Office of the Information Commissioner
Queensland

Level 7
133 Mary Street
Brisbane Q4000

PO Box 10143
Adelaide Street
Brisbane Q4000

Phone (07) 3234 7373
www.oic.qld.gov.au

ABN: 70 810 284 665

27 October 2021

Digital Identity
Digital Transformation Agency
PO Box 457
CANBERRA CITY ACT 2601

By electronic submission

Trusted Digital Identity Bill 2021

The Queensland Office of the Information Commissioner (**OIC**) welcomes the opportunity to provide a submission on the exposure draft of the Trusted Digital Identity Bill 2021 (**the Bill**).

The stated purposes of the Bill are to:

- enable the expansion of the Australian Government Digital Identity System, specifically to enable greater participation by state and territory governments and the private sector
- enshrine in law various privacy and consumer protections, so that Australians can have confidence in the System and know that their personal information is safe and secure
- establish permanent governance arrangements and a strong regulatory regime.[1]

OIC notes that the Bill enshrines in law two distinct voluntary schemes, the Australian Government run digital identity system (trusted digital identity system) and the TDIF accreditation scheme, for entities wanting to provide or rely on digital identity services.

OIC acknowledges the significant and wide-ranging consultation undertaken by the Digital Transformation Agency (**DTA**) on the development of the Bill and notes that Digital Identity can be privacy enhancing by improving the integrity of identity information, combatting identity theft and the fraudulent use of stolen and assumed identities.

About the OIC

The OIC is an independent statutory body that reports to the Queensland Parliament. We have a statutory role under the *Right to Information Act 2009* (**RTI Act**) and the *Information Privacy Act 2009* (**IP Act**) to facilitate greater and easier access to information held by government agencies. We also assist agencies to understand their obligations under the IP Act to safeguard personal information that they hold.

OIC's statutory functions include mediating privacy complaints against Queensland government agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting audits and reviews to monitor agency performance and compliance with the RTI Act and the IP Act. Our office also reviews agency decisions about access and amendment to information.

The Office of the Information Commissioner is an independent statutory authority.

The statutory functions of the OIC under the Information Privacy Act 2009 (Qld) (IP Act) include commenting on the administration of privacy in the Queensland public sector environment.

This submission does not represent the views or opinions of the Queensland Government.

[1] https://www.digitalidentity.gov.au/have-your-say/phase-3

OIC provides the following high-level comments on certain aspects of the Bill:

1. Privacy and consumer safeguards

OIC welcomes new privacy and consumer protections enshrined in primary legislation and considers these new protections are critical to enhancing community trust and confidence in the Digital Identity system. OIC considers the privacy protections contained in the Bill, with regulation and oversight of the additional privacy safeguards by the Australian Information Commissioner, address a number of privacy concerns raised by the establishment of a digital identity system such as data profiling, surveillance, and use and disclosure of biometric information. Additional privacy protections entrenched in the Bill include:

- requirement for express consent to disclosure of attributes of individuals to relying parties
- prohibition on single identifiers
- restrictions on collecting, using and disclosing biometric information
- prohibition on data profiling
- prohibition on certain marketing purposes
- digital identity information must not be held, stored, handled or transferred outside of Australia (with limited exceptions)
- limits on use of digital identity information for enforcement purposes; and
- providing individuals with the right to request an accredited identity service provider to deactivate their digital identity.

The privacy protections entrenched in the Bill are further strengthened by the expanded definition of 'personal information' under the Commonwealth Privacy Act to include attributes, restricted attributes and biometric information and these new legislated safeguards are additional to existing protections under the Commonwealth Privacy Act. Under the Bill, the Australian Information Commissioner has been granted additional powers to seek enforceable undertakings, seek injunctions and seek civil penalties for breaches of the additional privacy safeguards.

