BCA

Business Council of Australia

Digital Identity

October 2023

Contents

1. Overview

The Business Council of Australia supports the government implementing an economy-wide digital identity system.

Properly set up, the digital identity system will be fundamental to lifting privacy across Australia – providing government and businesses a way to positively identify an individual without requiring the collection of personally identifiable information. It will also be a critical enabler for a modern seamless economy. It will make it easier for Australians to verify who they are without having to manage a cumbersome set of cards or numbers.

Following recent criminal attacks on Australian businesses, it has become clear reform is needed. As it stands, Australians currently have little choice but to use documents like passports and driver's licences to establish their identity. Businesses and governments are required – often by legislation – to collect and hold this information.

Australia must move beyond this. Digital identity will be a chance to lift privacy outcomes while making it simpler, easier, and safer for Australians to prove who they are.

A federated digital identity model will ensure Australians can choose how they prove who they are online, without relying on a single government or business authority. This will reduce the amount of personal information that businesses or governments have access to about Australians. By removing the need for businesses to hold personal documents, it will limit the number of copies of documents that need to be provided and stored – reducing the risk of criminals getting hold of them. Moreover, a federated model will ensure that no single authority – including government – can remove the ability of Australians to prove who they are online.

For Australia to fully reap the benefits, Government must set out a clear timeline for when businesses and citizens can expect to use digital identity in the private sector, not just for government services.

This must also be combined with an urgent review of all legal provisions requiring retention of personal information, with reform aimed at not only harmonisation of the requirements but also enabling digital identity in place of identity documents.

This legislation also comes at a key time for cyber and privacy, with the recent government response to the Privacy Act Review and the coming Cyber Security Strategy. Ensuring trust and confidence in the system will be critical, and we support government measures that enable this – both for digital identity providers and users. However, any requirements should not create unnecessary or conflicting requirements with domestic or international laws.

While the digital identity legislation has been under development for some time, it is likely that it will require refinement and improvement as the system rolls out. We support the inclusion of a review undertaken two years after the commencement of the Act. But Government will also need to continuously be examining whether the system remains resilient to new technologies or innovations.

2. Key recommendations

The Business Council recommends:

1. The government implement an economy-wide digital identity system that enables businesses to positively identify an individual (or relevant attributes about an individual).
2. Government prioritise and set out a clear timeline for private sector access to and use of digital identity, particularly to meet legislative requirements to positively identify individuals.
3. The review of all legal provisions requiring retention of personal information be undertaken as a matter of urgency, with opportunities for digital identity to be used to reduce the identity documents organisations are required to collect.

4. That section 73 of the exposure draft be removed or revised. Instead, government should work with digital identity providers and sectoral regulators to provide guidance on appropriate cyber security settings relevant to the digital identity ecosystem.
5. Government align any guidance or requirements imposed either by legislation or subordinate rules with international standards, such as ISO or NIST standards.

3. A truly national digital identity system

The government proposes rolling out the digital identity program across four phases, initially focusing on the use of digital identity in Commonwealth and state and territory services before private sector services and providers.

We support an orderly rollout of the system, particularly one that enables businesses and other organisations to verify Australian's identity (or a specific attribute, such as being an appropriate age to purchase liquor) without needing to collect or hold personal information. To this end, it will be critical that clear timelines are set out for private sector access to and use of digital identity for some government services (phases 3 and 4). One of the key benefits for all citizens will come when industry does not need or have obligations to use and retain full identity documentation for their activities and functions.

For example, airlines need to hold onto certain passport data in the context of sharing advanced passenger information with various government agencies for immigration and border security purposes. Use of a digital identity token could streamline passenger movement and improve aviation security (including data security) outcomes, while minimising the amount of personal information aviation providers need to hold.

Moving beyond the current system to use systems like digital identity would align with the outcomes government has set out as part of the Aviation Green Paper, which states that government agencies and businesses must work together "to better anticipate and manage risks at the border, to reduce the number of touchpoints for passengers, and move to contactless processes where possible". The Green Paper references the need to "move to contactless processes where possible". Use of the Digital ID system for identity tokens from booking to boarding (that is, beyond initial online applications and transactions) could streamline passenger movement and improve aviation security (including data security) outcomes.

We recommend government prioritise and set out a clear timeline for phases 3 and 4.

4. Improving privacy outcomes

Government must look where further legislative change is required to reduce the identity documents organisations are required to collect.

As part of the Privacy Act Review government response, the Commonwealth has agreed-in-principle to the importance of undertaking a review of all legal provisions requiring retention of personal information, subject to further consultation across the Commonwealth and with states and territories to determine the appropriate scope and scale of a review. This review must not be delayed.

Businesses and other organisations are required to hold substantial volumes of information by a wide range of regulations set by all layers of government.

Many sectors are similarly required to collect and hold information, including requirements under the Telecommunications Act (including for metadata retention requirements and customer identity authentication rules set by the Australian Communications and Media Authority). Similar rules are in place for other industries, such as for the financial sector and some parts of the health sector.

Many of these laws have been in place for decades, often without review or modernisation to reflect new technologies. The complex web of data retention laws has been put in place by both the Commonwealth and state/territory governments, and apply across many sectors in Australia.

Digital identity provides an opportunity to reduce these requirements dramatically. Legislative and regulatory change through this audit will be critical. Changes need to enable organisations to meet government requirements through the digital identity system. Without these changes the digital identity system will be unsuccessful.

5. Data localisation requirements

Section 73 of the exposure draft legislation allow the digital identity rules to make provisions in relation to information held, stored, handled, or transferred outside Australia. This may have the implication that government would seek to impose data localisation requirements on entities participating in the digital identity system. The Business Council does not support data localisation requirements and we recommend government remove this section of the legislation.

Data localisation requirements prevent businesses from accessing the latest security capabilities offered by global businesses. Despite the argument being made that holding data locally is more secure, this is not the fact and is more an emotional than a practical or technical response. Access to the security capabilities and timely threat intelligence offered by globally scaled cloud service providers will be critical to ensuring the integrity of the digital identity system. A local siloed system risks limiting the capabilities of digital identity service providers, who may face challenges accessing global cyber security solutions. A more nuanced approach is needed.

The government has stated its commitment to the free flow of information, including as recently as in the government's response to the Privacy Act Review, which noted the government is working towards 'supporting the free flow of information with appropriate protections'. This was also supported in the government's Digital Trade Strategy.

Instead of imposing data localisation requirements, the government should instead work with digital identity providers and sectoral regulators to provide guidance on appropriate cyber security settings relevant to the digital identity ecosystem.

6. International and domestic harmonisation

The legislation includes additional privacy and security obligations on entities in the digital identity system, including on tracking, the collection of information on certain sensitive attributes, and reporting of data breaches.

As discussed earlier, part of the challenge all businesses are facing is the wide range of requirements imposed under many different pieces of legislation. The ongoing reforms to the Privacy Act also create additional uncertainty. Rather than creating an additional layer of bespoke regulation for the digital identity system, government should consider whether references to existing internationally recognised standards would meet the policy outcomes.

We recommend government consider whether standards such as ISO 27001 or as set out by NIST may meet the policy outcome without creating additional unnecessary regulatory impost. These standards are well recognised by businesses and will help deliver privacy and security outcomes without creating unnecessary regulatory burdens that would limit uptake and use.

BUSINESS COUNCIL OF AUSTRALIA

GPO Box 1472, Melbourne 3001 T 03 8664 2664 F 03 8664 2666 www.bca.com.au