Australian Chamber of Commerce and Industry

2023 Digital ID Bill and Rules

Submission to the Department of Finance
October 2023

Introduction

ACCI welcomes the opportunity to provide feedback on the 2023 Digital ID Bill and Rules submission.

Overall, ACCI is supportive of the proposed Digital ID system and believes that with a well-considered and phased rollout plan, customers, suppliers, and the broader community can positively benefit from its implementation.

Specifically, ACCI and our members recognise the potential for the Digital ID to significantly reduce the administrative and compliance burden of storing and verifying personal information and the associated risks with data leaks and privacy. Barriers to the successful adoption of this technology includes lack of public trust in government ID related apps, the potential for confusing communication strategies targeted at different stakeholders across different stages of the rollout, and poor coordination with parallel legislative reviews, primarily the Privacy Act.

Small business transition to the digital ID system

Appropriate definitions

ACCI has always advocated for a consistent definition of 'small business' across all government bodies. ACCI acknowledges that the exposure draft refers to the Privacy Act definition and notes that this definition may change/need to be changed when further reforms to the Privacy Act with regards to the small business exemption are made. ACCI urges the government to keep a close eye on this and consult with industry again before phase three is rolled out to avoid unnecessary confusion.

Targeted transition support for SMEs

The government needs to have a clear plan along with support measures and guidance for smaller businesses who will seek to transition their own internal systems to recognise the benefits of the digital ID app. Such as instances where consumers (including employees) wish to use their Digital ID app to provide personal data verification, but employers and businesses do not have the appropriate internal systems set up to recognise it. Unlike with previous transitions to new ID apps where there has been a central agency in charge of the app and a central contact point, the piecemeal rollout and variety of accredited providers will mean information is decentralised. This will potentially make it more difficult to onboard smaller businesses without a targeted communications and support plan.

Phased rollout

ACCI is supportive of the government expanding the system in phases and notes that a round of consultation is recommended after each phase concludes. This is most important after the first phase when most gaps (especially security related) will be exposed. Consultation with industry will help to plug those gaps and other teething issues prior to its release to the general public.

Trust in government systems

Significant efforts should be made early in the process to address perceptions of poor data governance by government agencies and decreasing trust in the security of systems handling of sensitive digital information.

Statistics from Webber Insurance shows that 14 of the 44 recorded data breaches between January to June this year were reported by government authorities. These included the Department of Home Affairs, and the Northern Territory, Tasmania, ACT and NSW governments. This is on top of data breaches involving ATO, National Disability Insurance Scheme and MyGov, as reported by the ABC last year.

In 2021, an Office of the Australian Information Commissioner (OAIC) report showed that only 71 per cent of government agencies identified an incident within 30 days of it occurring, and 65 per cent took longer than a month to report an incident after becoming aware of it.

Given that the Privacy Act does not cover some local, state and territory government agencies including state and territory public sector health service providers, it has not been possible to get a number on how many government data breaches have occurred. Additionally, it has not been possible to ascertain how the overlapping legislations and loopholes will interact with the Digital ID system's notification protocols.

Another concern raised by people has been that the Digital ID system is being set up primarily for the purpose of greater government surveillance. This is following the changes made to the Surveillance Legislation Amendment (Identify and Disrupt) Act in 2021 potentially allowing the government to track users' location among other things. Linking all existing systems into one that is government run will pressure people into 'consenting' to giving the government complete access to all personal identification data. To garner and maintain public trust, the government will need to ensure system integrity, and transparency in motivation and method to get more people and entities to voluntarily use the Digital ID scheme.

Trust in the system is the driving force to ensure that businesses get accredited, and consumers use the app. This is especially applicable to small businesses who will only get involved once there is clear evidence that the system works safely, is easy to adopt (lower administrative burden), accessible and reliable, and not unnecessarily compliance heavy and expensive, alongside their desire to hold less data that makes them prone to attacks.

