned to the Australian Data and Digital Council's (ADDC) principle of national reusability, leveraging the parallels between the proposed Digital Identity governance structure and the CDR governance model would be considered a tangible realisation of national reusability.

In the proposed Digital Identity governance structure, there are three key roles that mirror the governance model of the CDR – Minister & Policy Adviser, Information Commissioner and Oversight Authority.

Minister & Policy Adviser
The lead agency role is responsible for the development and issuing of rules under the Bill, running consultation to inform rules design and long term system strategy. The CDR lead agency is Treasury who performs a similar policy and rule making role on the CDR program.

Information Commissioner
The Digital Identity Information Commissioner is focused on designing the privacy and data and information standards. Similarly, on the CDR, the Office of the Australian Information Commissioner and the Data Standards Body provides these standards and design guidance.

Oversight Authority
Provides management/development of the Digital Identity system, rules enforcement, accreditation, on-boarding and security monitoring. The Australian Competition and Consumer Commission (ACCC) is the lead implementation agency for the CDR and provides the same established functions as the proposed Digital Identity Oversight Authority.

The ACCC is familiar with a similar framework for the CDR where Policy, Rules and Standards are set externally and the ACCC plays the implementation, accreditation and enforcement role.
Leveraging an existing proven governance structure will reduce the time and effort required to establish and define the structure and process. The CDR governance structure, or the most relevant parts of it, could potentially be extended to cater for Digital Identity requirements.

Oversight Authority

The consultation paper proposes that there should be a person appointed as an independent Oversight Authority to be responsible for the Digital Identity framework and is suggesting that existing government agencies ‘provide staff to’ the Oversight Authority.

The functions of the Oversight Authority include;

- accreditation of participants
- on-boarding participants
- maintaining a register of accredited entities
- enforcement of legislation and rules
- suspending and terminating participant access
- cyber-security
- incident management
- and a range of incidental functions

The functions required to support Digital Identity align very closely with the functions that the ACCC currently performs for the Consumer Data Right (CDR).

As suggested in the consultation paper, the ACCC is a good candidate for consideration for the role of the Oversight Authority because of their successful role in administering the CDR by leveraging the recent experience of the ACCC in delivery of the CDR which will enable economies of scale by pooling like functions in an already established capability . Whilst appointment of the ACCC to the Oversight Authority will embodies the concept of national reusability, the ACCC is a strong candidate for this role due to their independence, as they do not operate within the Digital Identity system (i.e. the ACCC is not a Digital Identity provider). The ACCC’s role within the Australian economy as a highly reputable regulator, to safeguard consumers and strengthen competition, provides an element of trust that will expedite uptake of Digital Identity.

Align Digital Identity and Action Initiation

A key recommendation from the Inquiry into the future directions of the Consumer Data Right (Farrell review) is the addition of action initiation functionality, similar to the more commonly known write access. Currently the CDR offers read access, facilitating data sharing.

In the CDR, an action initiation framework would give the consumer the ability to consent to providing the Accredited Data Recipient delegation authority over their account to perform “transactions” (being data changes, new product, close and open accounts, etc.) on the consumers behalf.

The position of the paper implies that Digital Identity is treated as an independent, standalone ecosystem. When considering the Digital Economy, the CDR (data sharing) and Digital Identity should be viewed as complementary activities within the same legal and technical ecosystem. With action initiation functionality introduced into this ecosystem, the two activities would converge to unlock the true value of the Digital Economy – enabling the provision of streamlined digital processes for consumers.

Globally, the successful use cases of Digital Identity are limited. In the US, Covid-19 stimulus payments for citizens were issued as physical cheques, which were delivered by mail to the last recorded address for the individual and needed to be deposited into a bank before they could be spent. In India, money was sent directly to citizen’s bank accounts, at the touch of a button with their digital ID system, Aadhaar. What is clear here is, India’s successful use case employs the full Digital Economy offering from a CDR equivalent with action initiation (or payment initiation) and Digital Identity to provide true value to citizens.

