Digital Identity Legislation

Phase 2 Consultation Paper

July 2021

Ashley Diffey
Head of APAC and Japan
Ping Identity

Steve Dillon
Senior Solution Architect
Ping Identity

CONTENTS

Preamble

Much of the content contained in this submission is derived from Ping Identity's experience working with the Australian banking community to implement solutions for the Consumer Data Right.

Originally announced in 2017, the CDR was enacted by the Treasury Laws Amendment (Consumer Data Right) Act 2019 which inserted a new Part IVD into the Competition and Consumer Act 2010.

The CDR gives consumers greater access to and control over their data and improves consumers' ability to compare and switch between products and services. It encourages competition between service providers, leading not only to better prices for customers but also more innovative products and services.

Currently the CDR applies only to the financial sector, however a progressive rollout to the rest of Australia's consumer-centric industries (energy, telecommunications etc) will occur over the coming years.

While the CDR operates in a different space to the proposed digital identity legislation there are similarities and overlaps in technology, regulatory considerations and consumer outcomes. These include:

- Enablement of an efficient, modern digital economy for Australia
- A focus on citizen/customer privacy and empowerment
- A strong dependence on identity standards and practices
- Oversight of the framework by a regulatory body

Given these similarities, we believe there are opportunities to learn from the successes and challenges of the CDR, and use these lessons to improve the approach taken to the digital identity framework. Further, there is also scope to align with the path already forged by the CDR.

Interoperability

Discussion

The CDR is overseen by the ACCC, while the technical specification of the CDR was developed by the CSIRO's Data61 group. The CDR was modelled largely off a similar initiative that came out of the UK: Open Banking.

Where practical, Open Banking is built on existing standards such as OAuth and OpenID Connect. Wherever there is a need to modify or extend existing standards, the Open Banking initiative works with the OpenID Foundation to have the standards amended in a collaborative manner resulting in outcomes that meet their needs while also being open, standards based, and interoperable.

When reviewing the Open Banking specification, the ACCC and Data61 identified various parts of the specification that potentially fell short of expectations for an Australian standard. In these instances, the Australian standard was authored to provide the required functionality in various ways that don't align with existing standards, requiring extensive customisation and integration in order to achieve conformance with the CDR specification.

This has resulted in:

- Additional cost and complexity in an already complex problem space
- High cost to implement for the banking community; particularly for Tier 2 and Tier 3 banks
- Modest adoption of the specification within the fintech space, with five active data recipients at the time of writing, of which two are banks and three are fintechs

Without material uptake from the fintech community, the CDR cannot yield the desired benefits to Australian citizens. Having the CDR specification more stringently based on existing standards would improve vendor support for CDR solutions, and reduce the barrier to implementation for both data holders and data recipients.

Recommendations

Ensure that interoperability with relevant global, open standards is a key responsibility in the charter of the technical body responsible for administering the digital identity specification.

Ensure that collaboration with foreign governments such as NZ, Canada, Singapore, the Philippines, the EU, the UK, and the US is a key responsibility in the charter of the technical body responsible for administering the digital identity specification.

Ensure that participation in relevant standards bodies such as the OpenID Foundation is a key responsibility in the charter of the technical body responsible for administering the digital identity specification.

Ensure that there is a transparent and rigorous exception process where the technical body responsible for administering the digital identity specification identifies a legitimate need to deviate from applicable global, open standards.

This exception process should ensure that deviations from the aforementioned standards are not implemented without verifying that:

1. There is no viable means to deliver the same citizen outcome within an existing standard
2. There is no viable means to deliver the same citizen outcome by working with standards to bodies to either amend an existing standard, or create a new one

Provide a means for the technical body administering the digital identity specification to provide feedback to the relevant regulatory bodies overseeing the requirements. This will be useful in scenarios where minor changes to regulatory requirements could provide the same outcome to citizens without the need to deviate from global, open standards.

Reasoning

The recommendations above are aimed at ensuring the digital identity framework is aligned with international approaches to digital identity, as well as the technical specifications enabling those approaches. This approach is desirable because it:

- Maximises the opportunity for participation in an international or global identity framework if such a possibility emerges in the future
- Encourages vendors to provide solutions facilitating the digital identity framework by minimising or eliminating the need for region specific features that may not justify the cost of development given Australia's relatively small population on a global scale
- Encourages participation from the Australian business community via the ability to implement the digital identity framework using cost effective COTS software rather than expensive custom solutions
- Minimises the likelihood of security issues, implementation difficulties and usability challenges as widely adopted standards are vetted and used by a much larger community
- Ultimately maximises the overall chance of creating a successful, widely adopted ecosystem that delivers value to Australian citizens due to all of the aforementioned benefits

