[redacted]

27 October 2021

Submission in opposition to the Introduction of the Trusted Digital identity Bill 2021

I strongly oppose the introduction of a comprehensive digital identity system. Rather, it is my view that Option 1: status quo identified in the Regulation Impact Statement is the preferred approach.

Fundamentally, I do not accept the premise that there is **any** necessity for providing a centralised platform for verification of identity of individuals in online transactions nor does any purported benefits from the adoption of such a system outweigh the considerable and serious risks that such a system would introduce.

Far from enhancing privacy protections, such a system introduced by this Bill would increase the risk of unauthorised access to data, the likelihood of breach of privacy and fails to provide any access to financial redress for individuals who are harmed by such breaches.

In summary, my reasons for objecting to this legislation are as follows:

Centralisation increases the risks of data breach and unauthorised use of information

- We, as an Australian nation, have been successfully transacting online for over 20 years. The decentralisation of identity systems is helpful in minimising online fraud; hackers and others with malicious intent may access one system in a decentralised model, but cannot do so across the industry. By centralising identification verification and personal information, this will arguably make it easier for hackers and malware to access a broader spectrum of personal information.

- The nature of the system, in collating information and using that information across a variety of participants, would inherently increase the risk of data breach and loss of privacy for users in the system. Any errors in the system would also increase risks for individuals; individual users of the system could be 'locked out' of services if there is any error regarding the identification of an individual or the deactivation of an individual's access to the Digital Identity system.

  We have ample evidence of data breaches across many industries and centralising personal information with the provision of access to more participants, would make this inherent risk exponentially worse. Irrespective of the level of privacy protections or safeguards built into the legislation, centralisation of personal information would greatly increase the risk arising from any data breach and the likelihood of unauthorised access to personal data. This is conceded in the Bill which requires 'accredited entities' to contact people if there is a 'digital identify fraud incident' or 'cyber security incident' affecting them.

[redacted]

[redacted]

- There is reference to situations where verifying the identity of an individual will require express consent of the individual to disclosure of an attribute by an accredited entity[1]. However, it is unclear in what other circumstances the information could be accessed and what mechanisms will be in place to prevent unauthorised access to information collected by one accredited or participating entity by other entities, including government bodies.

  For instance, the Bill prohibits accredited entities from disclosing a person's digital identity information for marketing purposes unrelated to the digital services they provide to the user. Even where such activities are prohibited, we have experience from social media that, despite regulations and privacy laws, data breaches nevertheless occur. Large digital platforms such as Facebook have been found to be inappropriately sharing user personal information[2] and 533m users were more recently affected by data breaches[3]. The RIS itself suggests the use of private information; the Digital Identity system will have "capability to capture historical interactions with FinTech entities and profile spending habits"[4].

Greater compliance costs for businesses

- In order to achieve accreditation under the Trusted Digital Identity system, entities are required to undertake functional fraud control requirements, including appointing a digital identity fraud controller and a designated privacy officer as well as conducting annual assessments. This process will lead to greater compliance costs for business, with the added threat of the imposition of further penalties under this Bill for any non-compliance. It is reasonable to assume that only larger businesses will have the financial resources to perform all the requirements imposed by the Bill, which will further limit the competitiveness of smaller and medium sized businesses in the digital economy. The government is also developing a charging framework to charge for the cost of this unnecessary operation.

  The Regulation Impact Statement ("RIS") concedes that the legislation will impose costs on entities, but considers these costs to be minimal relative to the benefits of the Bill. At a time when small and medium businesses in Australia have been financially crippled by the lockdown measures, further regulation and cost will impact on the viability of their businesses; these 'minimal costs' could be the final straw for businesses.

No increased redress for individuals who have suffered a breach

- Currently, businesses are responsible for protecting consumer and individual privacy and there is Commonwealth legislation which holds businesses accountable for cyber security breaches. Businesses can be sued by individuals for breach of these obligations. This accountability framework has been working successfully to ensure that businesses invest in appropriate cyber security platforms for digital transactions and obtain insurance to provide

[1] Sections 73 and 74 of the Bill.
[2] Information shared with Cambridge Analytica resulted in a US$5bn fine for Facebook: https://www.dw.com/en/facebook-faces-5-billion-fine-over-privacy-violations/a-49575702
[3] https://www.theguardian.com/technology/2021/apr/06/facebook-breach-data-leak
[4] page 23 of the RIS

[redacted]

[redacted]

cover for claims.

- The Bill grants the Oversight Authority powers to issue infringement notices, seek enforceable undertakings, seek injunctions and seek civil penalties for failure to comply with the proposed legislation. However, this mechanism simply imposes fines (payable to the government) on governmental bodies or businesses, but provides no means of financial redress to the person who is actually harmed by the breach; whether from data breaches, unauthorised use of information or even exclusion from access to the digital identity system.

  By contrast, accredited entities are taken to have contracted with other accredited entities and participant relying parties and any breach by one party enables the party alleging breach to apply to the Federal Court for remedies, including compensation.