These examples highlight the inability to unlock true value for the consumer or citizen if Digital Identity is treated in silo.

Penalties and enforcement

The ACCC has an established and highly successful CDR enforcement function performing the following duties;

- Penalise entities if they do not comply with the legislation and rules
- Provide fair and proportionate penalties for the harm caused
- Establish civil penalties for breaches of privacy safeguards, including unrelated marketing, biometrics and user consent
- Suspension or revoke accreditation and access to systems, and issue directions for remedial action to address a breach

These duties align closely to the enforcement administrative sanctions in the Digital Identity legislation. The demonstrated and established enforcement capability of the CDR, administered by the ACCC, is a function which can potentially be extended and translated for use on Digital Identity.

The ACCC has the responsibility, as a regulator, to deliver consumer safeguards, positioning the ACCC best to perform enforcement activities within the digital economy, where consumers may be susceptible to risk and where intervention is required to strengthen competition.

The ACCC is widely perceived to be one of the most active enforcers in the world and is trusted by consumers and respected by industry. It has a strong history and promised future of enforcement, bringing its legal powers, resources and influence to bear against anticompetitive activity. The ACCC cares about due process, independence, transparency and analytical sophistication and investigating conduct. Beyond enforcement actions, the ACCC advocates against regulations that entrench incumbents and impede new entrants and strives for a consumer-oriented, progressive market.

The ACCC is an experienced and skilled enforcement body whose principles are guided by;

- Regulators do not unnecessarily impede the efficient operation of regulated entities
- Communication with regulated entities is clear, targeted and effective
- Actions undertaken by regulators are proportionate to the regulatory risk being managed
- Compliance and monitoring approaches are streamlined and coordinated
- Regulators are open and transparent in their dealings with regulated entities
- Regulators actively contribute to the continuous improvement of regulatory frameworks

Dispute resolution

Dispute resolution is a topic referenced only once in the consultation paper as a function of the Oversight Authority. There is significant complexity surrounding dispute resolution and this should not be underestimated. A whole-of-economy Digital Identity represents the convergence of a multitude of sectors, each bringing with them governing bodies and the need to accommodate different dispute management frameworks.

The CDR is demonstrating its ability to operate in this complex landscape, working with the differing governing bodies across sectors and regional boundaries through the proposed future introduction of the energy and telecommunications sectors. With these additional sectors, the CDR will need to take into account not only Australian Financial Complaints Authority (AFCA) for banking but the fragmentation across energy by state and the telecommunications ombudsman, all within a single ecosystem. The groundwork completed by CDR could and should be leveraged by Digital Identity to reduce duplication of effort and cost.

Within the CDR ecosystem, the ACCC has an established and effective participant-to-participant IT Service Management (ITSM) dispute resolution model. In the first instance, participants will attempt to resolve disputes between themselves with the option to escalate to ACCC for mediation where required. The ACCC provides the technology solution and has the ability to monitor and intervene in disputes.

This established dispute resolution structure, solution, process and resources will be particularly valuable for Digital Identity to leverage when it comes to identity theft. It will support the investigative activities involved in resolving disputes across the ecosystem.

Consumer safeguards

The ACCCs established consumer safeguard framework is guided by ACCCs purpose of maintaining and promoting competition, protecting the interests and safety of consumers, and supporting fair trading in markets affecting consumers and small business. This purpose aligns strongly with the objectives of the CDR, that in turn aligns to Digital Identity.

There are three key principles of the Digital Identity Legislation that are mirrored in the work conducted on the CDR.

Privacy protection
CDR developed new legislative safeguards to protect the personal information of individuals who engaged in data sharing services. Various safeguards were developed to help make the system accessible.

Building on existing laws
As with the Digtal Identity Legislation, CDR was not intended to duplicate or conflict with established principles in existing legislation. The Legislation was developed in a way that recognises the potential changes being made to broader privacy protections and aims to build consistency to the greatest extent possible. The Digital Identity Legislation will benefit from harnessing the established CDR legislation in reducing red tape for businesses and making it easier for consumers to understand their rights.

