Cohesion Consulting submission to the Trusted Digital Identity Bill 2021 – exposure draft

Cohesion Consulting Pty Ltd is a small boutique IT security consultancy specialising in cyber security consulting and IT services to the public and private sector. We welcome the opportunity to make this submission in relation to the draft legislation. Cohesion Consulting believes that public trust, careful design and effective government policy in any digital security system is paramount to its effectiveness and uptake by the broader community.

Executive summary

In the current environment where there have been numerous high profile data privacy breaches around the world in an already highly data saturated society, there is growing concerns of the erosion of personal liberties and an increase in the overreach of government to impose and monitor daily life in Australia.

With the recent announcement of proposed of a "covid passport" passport system further restricting access to goods and services based on vaccination status, this bill exacerbates the perception that the Australian government is further overreaching its remit and further eroding public freedoms by imposing the concept of identity for online transactions. Add to this the Australian government's poor track record in implementing even modestly sized IT systems much less one such as this on such a far reaching scale, and there is very little appetite to see this bill pass into law.

With this in mind, we express concerns about this bill in its current form:

- The draft bill fails to provide the clarity that addresses legitimate public concerns about the government's ability to protect individual data privacy. Public concerns are well founded. The sensitivity of personal information (including biometric data) that will be managed by such a system, demands an exceedingly high standard of care to ensure it is not misused, disclosed, and used for nefarious reasons. The bill fails to provide that assurance.
- While the system is intended to be "voluntary", as it is rolled out more widely and businesses adopt it, then those who decline to participate in the system will be excluded from these essential services. This is a form of implicit coercion which makes the original intent of "voluntary participation" meaningless.
- The act has poorly defined and weak compliance and enforcement framework that fails to ensure there is significant incentive for entities to enact the highest of standards. The bill has weak liability and redress measures for breaches by participating entities, especially for large organisations in jurisdictions outside of Australia. This leaves individuals exposed to privacy breaches with no reasonable redress for injury incurred.
- Penalties are laughably inadequate and will have little deterrent effect. Where breaches may occur, there is scant assurance that enforcement will be even possible against participating entities from overseas jurisdictions.

For these reasons, Cohesion Consulting wholly rejects this bill and its justification.

Critique and recommendations

Chapter 2

Part 2 – The trusted digital identity system

Division 2 – Onboarding to the trusted digital identity system

---

Section 23 Conditions relating to restricted attributes of individuals

(1) …

(2) In deciding whether to impose the condition, the Oversight Authority must have regard to the following matters:

(a) the potential harm that could result if restricted attributes of that kind were disclosed to an entity that was not authorised to obtain them;

(b) community expectations as to whether restricted attributes of that kind should be handled more securely than other kinds of attributes;

Critique: Sections (a) and (b) do not state what "potential harm" or "community concerns" means. The Oversight Authority shouldn't have the arbitrary power to assert what it thinks is "community expectations" or "potential harm" is when it is not representative of the community.

Recommendation (2): A creation of a public standards and community expectations body of lay experts and members of the public must be included in the bill to ensure that community standards are reflected in the enforcement of such rules.

Division 4 – Other matters relating to the trusted digital identity system

---

Section 31 Holding etc. digital identity information outside Australia

(1) The TDI rules may make provision in relation to the holding, storing, handling or transfer of digital identity information outside Australia if the information is or was generated, collected, held or stored by accredited entities within the trusted digital identity system.

Critique: The ability to hold, store and handle an individual's private data outside of Australia goes against the fundamental notion that an individual must have control over their data. The ability of an individual to enforce (if required) through legal action for the breach of this privacy is exceedingly difficult and cost prohibitive if the holding entity (service provider) is located outside of Australia. Individuals will have to effectively relinquish protection and redress for breaches of their personal data. This is not a satisfactory outcome.

Recommendation (3): The Australian government must provide guarantees that the cost to individuals seeking legal redress for data privacy breaches by an accredited entity are underwritten by the Australian government. This ensures that the principle of data privacy is strongly asserted.

Division 3 – Redress framework

"Section 43 Redress obligations of accredited entities

(1)…

(2) As soon as practicable after becoming aware of the incident, the accredited entity must make all reasonable efforts to contact:

(a) any individuals affected by the incident; and

(b) if the digital identity of an individual acting on behalf of a business has been compromised—that business."

Critique: This section lays out a proposed framework for redress obligations of accredited entities.

- Subsection (2) states that upon becoming aware of an incident, the entity must "contact" the individuals affected. Apart from the courtesy to notify, this offers little comfort to the affected individuals.
- Subsections (1), (2) and (3) set out civil penalties of "200 penalty units" when there is a (vaguely defined) "incident". Under Commonwealth penalty values, the current value of a penalty unit is $222. Therefore, these penalties represent a value in today's money (as at October 2021) of $44,400. This is inadequate for the following reasons:
    1. 200 penalty units are in Australian dollars, so for foreign entities this may not represent a reasonable disincentive when converted to their local currency.
    2. The term "incident" is not clearly defined relative to this section. Is an incident a class of breaches or is it 200 penalty units for *each* individual incident? E.g. If 5000 people are affected, is that one incident or 5000 separate incidents?
    3. The penalties are a standard size irrespective of the benefit derived and detriment avoided from the breach. That is, it's a "one size fits all" penalty. This is wholly inadequate.

