Australian Banking Association

18 December 2020

Jonathon Thorpe

a/g General Manager Digital Identity and myGov

Digital Delivery & Corporate Division

Digital Transformation Agency

Dear Mr Thorpe

Digital Identity Legislation: consultation paper

The Australian Banking Association (ABA) is pleased to make this submission to the Digital Transformation Agency (DTA) consultation on proposed digital identity legislation.

Benefits of government initiative and need for legislation

The Government has laid out a forward-looking vision for how digital identity services could be used to improve government service delivery and bolster privacy protections for citizens. The DTA is seeking to extend the Trusted Digital Identity Framework (TDIF) beyond federal government agencies, to state and territory agencies and the private sector.

The ABA welcomes the development of a digital identity ecosystem that supports interoperability between different solutions (both public and private), allows for customer choice and improves digital customer verification processes across the economy. Banks are actively exploring digital identity initiatives and see the benefit of collaboration between government and industry.

The interests of the Australian economy will be better served if there is flexibility to innovate and respond to the needs of consumers and businesses, instead of establishing a single government digital identity scheme. Government can also achieve genuine collaboration with industry without legislation.

As such, the intended scope and coverage of the proposed digital identity legislation should be limited to areas where parliamentary authority is explicitly required for the extension of the TDIF. This means:

- Legislation should only apply to instances where a party has been accredited by the TDIF and is transacting via a TDIF-accredited platform.
- The Government does not seek to establish a single government digital identity scheme in Australia and does not mandate a single digital identity framework.
- Access to Government services will not be limited to a government digital identity.

The ABA also considers:

- Matters that go to the operation of solutions within the TDIF are best left to operating rules and industry standards. Prescribing such matters in legislation may hamper the development of future digital identity schemes or reduce the incentives for the private sector to become participants of any government digital identity system.
- Where rules and standards are being created for digital identity solutions (whether or not they are TDIF-accredited), the Government should co-design these rules with the private sector to ensure that they align with industry best practice and do not hamper innovation.
- Digital identity information should be dealt with under the *Privacy Act 1988* (Privacy Act), rather than establishing a bespoke digital identity privacy regime that can diverge from the Privacy Act over time.

Australian Banking Association

Matters that are appropriate for legislation

The ABA makes the following suggestions in Table 1 on the matters or functions that have to be dealt with and/or be enforceable under legislation, and the matters or functions that can be enforced by contract under rules and policies. This means distinguishing between the proposed digital identity legislation, the TDIF and specific digital identity schemes. Key points are:

- Contractual arrangements have been proven to be successful in financial market infrastructure and payments.
- Legislation should be limited to matters that need to be prescribed or addressed by legislation and should not veer into specific solution designs. This will help to ensure legislation accommodates future innovations in this area and not unintentionally inhibit the development of digital identity schemes, ownership arrangements and business models.
- Legislation should avoid prescribing bespoke obligations and requirements where possible. This is particularly important in relation to privacy protections, and is also relevant for protection for victims of identity theft.
- Information that may be digital identity information will evolve, and not all digital identity schemes will operate under the proposed digital identity legislation.
- Simplicity and consistency will help consumers to understand what remedies are available and how to seek redress.

Table 1: matters that are appropriate for legislation

Matter or function	**Is legislation necessary**
Legislation to ensure constitutionality	DTA has stated that legislation is needed for constitutional reasons. The ABA seeks clarity about whether legislation is intended to offer myGovID to state/territory governments and the private sector, or to enable non-Commonwealth government entities to seek accreditation under TDIF. The ABA considers legislation should only apply to participants who have been accredited under the TDIF.
Establish body to administer framework rules	The ABA queries whether an oversight authority is necessary. The ABA also seeks clarity on whether the body would have responsibility for administering the legislation or would also have responsibility for administering TDIF. If other frameworks can operate under the proposed legislation, the ABA seeks clarity about the mechanism for doing so and consequences for the non-TDIF framework. Also refer to additional commentary about the role and mandate of the oversight authority below.
Complying with Privacy Act	The ABA agrees legislation may be needed, to the extent some parties are not already subject to the Privacy Act. The ABA seeks clarity on whether the extended application of the Privacy Act would apply to TDIF only or to all frameworks that operate in accordance with the legislation.
Establish safeguards for digital identity information	The ABA agrees digital identity information should be protected.