The government will need to have a strong communications campaign for consumers and businesses to get re-educated on just how much information they need to/should collect/store and the associated risks, and what/if there are any safer alternatives. At the moment more information is sold to them as a 'good marketing advantage' but the risks are not properly explained.

Competency and oversight for accredited providers

In the initial roll out, it will primarily be government agencies and APS staff who oversee the linking of the current data stored across various government systems and the implementation of the broader Digital ID system. Given that human error is the main cause of most notified data breaches, the government must ensure that adequate training, internal oversight, and verification is mandated and prioritised by those working on this project.

Securing the system seen as a honeypot for hackers

Cyber security costs the government almost $50 billion annually. While a Digital ID system creates a sense of hope in reducing these costs, consolidating existing identification systems into one will create an enticing 'honeypot' for cyber and data hackers and even the tiniest breach would cost substantially more with greater longer-term repercussions. Thus, securing this system should be the government's number one priority.

The case for digital literacy and public awareness is an important one here. Even if the government manages to provide the most secure app to consumers, the proposed scheme will only be as secure as the phone. Trustmarks will not be enough. Clear messaging on what the Digital ID system is, how it can be used, the importance of choice alongside the significance of installing Multi-factor Authentication (MFA) and strong passwords will ensure that consumers have all the information they need to trust and fully benefit from this system.

Cyber security incident reporting

The need for streamlined functioning is not limited to just government systems. In our submission on the Australian Cyber Security Strategy Discussion Paper, ACCI noted that the current cyber security obligations are already confusing and difficult to follow, and we encouraged the government to simplify what is at present a complicated web of interconnected legislation and department responsibilities. Our members have stated that there is a perception of "buck-passing" between various businesses and law enforcement, state, and government agencies resulting in confusion within the industry on the appropriate government contact for various cyber security concerns. ACCI notes that businesses of all sizes prefer a centralised platform for incident reporting.

That said, ACCI has the following issues with Part 4 (12) Cyber security incidents of the Digital ID Rules 2024. The creation of yet another regulator as a separate contact point is not supported by industry.

The National Office for Cyber Security along with the Australian Cyber Security Centre (ACSC) should always be the government contact for industry and they should be responsible for notifying other internal agencies such as the Digital ID Regulator in this case.

This scheme also proposes a notification process for data breaches. However, we note that the obligations and timelines differ to the existing Notifiable Data Breaches (NDB) Scheme. Conscious of the highly sensitive nature and risk level of Digital ID, ACCI recommends that the 24-hour cap first be tested in either just phase one or phases one and two (strictly limited to government entities) to get an initial reading on whether this is a realistic timeframe. If successful, it will boost public confidence and trust in the government. However, if agencies are consistently failing to notify in this period it will become clear than it is an unrealistic expectation prior to the roll out to industry. The period between phases two and three will provide opportunity to then come up with a more suitable timeframe that achieves the same objectives and works for all entities involved.

Clear justifications for any differences in obligations and timelines in comparison to the NDB needs to be clearly articulated in the Digital ID Rules to provide clarity and avoid future compliance complications.

Next steps

ACCI urges the government to conduct a thorough analysis of lessons learnt after each phase, followed by a round of consultation to scope out areas of improvement. This is especially important before phase three is rolled out. Based on the proposed phased approach, ACCI along with the state and territory chambers is well placed to facilitate discussions on Digital ID given our large and diverse membership base of industry associations across various sectors and businesses of all sizes across the country. Looping in peak bodies early and throughout the process to assist with troubleshooting and messaging will ensure the system is airtight and fit-for-purpose for public and private alike.

We thank you for your consideration of our feedback. Should you require any additional information or clarification of any points contained within, please contact Jennifer Low, Director Health, Safety, Resilience and Digital Policy at jennifer.low@acci.com.au or Tanya Roy, Policy Adviser Health, Safety, Resilience and Digital Policy at tanya.roy@acci.com.au.

Telephone 02 6270 8000 | Email info@acci.com.au | Website www.acci.com.au
Media enquiries: Telephone 02 6270 8020 | Email media@acci.com.au