Fostering participation and innovation
CDR requires strong consumer and privacy protections that are balanced with the requirement to foster participation in the system, and to enable technological and other forms of innovation as the system grows.

The ACCC's purpose is making markets work for consumers, now and in the future. It should be viewed in the context that competition provides the best incentive for businesses to become more efficient, innovative and flexible and to operate in the long-term interests of consumers.
Where competition is not feasible, effective regulation is required to deliver outcomes in line with those achieved by competitive markets. The ACCC champions strong, efficient and effective markets.

The ACCC provides consumers with the confidence to make the best choice for their circumstances, and work to ensure the long-term interests of all Australian consumers. The ACCC's consumer-oriented framework is well placed to ensure the Digital Identity legislation allows business and consumers to play a growing role in the digital economy.

National reusability

A key guiding principle for the Australian Public Service is national reusability. The concept of national reusability is instilled across the Australian Public Service and seeks to reuse people, process and technology where viable. There is strong public sentiment to effectively use taxpayer dollars and conversely, scrutiny if Government is perceived to be wasting taxpayer dollars. National reusability is clearly outlined in the Australian Data and Digital Council's (ADDC) guiding principles.

The ACCC has successfully delivered the CDR, in a similar capacity to the proposed Digital Identity Oversight Authority. There is a clear and compelling opportunity to demonstrate national reusability across people, process and technology, utilising the ACCC's delivery and operations of the CDR for Digital Identity.

The existing regulatory teams covering Accreditation, Compliance and Enforcement complemented by the Service Delivery and Operations functions of the CDR can be rapidly replicated or extended for Digital Identity needs. The CDR Register and Accreditation Application Platform (RAAP) should be considered as a technology option to support similar requirements for the Digital Identity Participant Register.

There are clear parallels between the ACCC's integral role in the roll out of the CDR and the regulatory, enforcement, delivery and operations requirements for the Digital Identity Oversight Authority. It is also clear that failure to re-use the CDR and leverage ACCC's regulatory and service delivery capability (people, process and technology) contradicts the Australian Public Service mandate for reusability and citizens expectations that their tax dollars will be used effectively. Additionally reuse will expedite speed to market and leveraging the already strong consumer trust of the ACCC will increase uptake.

There is only one digital economy, and to construct discrete legal and technical silos around complementary processes would create unnecessary friction that could impede, rather than assist, the development of Australia's digital economy.

Administration of charges for the Digital Identity system

There are many considerations when designing the Digital Identity charging framework including a wider digital economy approach, reducing expenditure to operate Digital Identity and reducing costs to enter the ecosystem.

Digital economy approach to designing the charging framework
The consultation paper approaches charging only from a Digital Identity perspective however, as outlined on action initiation, page 5, Digital Identity forms an activity within the digital economy. If you take the recommendation on page 5, to approach Digital Identity from a digital economy perspective, the charging framework should consider the role of the Consumer Data Right in streamlined digital processes. A digital economy approach to charging may support use cases for the digital economy as a whole that will unlock the greatest value for Australian businesses and consumers.

Reducing expenditure to operate Digital Identity
Whilst the charging framework is not intended to be used for cost recovery, it is prudent to consider the expenditure to establish and operate Digital Identity and reduce the investment of taxpayer dollars as much as possible, especially when there is a strong case for national reusability with the CDR. Both revenue and expenditure of Digital Identity should be considered together.

Costs to enter the Digital Identity ecosystem
The charging framework needs to be considered from a participant perspective and take into account all set up and establishment costs that a participant may incur to join the Digital Identity. It is important to be empathic and realistic when designing the charging framework to ensure that Digital Identity is a prosperous and viable solution for businesses and encourage adoption. Utilising learnings and already established processes that are being refined for CDR will reduce the cost barriers to entry for participants.