	However, our strong preference is for relevant protections to be established under the Privacy Act. The digital identity legislation can cross-refer the Privacy Act and/or clarify how the Privacy Act applies. This would ensure consistency between digital identity legislation and the Privacy Act in the protections and requirements that apply in relation to the same information. The pool of information that could constitute digital identity information will evolve over time. This would also ensure digital identity frameworks that do not operate under the proposed digital identity legislation are required to give consumers the same level of privacy protection.
Power to set rules	If the oversight authority will have responsibility for administering TDIF, it is for government to determine whether legislation is needed for the authority to have powers to set rules. The ABA notes administrators of other digital identity frameworks will not require legislation. If there is an oversight authority, the ABA recommends industry participation (including from private sector solution providers) to ensure that standards and accreditation takes into account industry best-practice and are not inhibiting innovation in the market. The ABA considers matters that should be dealt with in rules should not be prescribed under legislation. Refer comments below about charging model, liability, protections for victims of cybercrime and identity fraud, and transparency of fees and charges.
Enforcement of obligations and rules	If the proposed digital identity legislation will impose obligations, it may be necessary for the oversight authority to have enforcement powers in relation to those obligations. However, in relation to the TDIF, the ABA suggests government consider whether contractual enforcement mechanisms would be preferable to enforce TDIF rules and policies, noting contractual arrangements underpin critical payments and financial market infrastructure and have been proven to be effective. If government prefers to use legislation to provide certainty, legislation can be limited to ensuring the enforceability of contract between oversight authority and relevant parties.
Charging model	The ABA considers fees and charges should not be prescribed in legislation, as doing so can unintentionally inhibit private sector adoption of the government digital identity legislative regime and inhibit innovation. Prescribing fees can hamper the innovation of business models (such as bundled or value-added transactions). The proposed charging model may be a disincentive for other digital identity frameworks to operate under the proposed digital identity legislation.

Transparency of fees and charges	The ABA considers ensuring transparency of fees and charges, and what services will be provided, is key. Legislation may not be necessary to provide for transparency, and any requirement should not be prescriptive as to content or form.
Liability	This is distinguished from enforcement of legislative obligations. The ABA considers legislation should not prescribe a liability model, and instead should provide flexibility for digital identity schemes to determine the allocation and pricing of liability. Doing so would also enable innovation in business models and services. If the Government intends to prescribe a liability framework, it may be appropriate to define levels of protection for impacted groups, such as minimum levels of consumer protection.
Protections for victims of cybercrime and identity fraud	The ABA suggests the Government consider whether existing schemes such as IDCare are sufficient. If there are gaps, a preferable approach may be to ensure protections apply to all victims of identity fraud and cybercrime. Simplicity will help consumers to understand what remedies are available and how to seek redress.

Additional comments

The ABA also provides comments on the following proposals.

Charging framework

The consultation paper states a charging framework will help to ensure the system is financially sustainable. The consultation paper also proposes giving the Oversight Authority legal powers to set and administer a charging framework. The consultation paper further proposes that participants will be levied a single charge that covers all of their activities within the system, and the Oversight Authority will have responsibility for collecting the charges and distributing funds to participants.

The ABA does not consider a charging model is an appropriate matter for legislation. Commercial decisions about fees and charges are closely tied to the services offered (including levels of authentication), product innovations (such as bundled or value added payments, noting these will comply with applicable privacy protections), and pricing of liability.

A charging model should be distinguished from:

- Potential participants understanding and assessing the cost of participating in a digital identity scheme: this relates to transparency, not the specifics of a charging model.
- Financial sustainability of the oversight authority (if one is required).
- Speed and ease of dispute resolution. Contractual arrangements have been proven to be effective, refer the arrangements for payments and financial market infrastructure.

Finally, the ABA seeks clarity on whether fees will be set so as to recover sunk costs. This clarity is needed for private sector decision-making about investment in digital identity initiatives. The charge model should be established in a way that is consistent with existing Government policy (including the Department of Finance's Charge Model Framework) to ensure that the commercial construct does not undermine investment in private sector solutions.