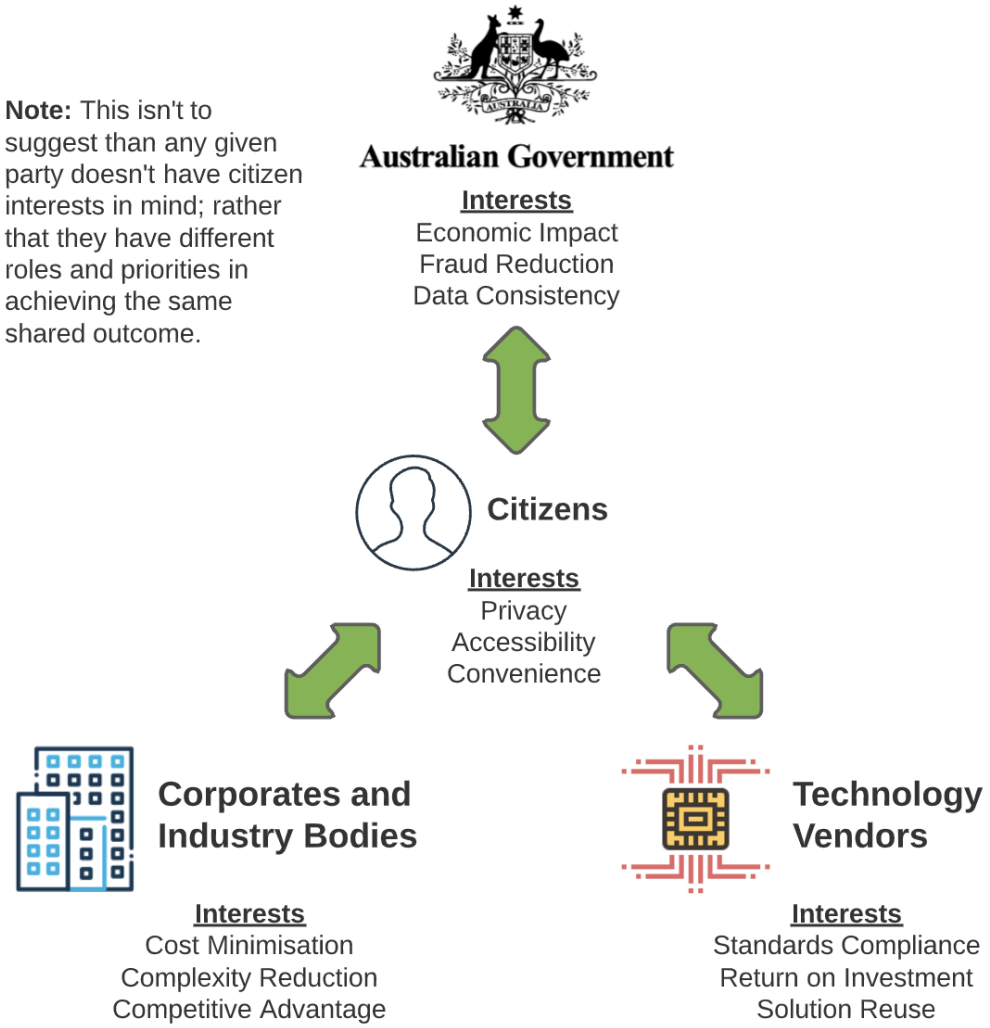
Regulatory Oversight of the System

Discussion

The CDR is overseen by the ACCC, while the technical specification of the CDR was developed by the CSIRO's Data61 group. The ACCC and Data61 recognised the importance of industry consultation, and in June of 2019, they announced a consultation process that would be conducted via GitHub.

While the approach was innovative, much of the feedback offered by both the banking and technology vendor communities wasn't reflected in the technical specification that went into production. This left the aforementioned communities feeling unheard, and led to the cost, complexity and supportability issues outlined in the interoperability section of this document.

It's exceptionally difficult to strike a balance between the various interests of the numerous parties involved in something like the CDR or a digital identity framework. All parties involved typically have valid, tenable positions to offer and reconciling them all is impossible. Introducing highly technical specifications into the mix only further muddies the waters.



Although Data61 is to be commended on their efforts to foster collaboration, unfortunately the magic balance was not found this time around. This shortfall represents an opportunity to improve however. We believe that all parties (including citizens) will benefit from an approach that allows for greater involvement of industry in the decision making process when it comes to technical specifications. To this end, we believe that The Digital Identification and Authentication Council of Canada (DIACC) could serve as a useful model to reference in how the overseeing body engages with industry.

Further to this, given the overlapping problem space and aligned technologies, we believe there is opportunity to consolidate (to some extent), oversight of the CDR and digital identity specifications. Specifically, it appears likely that the CDR will eventually adopt the OIDC FAPI 2.0 standard for authentication and grant management. This standard is potentially also applicable to the digital identity framework as are upcoming standards that build on FAPI 2.0 such eKYC.

Recommendations

Maintain separate oversight of the CDR and digital identity regulations (presumably via the ACCC and DTA respectively), but ensure a single technical body manages specifications across both CDR and digital identity with a view to achieving consistency, reusability and interoperability.

Ensure the aforementioned technical body allows not just for industry consultation, but for industry participation (similar to the model implemented by DIACC) to ensure that technical requirements are viable for Australian businesses and technology vendors while still facilitating citizen outcomes mandated by the government.

Reasoning

The oversight model outlined above provides separation between the outcomes necessary for citizens, and the technical details required to facilitate those outcomes. So while the government would be yielding some control of the technical specifications, full control of the overarching regulations that guide those specifications is retained.

Inviting full participation from relevant corporates, industry bodies and technology vendors will drive adoption by:

- Allowing high profile Australian businesses and state governments to participate in the process, and implement digital identity solutions that they were instrumental in defining
- Promoting standards compliance making it more feasible for global identity vendors to provide Australian companies with reusable, low cost solutions for consumption and provision of services under the digital identity framework
- Making it more cost effective for the broader Australian business community to consume the digital identity framework via the aforementioned reusable, low cost vendor solutions

About Ping Identity

At Ping Identity, we champion the unique identity needs of enterprises and simplify how they deliver secure and seamless digital experiences for their workforce and customers. We help prevent security breaches, increase productivity and deliver personalized experiences.