Queensland Law Society

Law Society House, 179 Ann Street, Brisbane Qld 4000, Australia
GPO Box 1785, Brisbane Qld 4001 | ABN 33 423 389 441
P 07 3842 5943 | F 07 3221 9329 | president@qls.com.au | qls.com.au
Office of the President

15 July 2021

Our ref: [LP: MC]

Confidential

Digital Transformation Agency
PO Box 457
Canberra City
ACT 2601

By email: digitalidentity@dta.gov.au

Dear Digital Transformation Agency

Digital Identity Legislation Position Paper

Thank you for the opportunity to provide feedback on the Digital Identity Legislation Position Paper. The Queensland Law Society (**QLS**) appreciates being consulted on this important discussion paper.

QLS is the peak professional body for the State's legal practitioners. We represent and promote over 13,000 legal professionals, increase community understanding of the law, help protect the rights of individuals and advise the community about the many benefits solicitors can provide. QLS also assists the public by advising government on improvements to laws affecting Queenslanders and working to improve their access to the law.

This response has been compiled with the assistance of the QLS Technology & Intellectual Property Law Committee, Innovation Committee and Privacy & Data Law Committee, whose members have substantial expertise in this area.

The following comments are intended to provide brief, high-level feedback on the proposal for a digital identity system. They are not intended to provide comprehensive feedback on the implementation or operation of the digital identity system. QLS intends to provide more complete feedback when draft legislation is released for review.

We acknowledge that the legislation is not intended to apply to all digital identities and digital identity systems in Australia; rather the proposal is confined to existing Commonwealth Government digital identity systems and participating State and Territory Government bodies and companies.

For the legal sector, the COVID-19 pandemic, and the associated restrictions on face-to-face interactions, have highlighted the utility of technology in facilitating interactions with clients and providing certain legal services, particularly for clients who live in regional or remote areas or those who have difficulty traveling to a solicitor's office for a range of reasons including caring or work responsibilities or disability. As lawyers increasingly rely on email, teleconference and

videoconference to interact with clients, the courts and other parties, it is important that they have safe and reliable means by which to confirm the identities of the people with which they are interacting.

Despite potential benefits, any digital identity system will need to be carefully constructed and controlled in a way that prioritises reliability, information security, governance, privacy and consumer safeguards. The design of the system will need to take into account the following considerations:

- The per-transaction cost of any solution should be minimised to ensure the digital identity system is accessible, including for small business transactors.
- Access to the digital identity system should not create unwarranted 'red tape', complex processes, a steep learning curve for users, or other burdens on business transactions where verification of identity is necessary.
- Where relevant, digital identification systems should integrate with other legislative regimes that require verification of identity, such as the Personal Property Securities Register, State and Territory Land Title Offices, and the forthcoming DirectorID system. We note that this may require multi-level governmental adoption and implementation of the digital identity system.
- Any 'trustmark' should be secured as a registered trade mark (for example, as a certification mark) and/or otherwise protected by legislation to enable protection and enforcement of the trust regime. To ensure transparency, Standards or Rules for the issuance of 'trustmarks' should be publicly available for consultation prior to being submitted to the Australian Consumer and Competition Commission.
- The reliability and trustworthiness of the accredited providers within the digital identity system will be integral to the overall success of the system. Managing the participants in the system will be important to ensuring the overall integrity of the system. This may involve implementing robust procedures to respond to participants who misuse the system or fail to comply with the legislation and other privacy and information security obligations.
- The digital identity system and the governance arrangements for the system must prioritise privacy safeguards for individual users. Critically, the digital identity system must implement and maintain appropriate and effective technological and organisational measures to guard against data breaches, fraud and misuse. Prioritising information security and the on-going integrity, availability and resilience of the system will be essential in generating (and maintaining) public confidence and use of the system.
- Related to this, the legislative framework for the digital identity system must provide for appropriate independent oversight (we welcome the proposed establishment of the Oversight Authority and retained policy function of the DTA), as well as an accessible and practical means of redress for individuals (particularly with respect to identity theft).
- The digital identity system will need to maintain an element of flexibility to accommodate possible developments and reforms in privacy law that may impact the use of digital identity data.
- Provisions should be made to enable persons to opt out of the creation of a digital identity, alter or amend their digital identity and require their digital identity to be deleted. People using the digital identity system should be able to engage anonymously where appropriate, to ensure that they are not required to identify themselves for all transactions (such as online purchases from an online-only retailer).

- We note that the right to have a digital identity deleted may conflict with the proposed record keeping obligations with respect to meta data and activity logs. The 7 year record-keeping obligation with respect to meta data and activity logs will need to be balanced against the potential privacy impacts for individuals.
- Finally, regard should be had to how the digital identity system may impact access to justice and important social support services. While digital identity has the potential to promote access to justice and access to services by, for example, enabling remote transactions for people who cannot easily travel, it may also exclude people who cannot (or choose not) to engage in the digital identity system. Those without access to or the ability to use technology, including some older persons and people with disability, may be particularly excluded.

If you have any queries regarding the contents of this letter, please do not hesitate to contact our Legal Policy team via policy@qls.com.au or by phone on (07) 3842 5930.

Yours faithfully

Elizabeth Shearer
President