While OIC notes the additional privacy safeguards in the Bill apply to all accredited entities, whether or not they are onboarded to the trusted digital identity system (TDIS), civil penalties for non-compliance with the additional privacy safeguards in the Bill only apply if the contravention occurs within the TDIS. This means that if an accredited entity chooses not to onboard to the TDIS, there is no civil penalty for contravention of the additional privacy safeguards, no obligations and penalties imposed under the redress framework in the Bill and no powers granted to the Australian Information Commissioner for investigation and enforcement, potentially leading to a weakening of the additional privacy safeguards.

2. Introduction of Digital Identity Bill without legislation in place to support the National Driver Licence Facial Recognition Solution

In its previous submission on the Digital Identity Legislation Consultation Paper, OIC raised concerns that the re-introduced Commonwealth Identity-Matching Services Bill

2019 (**IMS Bill**) had not been passed. It is OIC's understanding that the IMS Bill is yet to be passed and the timeframe remains uncertain.

The IMS Bill provides the authorisation for the Department of Home Affairs to develop, operate and maintain two centralised facilities for the provision of identity-matching services, namely:

- an '**interoperability hub**' operating as a router through which participating government and non-government entities can request and transit information as part of an identity-matching service; and
- the **National Driver Licence Facial Recognition Solution** (NDLFRS), a federated database of information contained in government identity documents such as driver licences.

In October 2019, the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) recommended[2] the IMS Bill is re-drafted amid serious concerns that the privacy safeguards were not sufficient in their existing form. Importantly, the Committee outlined a broad set of principles and findings to be used as a template for the re-drafting of the IMS Bill.

It is OIC's understanding that the IMS Bill, which is intended to govern the operation of the Document Verification Service (**DVS**) and Face Verification Service (**FVS**), will complement the Digital Identity Legislation. It is OIC's view that the revised and strengthened IMS Bill needs to be passed and the NDLFRS operational before there can be any reliance on it to establish Digital Identity. OIC further notes that despite the legislation underpinning the NDLFRS not being passed, the Victorian, South Australia and Tasmanian governments have uploaded their driver licence images to the NDFLRS.

3. Privacy coverage across state and territories

OIC notes that the Bill requires any entity applying for accreditation to be covered by the Commonwealth Privacy Act, or the entity opts in to the rules in that Act. State and territories are not required to be covered by the Australian Privacy Principles (**APPs**) if they are already covered by laws with privacy protections comparable to those provided by the APPs. For those state and territory entities in jurisdictions without privacy legislation, the Bill provides a further option of entering into a trusted provider agreement with the Commonwealth.

The Bill is silent on who decides whether the privacy laws of a state or territory offer comparable privacy protections to the those provided by the APPs. OIC has previously raised that is not certain that Queensland's current privacy laws offer equivalent coverage to the Commonwealth Privacy Act. The current review of the Commonwealth Privacy Act may lead to a further widening of the gap between Commonwealth, State and Territory privacy legislation. OIC considers that any determination of equivalency of state and territory privacy laws should not be left to self-assessment by the states or territories, which may lead to inconsistencies in privacy coverage and potentially challenge by other participating jurisdictions.

[2] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019*, October 2019.

While the Bill provides the additional option of entering into a trusted provider agreement, under the current provisions of the Bill, it is open to a state or territory to assert that their privacy laws offer comparable privacy protections to those provided by the APPs under the Commonwealth Privacy Act.

4. Data Breach Notifications

OIC notes that under the data breach notification provisions in the Bill, accredited entities are required to either notify the Office of the Australian Information Commissioner (**OAIC**) under the Notifiable Data Breaches Scheme (**NDB**) or notify under a comparable state or territory data breach notification scheme. It is not certain from the current drafting of the Bill what constitutes a comparable NDB scheme and which body will make that assessment.

In conclusion, while OIC notes that participation in the Digital Identity System at this time is voluntary, any transition by governments to a wholly digital identity scheme will need to ensure those sectors of the community who lack access to skills or technology resources are not excluded from the benefits of a digital economy.

Yours sincerely

Rachael Rangihaeata
Information Commissioner