Liability

The ABA does not consider liability to be an appropriate matter for legislation, for similar reasons as above. The liability of private sector participants when interacting with government entities will need to be defined, but the TDIF liability provisions may not be appropriate for other digital identity schemes. Allocation of liability is also related to considerations of pricing (for example, pricing for potential liability shift). As such a prescriptive approach to liability can hamper the development of digital identity solutions or reduce incentive to participate in the TDIF.

Allocation of liability under a digital identity framework or scheme should be distinguished from:

- Enforcement of legislative obligations and of a standard of behaviour. Enforcement of behaviour or conduct is appropriate for rules or legislation and would not depend on questions of liability (whether a loss has occurred) or agreements between parties about the allocation of loss and liability.
- Dispute resolution. Noting the effectiveness of contractual arrangements.
- Support for support victims of identity theft, noting existing schemes such as IDCare and the case for any support arrangements to be available to all victims of identity theft.

Privacy protections

The legislation proposes enshrining privacy and consumer protection requirements of the TDIF into law. The consultation paper also acknowledges the Government is undertaking a review of the Privacy Act.

The ABA considers the preferred approach is for privacy protections to be enshrined in the Privacy Act, and for the digital identity legislation to cross-reference terms and concepts in the Privacy Act and/or clarify their application. The pool of information that may constitute digital identity information will evolve over time, and not all digital identity schemes used by Australian consumers will operate under the proposed digital identity legislation. The concepts of digital identity information, biometric information and restricted attributes appear to imperfectly overlap with concepts of personal information and sensitive information under the Privacy Act.

Inconsistencies in legislation can add legal and operational complexity and discourage participation in the digital identity system. Importantly, complexity also makes it harder for consumers to understand what protections are afforded their information and manage consents on an informed basis.

Specific consideration should also be given to requirements relating to consent management and a possible right to erasure under the Privacy Act.

Finally, the ABA seeks clarity on the proposals relating to biometrics: whether legislation or rules will set standards for biometric checks or whether the administrator of the system will undertake the biometric checks. The latter may give rise to concerns about competitive neutrality.

Oversight Authority

The ABA queries whether an Oversight Authority is needed and what would be the Authority's role. If the Government proposes to establish an Oversight Authority, the role and mandate of the Oversight Authority should align with these principles:

- The Authority cannot have a conflict of interest between accreditation and enforcement, or the Authority needs to be structured so it can carry out each role effectively.
- The Authority should be structured so enforcement can occur and there is no gap in accountability.
- Rule-making by the Authority should be structured so it draws on private sector expertise and meaningfully reflects the interests of participants in the system.

These principles do not prevent the Oversight Authority role being carried out by two agencies.

Australian Banking Association

Interaction with other regimes

Consumer Data Right (CDR): the ABA has previously stated that digital identity is necessary to enable the next expansion of the CDR to read-write access, and the two regimes must be interoperable. However, CDR and digital identity should be dealt with separately.

Anti-money laundering/counter terrorism financing (AML/CTF): the consultation paper states the proposed legislation is 'intended to create opportunities to support the operation of existing legislation, for example the identification aspects of the *AML/CTF Act'*. The AML/CTF Act may need to be amended or regulatory guidance provided to clarify how entities can use digital identity to place reliance on another party that conducts know your customer (KYC) procedures. Further amendments to the AML/CTF regime may also be considered to improve efficiency, for example by allowing a user to update their identity information once across the system.

Interactions with other aspects of Government policy agenda

In its response to the Privacy Act review, the ABA has highlighted the multitude of live policy/legislative consultations and other government initiatives which overlap and will impact on considerations of privacy. Many of these initiatives also have implications for the proposed legislation.

The ABA response to the Privacy Act review urged the Government to first design an overarching blueprint and roadmap for data and information privacy. Without oversight and co-ordination, it is a risk that no reform will fully achieve the intended outcomes because siloed approaches will potentially conflict with or hinder the planned benefits of the other government initiatives. We reiterate this request in context of the DTA consultation.

Conclusion

Thank you for the opportunity to provide feedback, the ABA looks forward to working with the DTA on further stages of this consultation.

Yours faithfully

Rhonda Luo

Policy Director