Recommendations

1. **The bill must define more clearly what constitutes an incident. We recommend that penalties must be commensurate with the number of individuals that are impacted. That is, if 5000 individuals experience data breach injury, then the penalty should be applied as a multiple of the number of individuals impacted.**
2. **Merely demanding a feeble requirement to only contact an impacted individual is inadequate. There must be a baseline penalty payable to each individual by the offending entity or participating relying party to remediate for the data privacy injury incurred.**

"46 Oversight Authority to assist individuals and businesses affected by incidents

If an individual is affected by a digital identity fraud incident or a cyber security incident, the Oversight Authority must provide reasonable assistance to such individuals and businesses, including by:

(a) informing individuals and businesses affected by the incident about support services available to them; and

(b) providing individuals and businesses affected by the incident with the contact details of the accredited entities and participating relying parties involved in the incident; and

(c) coordinating the collection of information from the trusted digital identity system that relates to a particular incident; and

(d) facilitating the sharing of information that relates to particular incidents between entities involved in the incident; and

(e) monitoring, and reporting on the nature and quality of the services provided by accredited entities and participating relying parties to individuals and businesses affected by an incident."

Critique: Similar to the critique of section 45, these obligations upon the Oversight Authority are at best, enfeebled. Merely just facilitating communication between injured party and accredited entity does not constitute satisfactory "assistance". It means that the Australian government has side-stepped its responsibility to protect Australian individuals and businesses, leaving the burden for any data breach injury with the individual or business.

Recommendations: The language of the act must be strengthened to ensure that the Australian government underwrites the cost of remediating any data breach injury incurred by an individual or business. It must also create a legal enforcement framework to recoup costs to Australian tax-payers from offending accredited entities and participating relaying parties. Such an amendment will strengthen public trust in the system.

Chapter 4 – Privacy

Part 2 – Privacy

Division 2 – Additional privacy safeguards

---

76 Restrictions on collecting, using and disclosing biometric information

(1) An accredited entity may collect, use or disclose biometric information of an individual only if:

(a) the collection, use or disclosure is authorised under section 77 or 78; and

(b) the individual to whom the information relates has expressly consented to the collection, use or disclosure.

Critique: While the intent of 76 (1) (b) to ensure consent is clear, the implementation of what "consent" means is relevant. If a government service provider (e.g. Medicare, social security, passport office) or other entity participating in the system, states in the fine print that in using its services, the individual agrees to having their biometric information stored, collected and disclosed, does that constitute consent? Are images captured in public places on CCTV considered "consensual"? Where such services are essential (such as social security payments), individuals won't have the reasonable option to deny consent. We don't want the data identity equivalent of "click here to accept all our terms and conditions" as you would downloading an app to your phone!

Recommendation: The wording of what "consent" means must be strictly defined including who it strictly applies to. The language may be better defined by asserting "informed consent" in the manner that consent is granted for medical and other healthcare procedures and interventions. It implies that the individual is informed of the pros and cons of providing consent and has access to such information to allow them to make a fully informed choice.

Sections:

- 81 – Digital identity information must not be used for prohibited enforcement purposes
- 82 - Digital identity information must not be used or disclosed for prohibited marketing purposes
- 83 – Accredited identity exchanges must not retain attributes or restricted attributes of individuals

---

Critique: While the intention behind these sections is laudable, the ability for a centralised Oversight Authority to enforce these measures, especially as adoption by private enterprises and business expands exponentially throughout the community, will be nigh on impossible. It renders these sections as effectively impotent.

Recommendation: The act must consider how the enforcement of these (and other related privacy considerations) are going to scale as the uptake of the system increases. We recommend that a federated organisation of enforcement powers (e.g. by industry sector) be considered to accommodate this inevitable scalability problem.

Chapter 7 – Administration

Part 2 – Registers

---

*"*118 *TDIS register*

*(1) The Oversight Authority must establish and maintain a register (the **TDIS register**) of entities who have onboarded to the trusted digital identity system.*

(2) The TDIS register must contain the following details for each entity:

(a) the day the entity's approval to onboard to the trusted digital identity system came into force;

(b) the entity's onboarding day;

(c) if the entity is a participating relying party

:

:

: "

Critique: While we commend the intention of this section, we recognise the importance of full public disclosure of any data breaches by an entity. This would help increase overall accountability and elevate public confidence in the system

Recommendation:

- **We recommend extending the TDIS register, or in the absence of doing so, support the creation of a data breach register to publicly publish all identified security and data privacy incidents for each participating entity. This will elevate public trust and apply a higher level of accountability for all accredited entities for their data security obligations under the act.**
- **It is not clear if the TDIS will be publicly available. The wording must be amended to state that it will be publicly available.**