  This Bill provides **no** additional redress or access to compensation for individuals who are adversely impacted by the Digital Identity system (whether through breach of privacy or data protections or through inability to access the system).

Back-door route to consistently rejected national identity card system

- This form of digital identity system is a back-door route to a national identity card, which Australians have consistently rejected[5].

  The Regulatory Impact Statement admits this in its statement that the "government entities [are] leading the development of a national federated Digital Identity System" and its vision for the system is that "people will be able to verify their identity with their choice of identity providers to create a Digital Identity" which they can reuse "to transact across all tiers of government and with private sector services"[6]. It is a 'whole-of-economy solution' aiming to 'integrate data and technologies'. In addition, mutual recognition work is underway with other jurisdictions, which suggests that the system will be used and accessed also by foreign entities.

  The RIS references the wariness of the majority of Australians to providing digital and, in particular biometric, information to a business, organisation or government agency and that Australians are generally uncomfortable with personal information being shared[7]. This is attributed to the prevalence of identity crime. However, it could equally be attributed to a distrust of the use of an individual's personal data by third parties, including governments. Introducing such a system will not make individuals more comfortable in providing their personal data; it would make them even more hesitant to do so.

  I do not accept that online security provides justification for the introduction of such a system, nor do 'efficiency opportunities' provide sufficient benefit for individuals or businesses who

---

[5] https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/archive/identitycards

[6] Page 4 of the RIS

[7] Page 28 of the RIS

[redacted]

[redacted]

will be subject to increasing risk of loss of privacy, unauthorised use of information, red tape and regulation as well as higher business and operational costs which are inevitably passed on to consumers. Indeed, the RIS anticipates that fees will be charged by relying parties accessing the system[8].

- This digital identity system will allow for the introduction of full governmental control of access by individuals to government and business services. There will, inevitably, be a desire by government to ensure that all services are verified using a single digital platform. Whilst the RIS indicates that the Australians who cannot or do not wish to use a Digital Identity can continue to access government and other services at shopfronts or over the phone, it is by no means certain or guaranteed that such access will be continued in future. During lockdowns, access to storefronts has not been possible and many business operate with limited phone access to the public. It is also unclear how other forms of identity verification will interact or remain available to the public.

Insufficient and unclear protections regarding the use of data

- The protections on the use of the digital and, in particular, biometric information obtained under this system are unclear and insufficient.

  Whilst the Bill prohibits disclosure of biometric information to law enforcement[9], "digital identity information" can be disclosed where the enforcement body reasonably believes that a person has committed an offence or has breached a law[10]. The Bill defines "digital identity information" to mean information that is generated from the digital identity system, being the system that manages the verification of the identity of individuals. It is unclear how these inconsistent provisions are intended to operate in practice and would appear to provide a broad ability for enforcement bodies to demand disclosure from what appears to result in a centralised and larger repository of individual personal information and biometric data.

  In addition, the TDI Framework Accreditation Rules anticipate the use of biometric data for testing purposes[11] and to undertake detection of digital identity fraud[12].

- The RIS indicates that legislation will ensure that relying parties may not compel individuals to use the system to access services and, with some exceptions, must continue to provide alternative options for identity verification[13].

  Whilst there is reference in the Bill to a participating relying party not requiring an individual to use the digital identity as a condition of being able to access their services, it is possible for the participating relying party to gain an exemption from the Oversight Authority. It is unclear in what circumstances an entity would be entitled to such an exemption.

[8] page 67 of the RIS
[9] section 76 of the Bill
[10] section 81 of the Bill
[11] Section 3.9.2 of the Framework
[12] section 3.9 3 of the Framework
[13] page 66 of the RIS

[redacted]

[redacted]

It is considered that the legislation would need further safeguards to ensure individuals will be able to use alternative options for verification indefinitely. There must be no denial of access to any service by the provider, nor the introduction of any element of incentive or coercion for individuals to use this Digital Identity service, under any circumstances and without the application of any exceptions.

In addition, further clarity would be required where an individual requests the deactivation of their digital identity, including further details regarding what happens to the data which has been provided relating to that individual and how an individual can be confident that all relevant data relating to that individual has been permanently removed.

Concerns over the Independence of the Oversight Authority

- It is unclear how it will be ensured that the Oversight Authority is independent, not otherwise conflicted and completely transparent. The Oversight Authority is appointed by the Minister, supported by Australian Public Service staff and by an advisory board and committees appointed by the Minister. It is difficult to see how the Oversight Authority will be independent of government (and regulate government bodies' access to the Digital Identity information).

  A permanent oversight body comprising members of the government which are essentially overseeing government bodies (as well as private businesses) does not provide a framework which instils greater confidence than the operation of the free market.

  In addition, it is unclear as to how the Oversight Authority will evidence its transparency and how decisions made by the Oversight Authority will be reported.

Yours sincerely,

[redacted]

[redacted]