29 January 2024

Tech Council Submission to the Senate Economics Legislation Committee Inquiry into the *Digital ID Bill 2023* and the *Digital ID (Transitional and Consequential Provisions) Bill 2023*

Thank you for the opportunity to make a submission to the inquiry into the *Digital ID Bill 2023* and the *Digital ID (Transitional and Consequential Provisions) Bill 2023*.

The Tech Council of Australia (TCA) is Australia's peak industry body for the tech sector. The tech sector is a key pillar of the Australian economy, employing over 935,000 people. This makes the tech sector equivalent to Australia's seventh largest employing sector. The TCA represents a diverse cross-section of Australia's tech sector, including startups, scale-ups, venture capital funds and global tech companies, with many of our member companies involved in providing or supporting digital ID services.

The TCA has long supported the development of legislation to create a secure, convenient, interoperable and inclusive digital ID system in Australia. In an era of unprecedented digital connectivity, with an increasing number of transactions and interactions taking place online, digital IDs are a cornerstone for the integrity of digital economies – helping to boost productivity, improve citizen experience and enhance security and privacy in a time of increasing cyber attacks, scams and data breaches. Building trust and confidence will be key to driving the uptake of digital identity by Australians and realising these benefits. The proposed legislative framework is central to achieving this.

The TCA has engaged closely with the Government on the development of these Bills. We have formed a multidisciplinary expert group comprised of individuals and companies with digital ID expertise from Australia and abroad, to help identify key design and implementation features to enable our national legislative framework to be fit-for-purpose. We support the final Bills and strongly encourage their passage through the Parliament.

Our submission:

1. Offers evidence in support of the benefits of digital identities
2. Outlines our reasons for supporting the Bills
3. Highlights key issues that need to be addressed in rollout and implementation

1. The importance of digital ID in the modern economy

Digital ID is critical for unlocking a myriad of benefits for government, citizens and the broader economy. We categorise these benefits across three key areas:

Supporting productivity and innovation

Digital ID offers considerable potential to boost productivity at a time where Australia's productivity growth is at a 60-year low. For organisations and individuals, digital IDs improve cost savings by reducing the time and costs associated with manual identity verification, which includes tasks like physically scanning identity documents, certification of primary documents, mailing by post, human-processing of documents, as well as the number of related support calls throughout. The streamlining of verification allows for those resources to be redirected to more productive business processes, operations, or value-added tasks.

Digital ID also offers productivity gains for online services, as individuals no longer need multiple logins to access different services, and service providers can more confidently and securely verify identity without needing to collect and store sensitive information such as driver's licence and passport numbers.

The Productivity Commission has recognised the broad benefits of Digital ID in its recent 5-year productivity inquiry, and recommended expanded use of Digital ID across governments and the private sector.[1]

There is also a broader innovation opportunity to develop our local digital ID ecosystem which presents an opportunity for economic growth by fostering Australian entrepreneurs and startups, while also encouraging foreign investment. The global digital ID market was valued at $42.5 billion in 2022 and is expected to grow to over $125.9 billion by 2028.[2] Australia has an opportunity to capture more of this emerging market.

Enhancing citizen and customer experience

By providing a seamless and secure method of identity verification, digital ID enables smoother and more efficient customer onboarding processes while also enhancing overall citizen and customer experience. Instead of the need to manage a plethora of multiple different identity accounts and passwords, digital IDs enable identity credentials to be re-used across different sites and organisations. Once authenticated, users can selectively use the same identity credentials to access a myriad of affiliated platforms and services more efficiently. Not only does this reduce the time and effort required from both customers and businesses, but also fosters more positive and frictionless digital interactions online.

There are a number of practical use cases for Digital IDs for example:

- in financing and loan services where applicants can save time on manual and time-consuming processes to gather, certify, and submit multiple identity documents, and financial institutions can help reduce identity fraud;
- in emergency services by providing efficient and secure access to first responders, and for those seeking disaster relief where documents may be lost due to flood or fire, to verify identity and eligibility, reducing administrative government agencies, minimising the risk of fraud, and ensuring that essential services reach the intended recipients in a timely and targeted manner;
- in real estate by providing prospective tenants with an easier and more secure method to confirm their identity across multiple rental property applications, without their sensitive identity information having to be collected and stored.

Uplifting national cyber security and supporting privacy

The adoption of Digital ID across the economy can play a crucial role in uplifting cyber security and privacy, supporting broader public policy goals and reform processes (such as the 2023-2030 Australian Cyber Security Strategy and the Privacy Act reform process). Digital IDs can enhance privacy by enabling individual greater control over their personal data. Traditional identification processes often require individuals to share more information than necessary for a particular transaction or service. For example, to verify

[1] See Recommendation 4.2, Productivity Commission (2023), 5-year Productivity Inquiry: Australia's data and digital dividend, Vol. 4, Inquiry Report no. 100
[2] Statistica Research, November 23, 2023

one's age, individuals are often required to provide all information available on their driver's license, which includes personal home addresses and date of birth. The introduction of digital ID would enable the sharing of selectively relevant information, such as verified age alone, rather than all datapoints that can be found on a single identity.

From a cyber perspective, reducing the volume of identity documents collected by organisations can help mitigate the risk of data breaches and unauthorised access, by minimising the attack surface for cyber criminals. When citizens use secure digital ID to access services, the need for organisations to collect and retain copies of documents with personal information, or copies of other identification data, is minimised. This is fortified by requirements for digital ID services themselves to incorporate enhanced security measures to reduce the risk of identity theft and fraud. This ensures a higher level of confidence in the authenticity of an identity.

Taken together, these measures create a more secure environment for digital interactions that help increase safeguards for businesses and individuals from harms associated with scams, fraud and cyber attacks.

2. Tech Council support for the Digital ID Bills

Recommendation 1: Support passage of the Bills in their current form.

The *Digital ID Bill 2023* and the *Digital ID (Transitional and Consequential Provisions) Bill 2023* will be crucial to realising the benefits of digital IDs by creating a robust legislative framework that builds trust in the digital ID system and providers and ultimately drives uptake across government and private sector services.

We have no major concerns with the legislation and strongly encourage the passage of these Bills. In particular, we welcome:

- The intended national coverage of the proposed legislation, which will ensure a comprehensive and consistent approach across the country;
- Protections to support consumer choice and voluntary uptake of digital ID;
- Requirements for interoperability with existing identity verification services and existing state-based ID services, such as in New South Wales;
- The creation of a voluntary accreditation scheme, which will help build trust in private providers and enable innovation opportunities;
- Expansion of the Australian Government Digital ID System, including enabling the integration of private sector digital IDs (albeit, we have some concerns regarding the proposed phasing of this rollout, which we outline further below).
- Emphasis on strong cyber and privacy obligations – for example, we support the additional safeguards to prevent personal information being collected, profiled, used or sold for other purposes, such as direct marketing;
- Establishment of appropriate safeguards for law enforcement access;
- Clear oversight and governance arrangements, with the ACCC as the initial Digital ID regulator;
- Tough penalties and compliance/enforcement measures to prevent against bad actors that could undermine consumer trust in the overall system.

Our main recommendations relate to implementation, which are outlined below.

3. Recommendations on implementation and rollout

While we firmly support the passage of the Digital ID Bills, we have highlighted some additional practical matters relating to implementation (including on the Digital ID Rules and the Digital ID Accreditation Rules) to bring to the Committee's attention. We believe these matters may be appropriate for the Committee to consider in its report, but importantly, do not affect the content of the primary legislation.

Recommendation 2: Provide greater clarity on the proposed timing of the phased expansion of the Australian Government Digital ID System and ensure swift integration of private providers

Competition and consumer choice is an important principle underpinning the Digital ID legislation. The Bill provides the capacity in the future for Australians to use their accredited private sector Digital IDs to access government services participating in the Australian Government Digital ID System.

We support this proposed expansion, noting private sector digital ID providers play a critical role in the national digital ID system, including by introducing innovative new products, services and technologies to the digital ID market which can improve economic activity, productivity and consumer experience.

However, we are concerned about the timing of the proposed phasing of the expansion, whereby private providers would not be integrated into the Australian Government system until “phase 4” at an unspecified time.

To maintain a fair competitive landscape and offer consumer choice, private providers should be quickly granted the same access and opportunities to the Australian Government Digital ID System as their public sector counterparts, contingent upon meeting equivalent accreditation requirements.

The current lack of clarity regarding the timing of these rollout phases poses a challenge for private sector planning and industry preparedness, and could also put private providers at a competitive disadvantage to public sector providers. A timely rollout schedule underpinned by transparent communication is crucial for private sector entities to strategically align their preparations with the phased implementation of the national digital ID system. By doing so, Australians would benefit from a wider array of choices, and private providers can contribute to a more robust and competitive digital identity landscape, ultimately enhancing the overall efficacy of our national digital ID system.

Recommendation 3: Ensure the national digital ID system and accreditation rules are technology-neutral, outcomes-focused, and robust to technological change

Innovation in digital ID is increasingly rapidly, with innovators exploring new approaches. For instance, decentralised ID uses cryptography and digital wallets to enable multiple entities to contribute credentials and empower individuals to manage their data.[3]

To that end, it is critical that the national digital ID system and the accreditation rules are adaptable to technological changes and the changing needs and expectations of the community. It should also take an outcomes-focused, not technology prescriptive

[3] World Economic Forum, Reimagining Digital ID, 2023

approach. This will help ensure Australia has a modern, innovative and competitive digital ID system that provides individuals and businesses with the best possible service while promoting trust in the system.

For example, while Electronic Data Interchange (EDI) validation via the Government's Document Verification Services system is currently the key underpinning of the digital ID system, there are other available and emerging technology options. We recommend digital ID requirements be designed and implemented in a way that is future-proof and does note prescribe or preclude specific technology options.

Recommendation 4: Better align record keeping, incident reporting and data storage requirements with the Government's broader privacy and cyber security agenda

Data retention and record keeping requirements

Retention of data can elevate cyber security and data breach risks. This means that is essential for any requirements to retain data to balance both the benefits and the risks.

The draft Digital ID Rules sets out a requirement that accredited entities whose approval has been revoked need to retain records for three years after the record was created or last used (as reflected in Section 22(2)(b)(i) of the Rules). In the circumstance that an entities' accreditation is revoked, we believe it would likely not be appropriate that they retain these kinds of records.

We have recommended removing this requirement and adding a requirement that ensures any records they may hold are securely transferred to the most appropriate entity, with the Digital ID Regulator or other government entity being the final 'backup' option

Reportable cyber / data breach incidents

Ensuring the cyber security of the Digital ID system is imperative and this will be best supported by ensuring best practice regulation is adopted. Following a cyber incident, there is an overwhelming volume of reporting and investigation requirements which can often put unnecessary pressure on an organisation's operational response, which is focused on understanding and minimising the impact of the cyber incident.

The Australian Government, via the Australian Cyber Security Centre (ACSC), currently requires entities responsible for critical infrastructure assets to report incidents within 72 hours. The Government's Privacy Act reforms are also proposing a 72 hour period for reporting data breaches. The Digital ID Rules, by contrast, propose a considerably shorter 24 hour period in Part 4 Section 12(5). There is also a considerable breadth of information required as part of that reporting.

We recommend changes to the Digital ID Rules to:

- Extend the notification period to align with the 72 hour period currently in place for entities responsible for critical infrastructure assets.
- Align all reporting requirements relating to cyber security incidents with the practices being developed through the National Cyber Security Coordinator to ensure best practice is adopted in these Rules.

Encourage safe and secure data flows through entity accreditation, not data localisation

We strongly support the Digital ID Rules and Accreditation Rules prioritising measures that support data security within the Digital ID system. This is in line with the broader cybersecurity uplift that is occurring in Australia through the Cyber Security Strategy 2023-2030, with the Digital ID an important component of that the uplift.

However, the requirement to localise data in Part 3 Section 10(3) of the Digital ID Rules runs contrary to this objective. Data localisation is based on the misconception that cybersecurity risk is dependent on physical location. However, the main determinants of cyber-resilience are technical, such as strong encryption measures and infrastructure protection, and governance-related such as capability trainings and organisational security protocols. Weaknesses in these aspects can expose users to risks irrespective of the location of data.

We note that the Cyber and Infrastructure Security Centre's advice on offshoring of data to critical infrastructure entities under the SOCI Act, for example, does not require data localisation by default. It instead sets out a range of risk-based mitigation measures that can be followed.

Recommendation 5: Prioritise digital credentials as part of the phased rollout of the national digital ID system

Digital Credentials are interconnected with Digital IDs in that they both play a role in modern identity management. While a digital ID establishes the foundation for verifying an individual's identity in the digital realm, digital credentials serve as the specific attributes or qualifications associated with that identity. They help verify individuals' identity as well as their qualifications, skills and achievements, which can be used to determine permission and access to different services, systems and opportunities. The innovation opportunity for digital IDs are also found in growing a parallel credentialling ecosystem.

For example, digital credentials support innovation in a range of areas, particularly in education and training. They promote credential transparency which helps employers better identify candidates with the right skills and experiences they need. They promote credential portability and recognition of past credentials and experiences. This helps support workers to change jobs and pursue new work and study opportunities. They also promote personalised learning by helping educators and trainers to create personalised learning paths based on a learner's prior achievements and qualifications.

The Bill affords the option to extend the digital ID system to include credentials through the powers given to the Minister to include other services, as detailed in Section 60 of the Digital ID Bill. We would recommend prioritising this work as soon as possible and engaging with industry on feasible timelines. Through leveraging tried-and-tested solutions from industry, we could bring forward the inclusion of digital credentials in a safe, secure and useful manner sooner than may otherwise be possible.

Summary of Tech Council recommendations:

1. Support passage of the Bills in their current form.
2. Provide greater clarity on the proposed timing of the phased expansion of the Australian Government Digital ID System and ensure swift integration of private providers.
3. Ensure the national digital ID system and accreditation rules are technology-neutral, outcomes-focused, and robust to technological change.

4. Better align record keeping, incident reporting and data storage requirements with the Government's broader privacy and cyber security agenda.

5. Prioritise digital credentials as part of the phased rollout of the national digital ID system.

We appreciate the opportunity to make a submission and look forward to ongoing dialogue.